GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

CCN
CENTRO CRIPTOLÓGICO NACIONAL

GUÍA DE SEGURIDAD (CCN-STIC-401)

GLOSARIO Y ABREVIATURAS

AGOSTO de 2015

Edita:

NIPO: 002-15-018-4

Fecha de Edición: agosto de 2015

José Antonio Mañas ha participado en la elaboración y modificación del presente documento y sus anexos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Agosto de 2015

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1 INTRODUCCIÓN

Este documento describe una serie de términos en materia de seguridad, tomados de glosarios y guías de referencia.

2 TÉRMINOS

2.1 A PRUEBA DE FALLOS

2.1.1 A PRUEBA DE FALLOS

Sistema automático de protección de programas y elementos de procesamiento cuando se detecta un fallo.

2.1.1 (EN) FAIL SAFE

Automatic protection of programs and/or processing systems when hardware or software failure is detected. [CNSSI_4009:2010]

2.1.2 (EN) FAIL SOFT

Selective termination of affected nonessential processing when hardware or software failure is determined to be imminent. [CNSSI_4009:2010]

2.1.1 (EN) FAIL-SAFE

1. (I) Synonym for "fail-secure".

2. (I) A mode of termination of system functions that prevents damage to specified system resources and system entities (i.e., specified data, property, and life) when a failure occurs or is detected in the system (but the failure still might cause a security compromise). (See: failure control.)

[RFC4949:2007]

2.1.2 (EN) FAIL-SECURE

(I) A mode of termination of system functions that prevents loss of secure state when a failure occurs or is detected in the system (but the failure still might cause damage to some system resource or system entity). (See: failure control. Compare: fail-safe.) [RFC4949:2007]

2.1.3 (EN) FAIL-SOFT

(I) Selective termination of affected, non-essential system functions when a failure occurs or is detected in the system. (See: failure control.) [RFC4949:2007]

2.1.4 (EN) FAILURE CONTROL

(I) A methodology used to provide fail-safe, fail-secure or fail- soft termination and recovery of system functions. [FP039] [RFC4949:2007]

2.2 A5 - CIFRADO DE VOZ GSM

Acrónimos: A5

Ver:

- *Módulo de identificación de usuario*
- *Cifrado de flujo*
- *Criptografía de clave secreta*
- *KASUMI*

2.2.1 A5 - CIFRADO DE VOZ GSM

Algoritmo secreto de cifra en flujo empleado por el sistema de telefonía móvil digital GSM (Global System for Mobile Communications), para cifrar el enlace entre el terminal y la estación base.

NOTA. El algoritmo ya no es secreto. [CESID:1997]

2.2.2 (EN) A5 - GSM VOICE ENCRYPTION

A5/1 is a stream cipher used to provide over-the-air communication privacy in the GSM cellular telephone standard. It was initially kept secret, but became public knowledge through leaks and reverse engineering. A number of serious weaknesses in the cipher have been identified.

http://en.wikipedia.org/wiki/A5/1

2.3 AAA - AUTENTICACIÓN, AUTORIZACIÓN Y REGISTRO

Acrónimos: AAA

Ver:

- *Autenticación*
- *Autorización*
- *RADIUS - Remote Access Dial-In User Server*
- *TACACS - Terminal Access Controller Access Control System*

2.3.1 AAA - AUTENTICACIÓN, AUTORIZACIÓN Y REGISTRO

Conjunto de herramientas, procedimientos y protocolos que garantizan un tratamiento coherente de las tareas de autenticación, autorización y registro de actividad de las entidades que tienen acceso a un sistema de información.

2.3.2 AAA

Acrónimo de “authentication, authorization, and accounting” (autenticación, autorización y contabilización). Protocolo para autenticar a un usuario basándose en la identidad verificable del usuario, autorizar a un usuario basándose en sus derechos de usuario y contabilizar el consumo de recursos de una red de un usuario.

http://es.pcisecuritystandards.org

2.3.1 (EN) AAA

Acronym for “authentication, authorization, and accounting.” Protocol for authenticating a user based on their verifiable identity, authorizing a user based on their user rights, and accounting for a user’s consumption of network resources.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.3.2 (EN) AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING (AAA)

Authentication, authorization, and accounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security.

As the first process, authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted. The process of authentication is based on each user having a unique set of criteria for gaining access. The AAA server compares a user's authentication credentials with other user credentials stored in a database. If the credentials match, the user is granted access to the network. If the credentials are at variance, authentication fails and network access is denied.

Following authentication, a user must gain authorization for doing certain tasks. After logging into a system, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Usually, authorization occurs within the context of authentication. Once you have authenticated a user, they may be authorized for different types of access or activity.

The final plank in the AAA framework is accounting, which measures the resources a user consumes during access. This can include the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging of session statistics and usage information and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

http://searchsecurity.techtarget.com/

2.3.3 (EN) AAA - AUTHENTICATION, AUTHORISATION AND ACCOUNTING

Authentication. Authentication refers to the confirmation that a user who is requesting services is a valid user of the network services requested. Authentication is accomplished via the presentation of an identity and credentials. Examples of types of credentials are passwords, one-time tokens, digital certificates, and phone numbers (calling/called).

Authorization. Authorization refers to the granting of specific types of service (including "no service") to a user, based on their authentication, what services they are requesting, and the current system state. Authorization may be based on restrictions, for example time-of-day restrictions, or physical location restrictions, or restrictions against multiple logins by the same user. Authorization determines the nature of the service which is granted to a user. Examples of types of service include, but are not limited to: IP address filtering, address assignment, route assignment, QoS/differential services, bandwidth control/traffic management, compulsory tunneling to a specific endpoint, and encryption.

Accounting. Accounting refers to the tracking of the consumption of network resources by users. This information may be used for management, planning, billing, or other purposes. Real-time accounting refers to accounting information that is delivered concurrently with the consumption of the resources. Batch accounting refers to accounting information that is saved until it is delivered at a later time. Typical information that is gathered in accounting is the identity of the user, the nature of the service delivered, when the service began, and when it ended.

http://en.wikipedia.org/wiki/AAA_protocol

2.3.4 (FR) AAA

Acronyme d'«authentication, authorization, and accounting» (authentification, autorisation et traçabilité). Protocole permettant d'authentifier un utilisateur en fonction de son identité vérifiable, d'autoriser un utilisateur en fonction de ses droits d'utilisateur et de vérifier la consommation des ressources réseau d'un utilisateur.

http://fr.pcisecuritystandards.org/

2.4 ACCESO

Ver:

- *Gestión de derechos de acceso*
- *Control de acceso*
- *Acceso por red*

2.4.1 ACCESO

Utilización de los recursos de un sistema de información.

2.4.1 (EN) ACCESS

Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions. [CNSSI_4009:2010]

2.4.2 (EN) ACCESS

(I) The ability and means to communicate with or otherwise interact with a system to use system resources either to handle information or to gain knowledge of the information the system contains. (Compare: handle.)

1b. (O) "Opportunity to make use of an information system (IS) resource." [C4009] [RFC4949:2007]

2.4.3 (EN) ACCESS

A specific type of interaction between a subject and an object that results in the flow of information from one to the other. [TCSEC:1985]

2.4.4 (FR) ACCÈS

Mot employé dans des expressions composées pour caractériser le moyen d'obtention des informations (par exemple mémoire à accès sélectif) ou des résultats consécutifs à un traitement (traitement en accès direct).

http://www.cases.public.lu/functions/glossaire/

2.5 ACCESO FIABLE

Ver:

- *Confianza*

2.5.1 VÍA FIABLE

Mecanismo de seguridad que permite a un usuario establecer una conexión segura con el sistema, evitando así cualquier intento de suplantación de éste. Además, este mecanismo es imposible de imitar o desactivar por un programa no fiable.

Para arrancar el mecanismo existe una secuencia de teclas (p.e., en Windows NT: Ctrol + Alt + Del) que al ser pulsada elimina todos los procesos actuales y comunica directamente con el sistema. [Ribagorda:1997]

2.5.2 (EN) TRUSTED PATH

A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software. [CNSSI_4009:2010]

2.5.3 (EN) TRUSTED PATH

1a. (I) /COMPUSEC/ A mechanism by which a computer system user can communicate directly and reliably with the TCB and that can only be activated by the user or the TCB and cannot be imitated by untrusted software within the computer. [NCS04]

1b. (I) /COMSEC/ A mechanism by which a person or process can communicate directly with a cryptographic module and that can only be activated by the person, process, or module, and cannot be imitated by untrusted software within the module. [FP140] [RFC4949:2007]

2.5.4 (EN) TRUSTED PATH

A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software. [NIST-SP800-53:2013]

2.5.5 (EN) TRUSTED PATH

a means by which a user and a TSF can communicate with necessary confidence.

TSF - TOE Security Functionality

TOE - Target of Evaluation

[CC:2006]

2.5.6 (EN) TRUSTED PATH

A mechanism by which a person at a terminal can communicate directly with the Trusted Computing Base. This mechanism can only be activated by the person or the Trusted Computing Base and cannot be imitated by untrusted software. [TCSEC:1985]

2.6 ACCESO POR RED

Ver:

- *Acceso*

2.6.1 ACCESO POR RED

Acceso a un sistema de información a través de una red (sea una red local, metropolitana, o Internet).

2.6.2 (EN) NETWORK ACCESS

Access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet). [NIST-SP800-53:2013]

2.7 ACEPTACIÓN DEL RIESGO

Ver:

- *Riesgo*

2.7.1 ACEPTACIÓN DEL RIESGO

Decisión informada en favor de tomar un riesgo en particular. [UNE-ISO GUÍA 73:2010]

NOTA 1 La aceptación del riesgo puede tener lugar sin que exista tratamiento del riesgo o durante el proceso de tratamiento del riesgo.

NOTA 2 Los riesgos aceptados son objeto de seguimiento y de revisión.

[UNE-ISO/IEC 27000:2014]

2.7.1 ACEPTACIÓN DEL RIESGO:

Decisión informada en favor de tomar un riesgo particular.[UNE Guía 73:2010]

2.7.2 ACEPTACIÓN DE RIESGOS

La decisión de aceptar unos riesgos. [UNE-71504:2008]

2.7.3 (EN) RISK ACCEPTANCE

informed decision to take a particular risk [ISO Guide 73:2009]

NOTE 1: Risk acceptance can occur without risk treatment or during the process of risk treatment.

NOTE 2: Accepted risks are subject to monitoring and review.

[ISO/IEC 27000:2014]

2.7.4 (EN) RISK ACCEPTANCE

informed decision to take a particular risk [ISO Guide 73:2009]

(en) RISK ACCEPTANCE:

explicit or implicit decision not to take an action that would affect all or part of a particular risk

Annotation: Risk acceptance is one of four risk management strategies, along with risk avoidance, risk control, and risk transfer.

DHS Risk Lexicon, September 2008

2.7.5 (EN) ACCEPTABLE RISK

A risk that is understood and tolerated by a system's user, operator, owner, or accreditor, usually because the cost or difficulty of implementing an effective countermeasure for the associated vulnerability exceeds the expectation of loss. (See: adequate security, risk, "second law" under "Courtney's laws".) [RFC4949:2007]

2.7.6 (FR) ACCEPTATION DU RISQUE

décision argumentée en faveur de la prise d'un risque particulier. [ISO Guide 73:2009]

2.7.7 (FR) VALIDATION DU TRAITEMENT DES RISQUES

Sous-processus de la gestion des risques visant à décider d'accepter la manière dont les risques ont été traités ainsi que les risques résiduels à l'issue du traitement des risques. [EBIOS:2010]

2.8 AC PUENTE

2.8.1 AC PUENTE

PKI reducida a una única autoridad de certificación que establece certificados cruzados con una serie de autoridades de certificación de diferentes PKI clientes, de forma que quedan todas indirectamente certificadas entre ellas.

2.8.2 (EN) BRIDGE CA

(I) A PKI consisting of only a CA that cross-certifies with CAs of some other PKIs. (See: cross-certification. Compare: bridge.) [RFC4949:2007]

2.9 ACREDITACIÓN

Ver:

- *Clave*

- *Evaluación*
- *Certificación*
- *Organismo de certificación*

2.9.1 ACREDITAR

Dar seguridad de que alguien o algo es lo que representa o parece.

DRAE. Diccionario de la Lengua Española.

2.9.2 ACREDITADO

Autorizado oficialmente para un Rol. Por ejemplo, una organización acreditada podría estar autorizada para impartir cursos o para dirigir una Auditoría. [ITIL:2007]

2.9.3 ACREDITACIÓN

Autorización otorgada por la autoridad responsable de la acreditación, para manejar información nacional clasificada hasta un grado determinado, o en unas determinadas condiciones de integridad o disponibilidad, con arreglo a su concepto de operación.

2.9.4 AUTORIDAD DE ACREDITACIÓN (AA)

Autoridad responsable de conceder autorización a un Sistema para manejar información clasificada hasta un grado determinado, o en unas determinadas condiciones de integridad o disponibilidad, con arreglo a su concepto de operación.

2.9.5 ACREDITACIÓN

1. Acción de facultar a un sistema o red de información para que procese datos sensibles, determinando el grado en el que el diseño y la materialización de dicho sistema cumple los requerimientos de seguridad técnica preestablecidos.

2. Proceso de reconocer la competencia técnica y la imparcialidad de un organismo encargado de efectuar evaluaciones. [CCN-STIC-101:2005] [CESID:1997]

2.9.6 ACREDITACIÓN

1. Proceso de reconocimiento de la competencia técnica e imparcialidad de un laboratorio de evaluación para realizar las tareas que las corresponden (ITSEC).

2. Proceso de aceptación de un sistema o producto para su uso en un entorno particular con amenazas específicas. [Ribagorda:1997]

2.9.7 (EN) ACCREDITATION

Official approval given by an organization stating that sb/sth has achieved a required standard.

Oxford Advanced Learner's Dictionary.

2.9.8 (EN) ACCREDITATION

Formal declaration by a Designated Accrediting Authority (DAA) or Principal Accrediting Authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. See authorization. [CNSSI_4009:2010]

2.9.9 (EN) ACCREDITATION

in the context of this document: formal declaration by a designated approving authority that a system is approved to operate in a particular security mode using a prescribed set of safeguards.

NOTE. This definition is generally accepted within the security community; within ISO the more generally used definition is: Procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks [ISO/IEC Guide 2].

[ISO-21827:2007]

2.9.10 (EN) ACCREDITATION

(N) An administrative action by which a designated authority declares that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards. [FP102, SP37]

(See: certification.) [RFC4949:2007]

2.9.11 (EN) ACCREDITED

Officially authorised to carry out a Role. For example an Accredited body may be authorised to provide training or to conduct Audits. [ITIL:2007]

2.9.12 (EN) ACCREDITATION

The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. [NIST-SP800-53:2013] [FIPS-200:2006] [NIST-SP800-37:2004]

2.9.13 (EN) WHAT IS SECURITY ACCREDITATION?

Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. By accrediting an information system, an agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs. Thus, responsibility and accountability are core principles that characterize security accreditation. [NIST-SP800-100:2006]

2.9.14 (EN) ACCREDITATION

has two definitions according to circumstances:

- the procedure for accepting an IT system for use within a particular environment;
- the procedure for recognising both the technical competence and the impartiality of a test laboratory to carry out its associated tasks.

[ITSEC:1991]

2.9.15 (EN) APPROVAL / ACCREDITATION

The official authorisation that is granted to an Automatic Data Processing (ADP) system to process sensitive information in its operational environment, based upon comprehensive security evaluation of the system's hardware, firmware, and software security design, configuration, and implementation and of the other system procedural, administrative, physical, TEMPEST, personnel, and communications security controls. [TCSEC:1985]

2.9.16 (EN) ACCREDITATION

The written formal management decision to approve and authorize an organization to operate a classified information system (IS) to process, store, transfer, or provide access to classified information.

http://www.hr.lanl.gov/scourses/9369/76.htm

2.9.17 (FR) ACCRÉDITÉ

Officiellement autorisé à prendre en charge un Rôle. Par exemple, une personne accréditée ou un organisme accrédité peut être autorisée à fournir une formation ou à procéder à des Audits. [ITIL:2007]

2.10 ACTIVO

Ver:

- *Valor*

2.10.1 ACTIVO.

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [ENS:2010]

2.10.2 ACTIVO

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE-71504:2008]

2.10.3 ACTIVO

(Estrategia del Servicio) Cualquier Recurso o Capacidad. Los Activos de un Proveedor de Servicio incluyen todo aquello que se pueda atribuir a la entrega del Servicio. Los Activos pueden ser de los siguientes tipos: Administrativos, Organizativos, de Proceso, de Conocimiento, Personas, Información, Aplicaciones, Infraestructura, y de Capital. [ITIL:2007]

2.10.4 ACTIVOS

Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su Dirección. [Magerit:2012]

2.10.5 BIEN

Cualquier recurso que tenga valor para el organismo y que sea necesario para la realización de sus objetivos. Destacamos especialmente los elementos esenciales y las entidades que es conveniente proteger. [EBIOS:2005]

2.10.6 ACTIVO

Cualquier cosa que tiene un valor. [Ribagorda:1997]

2.10.7 (EN) ASSET

either tangible or intangible value that is worth protecting, including people, information, infrastructure finances and reputation infrastructure, finances and reputation

ISACA, Cybersecurity Glossary, 2014

2.10.8 (EN) ASSET

anything that has value to an individual, an organization or a government. [ISO-27032:2012]

2.10.9 (EN) ASSET

A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems. [CNSSI_4009:2010]

2.10.10 (EN) ASSET

Something of either tangible or intangible value worth protecting, including people, information, infrastructure, finances and reputation. [RiskIT-PG:2009]

2.10.11 (EN) ASSET

person, structure, facility, information, material, or process that has value

Extended Definition: includes: contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources, personnel, intelligence, technology, or physical infrastructure, or anything useful that contributes to the success of something, such as an organizational mission; assets are things of value or properties to which value can be assigned; from an intelligence standpoint, includes any resource – person, group, relationship, instrument,

installation, or supply – at the disposal of an intelligence organization for use in an operational or support role

Annotation: In some domains, capabilities and activities may be considered assets as well. In the context of the National Infrastructure Protection Plan, people are not considered assets.

DHS Risk Lexicon, September 2008

2.10.12 (EN) ASSET

(I) A system resource that is (a) required to be protected by an information system's security policy, (b) intended to be protected by a countermeasure, or (c) required for a system's mission. [RFC4949:2007]

2.10.13 (EN) ASSET

(Service Strategy) Any Resource or Capability. Assets of a Service Provider include anything that could contribute to the delivery of a Service. Assets can be one of the following types: Management, Organisation, Process, Knowledge, People, Information, Applications, Infrastructure, and Financial Capital. [ITIL:2007]

2.10.14 (EN) ASSETS

entities that the owner of the TOE presumably places value upon.

TOE - Target of Evaluation

[CC:2006]

2.10.15 (EN) ASSET

Any resource of value to the organisation and necessary for achieving its objectives. There is an important distinction between essential elements and entities needing to be protected. [EBIOS:2005]

2.10.16 (EN) ASSET

A component or part of the total system. Assets may be of four types: physical, application software, data, or end user services. [CRAMM:2003]

2.10.17 (EN) ASSET

Something of value to the enterprise. [Octave:2003]

2.10.18 (EN) ASSET

Any information resource with value that is worth protecting or preserving. [TDIR:2003]

2.10.19 (EN) ASSET

information or resources to be protected by the technical and non-technical countermeasures of a TOE. [ITSEM:1993]

2.10.20 (EN) ASSET

A physical item, informational item, or capability required by an organization to maintain productivity. Examples include a computer system, a customer database, and an assembly line.

http://www.symantec.com/avcenter/refa.html

2.10.21 (EN) CYBER ASSET:

A digitally connected asset; that is. an asset that is connected to a routable network or a Host. The term Cyber Asset is used within the NERC reliability standards. which defines a Cyber Asset as any Asset connected to a mutable network within a control system; any Asset connected to a routable network outside of the control system; and/or any Asset reachable via dial-up. [knapp:2014]

2.10.22 (EN) CRITICAL CYBER ASSET:

A critical cyber asset is a cyber asset that is itself responsible for per- forming a critical function, or directly impacts an asset that performs a critical function. The term “critical cyber asset" is used heavily within NERC reliability standards for Critical Infrastructure Protection. [knapp:2014]

2.10.23 (EN) CRITICAL DIGITAL ASSET:

A “critical digital asset" is a digitally connected asset that is itself responsible for performing a critical function, or directly impacts an asset that performs a critical function. The term "critical digital asset" is used heavily within NRC regulations and guidance documents. Also see: Critical Cyber Asset. [knapp:2014]

2.10.24 (EN) CYBER ASSETS

Programmable electronic devices, including the hardware, software, and data in those devices. [NERC:2014]

2.10.25 (FR) ACTIF

(Stratégie de Services) Toute ressource ou capacité. Les actifs d'un fournisseur de service regroupent tout ce qui peut contribuer à la fourniture d'un service. Les actifs peuvent appartenir à une des catégories suivantes: Gestion, Organisation, Processus, Compétences, Personnel, Informations, Applications, Infrastructure, et Capital financier. [ITIL:2007]

2.10.26 (FR) BIEN

tout élément représentant de la valeur pour l'organisme.

2.10.27 (FR) BIEN

Toute ressource qui a de la valeur pour l'organisme et qui est nécessaire à la réalisation de ses objectifs. On distingue notamment les éléments essentiels et les entités qu'il convient de protéger. [EBIOS:2005]

2.11 ACTUACIÓN RESPONSABLE

2.11.1 RESPONSABLE

Dicho de una persona: Que pone cuidado y atención en lo que hace o decide.

DRAE. Diccionario de la Lengua Española.

2.11.2 (EN) DUE DILIGENCE

the care that a reasonable person exercises under the circumstances to avoid harm to other persons or their property. [Merriam-Webster's]

2.11.3 (EN) DUE DILIGENCE

Due diligence is the requirement that organizations must develop and deploy a protection plan to prevent fraud, abuse, and additional deploy a means to detect them if they occur.

2.12 ACUERDO DE NIVEL DE SERVICIO (ANS)

Acrónimos: SLA, ANS (es), CES (fr)

2.12.1 SLA

Siglas de Service Level Agreement. Claúsulas en un contrato de outsourcing en el que se especifican las características mínimas de un servicio que deben cumplirse.

http://www.inteco.es/glossary/Formacion/Glosario/

2.12.2 (EN) SERVICE LEVEL AGREEMENT

Defines the specific responsibilities of the service provider and sets the customer expectations. [CNSSI_4009:2010]

2.12.3 ACUERDO DE NIVEL DE SERVICIO (SLA)

(Diseño del Servicio) (Mejora Continua del Servicio) Acuerdo entre un Proveedor de Servicio de TI y un Cliente. El SLA describe el Servicio de TI, documenta los Objetivos de Nivel de Servicio y especifica las responsabilidades del Proveedor de Servicio de TI y del Cliente. Un único SLA puede curbir varios Servicios de TI o varios Clientes. Ver Acuerdo de Nivel Operacional. [ITIL:2007]

2.12.4 SLA - ACUERDO DE NIVEL DE SERVICIO

Acuerdo por escrito entre un proveedor de servicios y los usuarios del cliente, el cual documenta los niveles de servicio acordados para un servicio prestado. [COBIT:2006]

2.12.5 (EN) SERVICE LEVEL AGREEMENT (SLA)

An agreement, preferably documented, between a service provider and the customer(s)/user(s) that defines minimum performance targets for a service and how they will be measured

ISACA, Cybersecurity Glossary, 2014

2.12.6 (EN) SERVICE LEVEL AGREEMENT (SLA)

(Service Design) (Continual Service Improvement) An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers. See Operational Level Agreement. [ITIL:2007]

2.12.7 (EN) SERVICE LEVEL AGREEMENT (SLA)

Written agreement between a service provider and the customer(s)/user(s) that documents agreed service levels for a service. [COBIT:2006]

2.12.8 (EN) SERVICE-LEVEL AGREEMENT

A service-level agreement (SLA) is a contract between a network service provider and a customer that specifies, usually in measurable terms, what services the network service provider will furnish. Many Internet service providers (ISP)s provide their customers with an SLA. More recently, IS departments in major enterprises have adopted the idea of writing a service level agreement so that services for their customers (users in other departments within the enterprise) can be measured, justified, and perhaps compared with those of outsourcing network providers. Some metrics that SLAs may specify include:

- What percentage of the time services will be available
- The number of users that can be served simultaneously
- Specific performance benchmarks to which actual performance will be periodically compared
- The schedule for notification in advance of network changes that may affect users
- Help desk response time for various classes of problems
- Dial-in access availability
- Usage statistics that will be provided.

http://searchsoftwarequality.techtarget.com/glossary/

2.12.9 (FR) ACCORD SUR LES NIVEAUX DE SERVICE (SLA)

(Conception de services) (Amélioration continuelle du service) Un accord entre un fournisseur de service des TI et un client. Le SLA décrit le service des TI, documente les cibles de niveau de service et spécifie les responsabilités du fournisseur de service des TI et du client. Un seul SLA peut couvrir plusieurs services des TI ou plusieurs clients. Voir Accord sur les niveaux opérationnels (OLA). [ITIL:2007]

2.12.10 (FR) CONTRAT D´ENGAGEMENT DE SERVICE (CES)

Systèmes de mesure de la qualité de service. Le fournisseur du service informatique s´engage, par contrat, sur une disponibilité de l´outil vis-à-vis des utilisateurs.

2.13 ACUERDO DE RESPALDO MUTUO

2.13.1 ACUERDO DE RESPALDO MUTUO

Convenio entre dos instituciones por el cual se comprometen, bajo ciertas condiciones de uso, a facilitarse mutuamente sus equipos y sistemas de tratamiento de la información caso de que un accidente inutilice o degrade los de una de ellas. [Ribagorda:1997]

2.13.2 (EN) MUTUAL BACKUP AGREEMENT

Agreement between organisations, or departments within an organisation, to backup each other in case of disaster. That is, the information system of one of them will [temporally] take charge of the needs of the other.

2.14 ACUERDO DE SEGURIDAD EN INTERCONEXIONES

Acrónimos: ISA

2.14.1 ACUERDO DE SEGURIDAD EN INTERCONEXIONES

Acuerdo entre organizaciones que van a interconectar sus sistemas de información.

2.14.1 ACUERDO DE SEGURIDAD DE INTERCONEXIÓN

Documento que regula los aspectos relevantes para la seguridad de una conexión prevista entre una organización y un sistema externo. Regula la interfaz de seguridad entre dos sistemas que operan bajo dos autoridades diferentes. Incluye una variedad de información descriptiva, aspectos técnicos, de procedimiento, y la planificación. Por lo general, viene después de un acuerdo formal que define las funciones y responsabilidades de alto nivel en la gestión de una conexión entre dominios.

2.14.1 (EN) INTERCONNECTION SECURITY AGREEMENT (ISA)

A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high-level roles and responsibilities in management of a cross-domain connection. [CNSSI_4009:2010]

2.14.2 (EN) WHAT IS AN ISA?

An Interconnection Security Agreement (ISA) is an agreement established between the organizations that own and operate connected information systems to document the technical requirements of the interconnection. The ISA is a security document that specifies the requirements for connecting the information systems, describes the security controls that will be used to protect the systems and data, and contains a topographical drawing of the interconnection. It is a commitment between the owners of two systems to abide by specific rules of behavior. These rules are discretionary and should be based on risk. [NIST-SP800-100:2006]

2.15 ACUMULACIÓN DE PRIVILEGIOS

Ver:

- *Escalada de privilegios*

2.15.1 ACUMULACIÓN DE PRIVILEGIOS

Proceso gradual por el que un sujeto va incrementando sus derechos de acceso por encima de los que estrictamente requiere para desempeñar su trabajo.

2.15.2 (EN) PRIVILEGE CREEP

Privilege creep is the gradual accumulation of access rights beyond what an individual needs to do his job.

http://searchsecurity.techtarget.com/

2.16 ADMINISTRADOR

Ver:

- *Administrador de seguridad*
- *Operador*

2.16.1 ADMINISTRADOR

Persona responsable de la instalación y configuración de los componentes de un sistema de información.

2.16.2 (EN) ADMINISTRATOR

1. (O) /Common Criteria/ A person that is responsible for configuring, maintaining, and administering the TOE in a correct manner for maximum security. (See: administrative security.) [RFC4949:2007]

2.16.3 (EN) ADMINISTRATOR

an entity that has complete trust with respect to all policies implemented by the TSF.

TSF - TOE Security Functionality

TOE - Target of Evaluation

[CC:2006]

2.16.4 (EN) ADMINISTRATOR

a person in contact with the Target of Evaluation who is responsible for maintaining its operational capability. [ITSEC:1991]

2.16.5 (EN) ADMINISTRATOR

A user with sufficient access rights to allow them to manage the access rights of other users and carry out other high-level computer management tasks.

http://www.getsafeonline.org/

2.16.6 (EN) ADMINISTRATOR

An individual who:

- Oversees the operation of a network.
- Is responsible for installing programs on a network and configuring them for distribution to workstations.
- May also update security settings on workstations.

http://www.symantec.com/avcenter/refa.html

2.16.7 (EN) SECURITY ADMINISTRATOR

The person charged with monitoring and implementing security controls and procedures for a system. Whereas each university will have one Information Security Officer, technical management may designate a number of security administrators.

http://www.utexas.edu/its/policies/glossary.html

2.17 ADMINISTRADOR DE SEGURIDAD

Ver:

- *Administrador*

2.17.1 ADMINISTRADOR DE SEGURIDAD

Persona que es responsable de la definición o aplicación de una o más partes de una política de seguridad. [X.810:1995]

2.17.2 (EN) SECURITY ADMINISTRATOR

A person who is responsible for the definition or enforcement of one or more parts of a security policy. [X.810:1995]

2.17.3 (FR) ADMINISTRATEUR DE SÉCURITÉ

personne qui est responsable de la définition ou de l'application d'une ou de plusieurs parties de la politique de sécurité. [X.810:1995]

2.18 ADWARE

2.18.1 SOFTWARE PUBLICITARIO

Aplicaciones que durante su funcionamiento despliegan publicidad en ventanas emergentes o barras de herramientas a cambio de la gratuidad en su utilización. La publicidad normalmente permite visitar la página web del anunciante, por lo que requiere conexión a Internet para funcionar. Se diferencian de los programas gratuitos (freeware) en que incorporan publicidad. La mayoría de los programas publicitarios son confiables, pero en ocasiones algunos de ellos son utilizados con fines poco éticos llegando a comportarse como auténticos programas espías. Sirviendo a las empresas patrocinadoras de los mismos para controlar movimientos de los usuarios.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.18.2 ADWARE

Tipo de software malicioso cuya instalación hace que la computadora muestre o descargue publicidad de manera automática.

http://es.pcisecuritystandards.org

2.18.3 ADWARE

Tipo de software que ofrece publicidad mientras está funcionando. Aunque se asocia al malware, no tiene que serlo forzosamente, ya que suele ser un medio legitimo usado por desarrolladores de sofware que lo implementan en sus programas, generalmente en las versiones shareware, haciéndolo desaparecer en el momento en que adquirimos la versión completa del programa.

Se convierte en malware en el momento en que empieza a recopilar información sobre el ordenador donde se encuentra instalado.

http://www.inteco.es/glossary/Formacion/Glosario/

2.18.4 (EN) ADWARE

A program, often installed without the knowledge of a user through such actions as visiting websites or downloading software, which pushes and displays paid advertising.

http://www.enisa.europa.eu/

2.18.5 (EN) ADWARE

Type of malicious software that, when installed, forces a computer to automatically display or download advertisements.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.18.6 (EN) ADWARE

Like spyware, adware is software that may track visited websites and act as a key logger. Adware tracks this information to automatically display downloaded or installed adverts to a user.

PC Security Handbook, Rich Robinson

2.18.7 (EN) ADWARE

A form of spyware that displays unwanted adverts on a computer.

http://www.getsafeonline.org/

2.18.8 (EN) ADWARE

Programs that facilitate delivery of advertising content to the user through their own window, or by utilizing another program's interface. In some cases, these programs may gather information from the user's computer, including information related to Internet browser usage or other computing habits, and relay this information back to a remote computer or other location in cyber-space.

Adware can be downloaded from Web sites (typically in shareware or freeware), email messages, and instant messengers. Additionally, a user may unknowingly receive and/or trigger adware by accepting an End User License Agreement from a software program linked to the adware or from visiting a website that downloads the adware with or without an End User License Agreement.

http://www.symantec.com/avcenter/refa.html

2.18.9 (FR) ADWARE

Encore appelé publiciel, ce type de logiciel malveillant, une fois installé, force un ordinateur à afficher ou télécharger des publicités de façon automatique.

http://fr.pcisecuritystandards.org/

2.18.10 (FR) ADWARE

Un adware est un logiciel doté de code et de fonctions additionnelles dans le but de délivrer des messages publicitaires aux utilisateurs (souvent sous la forme de pop-up ou de bannières publicitaires) via leur ordinateur. En théorie, l'adware ne transmet aucune information personnelle, mais dans la pratique, la frontière entre spyware et adware est difficile à cerner.

Le terme adware provient du mot anglais advertisment qui signifie publicité et de software.

http://www.cases.public.lu/functions/glossaire/

2.18.11 (FR) ADWARE

Logiciel dont l'auteur se rémunère par l'affichage de bannières publicitaires, sans pour autant recueillir de données personnelles sur ses utilisateurs.

http://www.secuser.com/glossaire/

2.19 AES - ADVANCED ENCRYPTION STANDARD

Acrónimos: AES

Ver:

- *Cifrado en bloque*
- *Criptografía de clave secreta*
- http://csrc.nist.gov/encryption/aes/
- http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

- *DES - Data Encryption Standard*
- [ISO-18033-3:2005]

2.19.1 AES - ADVANCED ENCRYPTION STANDARD

Algoritmo de cifra basado en un secreto compartido (clave). Cifra el texto en bloques de 128 bits. Utiliza claves de 128, 192 o 256 bits.

2.19.2 (EN) ADVANCED ENCRYPTION STANDARD (AES)

A U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. [CNSSI_4009:2010]

2.19.3 (EN) ADVANCED ENCRYPTION STANDARD (AES)

(N) A U.S. Government standard [FP197] (the successor to DES) that (a) specifies "the AES algorithm", which is a symmetric block cipher that is based on Rijndael and uses key sizes of 128, 192, or 256 bits to operate on a 128-bit block, and (b) states policy for using that algorithm to protect unclassified, sensitive data. [RFC4949:2007]

2.19.4 (EN) AES

a symmetric encryption mechanism providing variable key length and allowing an efficient implementation specified as Federal Information Processing Standard.[ISO-18028-4:2005]

2.19.5 (EN) AES

A NIST-standard cryptographic cipher that uses a block length of 128 bits and key lengths of 128, 192 or 256 bits. Officially replacing the Triple DES method in 2001, AES uses the Rijndael algorithm developed by Joan Daemen and Vincent Rijmen of Belgium. AES can be encrypted in one pass instead of three, and its key size is greater than Triple DESs 168 bits. In early 1997, the NIST invited cryptographers to submit an advanced algorithm. In late 2000, the Rijndael (pronounced rine-doll) symmetric block cipher algorithm was selected out of submissions by 21 teams from 11 countries.

http://www.spectralogic.com/index.cfm?fuseaction=home.displayFile&DocID=1235

2.19.6 (FR) AES

Algorithme de chiffrement basé sur la cryptographie symétrique, AES est le remplaçant de DES. Face aux vulnérabilités du DES vis-à-vis des attaques par force brute, l'institut NIST a lancé en janvier 1997 un appel d'offre pour le remplacement du DES par un nouvel algorithme de chiffrement par blocs de 128 bits, supportant des clés de chiffrement de 128, 192 et 256 bits minimum. Parmi les 5 algorithmes retenus (MARS, RC6, Rijndael, Serpent, Twofish), l'algorithme belge Rijndael a été choisi.

http://securit.free.fr/glossaire.htm

2.20 AGENTE EXTERNO

Ver:

- *Perímetro de seguridad*
- *Personal interno*

2.20.1 AGENTE EXTERNO

Persona que accede al sistema desde el exterior del perímetro de seguridad.

2.20.2 (EN) OUTSIDER

(I) A user (usually a person) that accesses a system from a position that is outside the system's security perimeter. (Compare: authorized user, insider, unauthorized user.) [RFC4949:2007]

2.21 AGOTAMIENTO DE RECURSOS

Ver:

- *Denegación de servicio*

2.21.1 AGOTAMIENTO DE RECURSOS

Ataque consistente en pedirle tantos recursos a un sistema que este queda a todos los efectos incapacitado de servir a nadie más.

2.21.2 (EN) RESOURCE EXHAUSTION

Resource exhaustion attacks involve tying up finite resources on a system, making them unavailable to others.

http://www.sans.org/security-resources/glossary-of-terms/

2.22 AGREGACIÓN

Ver:

- *Información clasificada*
- *Clasificación*

2.22.1 AGREGACIÓN

Circunstancia en la que un conjunto de elementos de información es objeto de una clasificación más elevada que la de cualquiera de sus componentes vistos individualmente.

2.22.2 (EN) AGGREGATION

(I) A circumstance in which a collection of information items is required to be classified at a higher security level than any of the items is classified individually. (See: classification.) [RFC4949:2007]

2.23 AGREGACIÓN DE DATOS

Ver:

- *Datos*
- *Inteligencia*

2.23.1 AGREGACIÓN DE DATOS

Recopilación de datos no clasificados de tal forma que el conjunto, correlacionado, debiera estar clasificado por cuanto sería de utilidad para perpetrar un ataque.

2.23.2 (EN) DATA AGGREGATION

Compilation of individual data systems and data that could result in the totality of the information being classified, or classified at a higher level, or of beneficial use to an adversary. [CNSSI_4009:2010]

2.23.3 (EN) DATA AGGREGATION

Data Aggregation is the ability to get a more complete picture of the information by analyzing several different types of records at once.

http://www.sans.org/security-resources/glossary-of-terms/

2.24 AH - AUTHENTICATION HEADER

Acrónimos: AH

Ver:

- *IPsec - IP security*
- *ESP - Encapsulating Security Payload*

2.24.1 AH - AUTHENTICATION HEADER

Cabecera IP que proporciona el servicio de autenticación de un paquete IP que viaje por la red.

2.24.2 (EN) AUTHENTICATION HEADER (AH)

(I) An Internet protocol [R2402, R4302] designed to provide connectionless data integrity service and connectionless data origin authentication service for IP datagrams, and (optionally) to provide partial sequence integrity and protection against replay attacks. (See: IPsec. Compare: ESP.) [RFC4949:2007]

2.24.3 (EN) AH - AUTHENTICATION HEADER

The IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams (hereafter referred to as just "integrity") and to provide protection against replays.

http://www.ietf.org/rfc/rfc4302

2.25 AIR GAP

Ver:

- [sneakernet]]
- *Protección del perímetro*
- *Pasarela de seguridad*
- *Guardia*

2.25.1 AIR GAP

Término usado para describir que dos redes están absolutamente separadas.

2.25.2 (EN) AIR GAP

(I) An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control).

(See: sneaker net. Compare: gateway.)

[RFC4949:2007]

2.25.3 (EN) AIR GAP

A term used to describe the absolute separation of two networks.

2.25.4 (EN) AIR-GAPPED NETWORK

Air gapping is a security measure that isolates a secure network from unsecure networks physically, electrically and electromagnetically.

http://cyber.law.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas

2.26 ALARP – AS LOW AS REASONABLY PRACTICAL

Ver:

- http://www.hse.gov.uk/risk/theory/alarp.htm

2.26.1 ALARP – TAN BAJO COMO SEA RAZONABLEMENTE PRÁCTICO

Un método para correlacionar de la probabilidad de un riesgo y la gravedad de sus consecuencias para determinar si la exposición al riesgo es razonable o si hay que seguir reduciendo el riesgo.

2.26.2 (EN) ALARP – AS LOW AS REASONABLY PRACTICAL

A method of correlating the likelihood of a hazard and the severity of its consequences to determine risk exposure acceptability or the need for further risk reduction.

2.27 ALEATORIO

Ver:

- *Generador de números aleatorios*
- *Generador de números seudo-aleatorio*

2.27.1 ALEATORIO

Término que indica que el resultado de un experimento sólo depende del azar, no teniendo relación con los resultados anteriores o posteriores. El fenómeno o experimento no es reproducible. (v. Pseudoaleatorio). [CESID:1997]

2.27.2 SEUDOALEATORIO

Sucesión de datos generados por un algoritmo pero que pasan las pruebas habituales de aleatoriedad.

Los números aleatorios son necesarios en gran número de técnicas y protocolos criptográficos, como generación de claves criptográficas, sistemas de autenticación fuerte, etc. [Ribagorda:1997]

2.27.3 PSEUDOALEATORIO

Término que indica que un suceso, aún no siendo estrictamente aleatorio, se puede considerar aleatorio debido a que satisface unas determinadas condiciones y test. El suceso puede repetirse si se producen idénticas condiciones iniciales a las que lo originaron. [CESID:1997]

2.27.4 (EN) RANDOM NUMBER

time variant parameter whose value is unpredictable. [ISO-9798-1:1997]

2.28 ALERTA

2.28.1 ALERTA

(Operación del Servicio) Advertencia de que se ha superado un umbral, de que algo ha cambiado, o de que hubo un Fallo. De forma regular, las Alertas se crean y gestionan con herramientas de Gestión de Sistemas y administradas por el Proceso de Gestión de Eventos. [ITIL:2007]

2.28.2 ALERTA

Notificación de que el sistema de información es objeto de un ataque.

2.28.1 (EN) ALERT

NotifNotification that a specific attack has been directed at an organization’s information systems. [CNSSI_4009:2010]

2.28.2 (EN) ALERT

(Service Operation) A warning that a threshold has been reached, something has changed, or a Failure has occurred. Alerts are often created and managed by System Management tools and are managed by the Event Management Process. [ITIL:2007]

2.28.3 (EN) ALERT

A notification of an important observed event. [NIST-SP800-94:2007]

2.28.4 (EN) ALERT

an "instant" indication that an information system and network may be under attack, or in danger because of accident, failure or people error. [ISO-18028-1:2006]

2.28.5 (FR) ALERTE

(Exploitation de Services) Avertissement qu'un seuil a été atteint, que quelque chose a changé, ou qu'une panne s'est produite. Les avertissements sont souvent créés et gérés par les outils de Gestion du Système et sont gérés par le Processus de Gestion des Événements. [ITIL:2007]

2.29 ALGORITMO

Ver:

- *Algoritmo criptográfico*

2.29.1 ALGORITMO

Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema.

DRAE. Diccionario de la Lengua Española.

2.29.2 (EN) ALGORITHM

A set of rules that must be followed when solving a particular problem.

Oxford Advanced Learner's Dictionary.

2.29.3 (EN) ALGORITHM

clearly specified mathematical process for computation a set of rules that, if followed, will give a prescribed result. [ISO-18031:2005]

2.29.4 (FR) ALGORITHME

Suite finie d'opérations ou de calculs mathématiques. L'algorithme est la base constitutive de tout programme informatique. Il définit le comportement du programme suite à des événements interagissant avec lui (saisies clavier, mouvements de la souris, etc.).

http://www.cases.public.lu/functions/glossaire/

2.30 ALGORITMO CRIPTOGRÁFICO

Ver:

- *Algoritmo*
- *Algoritmo público*
- *Algoritmo secreto*

- *Algoritmo de cifra*
- *Algoritmo irreversible*

2.30.1 ALGORITMO CRIPTOGRÁFICO

Función matemática que lleva a cabo un cierto cálculo criptográfico.

2.30.2 (EN) CRYPTOGRAPHIC ALGORITHM

A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output. [CNSSI_4009:2010]

2.30.3 (EN) CRYPTOGRAPHIC ALGORITHM

(I) An algorithm that uses the science of cryptography, including (a) encryption algorithms, (b) cryptographic hash algorithms, (c) digital signature algorithms, and (d) key-agreement algorithms. [RFC4949:2007]

2.30.4 (EN) CRYPTOGRAPHIC ALGORITHM

A well-defined computational procedure that takes variable inputs including a cryptographic key and produces an output. [NIST-SP800-57:2007]

2.30.5 (EN) CRYPTOGRAPHIC ALGORITHM

Mathematical function that computes a result from one or several input values. [H.235:2005]

2.31 ALGORITMO CRIPTOGRÁFICO ASIMÉTRICO

Ver:

- *Algoritmo de cifra*

2.31.1 ALGORITMO CRIPTOGRÁFICO ASIMÉTRICO

Algoritmo para ejecutar el cifrado o el descifrado correspondiente, cuyas claves para el cifrado y el descifrado son diferentes.

NOTA. Con algunos algoritmos criptográficos asimétricos, el descifrado del texto cifrado o la generación de una firma digital requiere la utilización de más de una clave privada.

[X.810:1995]

2.31.2 (EN) PUBLIC KEY (ASYMMETRIC) CRYPTOGRAPHIC ALGORITHM

a cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible. [NIST-SP800-57:2007] [FIPS-140-2:2001]

2.31.3 (EN) ASYMMETRIC CRYPTOGRAPHIC ALGORITHM

An algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ.

NOTE. With some asymmetric cryptographic algorithms, decipherment of ciphertext or the generation of a digital signature requires the use of more than one private key.

[X.810:1995]

2.31.4 (FR) ALGORITHME ASYMÉTRIQUE DE CRYPTOGRAPHIE

algorithme pour réaliser le chiffrement ou le déchiffrement correspondant dans lequel les clés utilisées pour le chiffrement et le déchiffrement sont différentes.

NOTE. Avec certains algorithmes asymétriques de cryptographie, il faut utiliser plus d'une clé privée pour déchiffrer un cryptogramme ou pour générer une signature numérique.

[X.810:1995]

2.32 ALGORITMO CRIPTOGRÁFICO SIMÉTRICO

Ver:

- *Algoritmo de cifra*

2.32.1 ALGORITMO CRIPTOGRÁFICO SIMÉTRICO

Algoritmo para realizar el cifrado o el algoritmo correspondiente para realizar el descifrado en el cual se requiere la misma clave para el cifrado y el descifrado. [X.810:1995]

2.32.2 (EN) SYMMETRIC KEY ALGORITHM

A cryptographic algorithm that uses the same secret key for an operation and its complement (e.g., encryption and decryption). [NIST-SP800-57:2007]

2.32.3 (EN) SYMMETRIC (SECRET-KEY BASED) CRYPTOGRAPHIC ALGORITHM

An algorithm for performing encipherment or the corresponding algorithm for performing decipherment in which the same key is required for both encipherment and decipherment (X.810). [H.235:2005]

2.32.4 (EN) SYMMETRIC ENCIPHERMENT ALGORITHM

an encipherment algorithm that uses the same secret key for both the originators and the recipients transformation. [ISO-9798-1:1997]

2.32.5 (EN) SYMMETRIC CRYPTOGRAPHIC ALGORITHM

An algorithm for performing encipherment or the corresponding algorithm for performing decipherment in which the same key is required for both encipherment and decipherment. [X.810:1995]

2.32.6 (FR) ALGORITHME SYMÉTRIQUE DE CRYPTOGRAPHIE

algorithme pour réaliser le chiffrement ou algorithme pour réaliser le déchiffrement correspondant dans lequel la même clé est requise à la fois pour le chiffrement et le déchiffrement. [X.810:1995]

2.33 ALGORITMO DE CÁLCULO DE CÓDIGOS DE AUTENTICACIÓN DE MENSAJES

Ver:

- *Código de autenticación de mensajes*

2.33.1 (EN) MESSAGE AUTHENTICATION CODE (MAC) ALGORITHM

algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following two properties:

- for any key and any input string the function can be computed efficiently;
- for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the ith input string may have been chosen after observing the value of the first i - 1 function values.

NOTE 1. A MAC algorithm is sometimes called a cryptographic check function (see for example ISO-7498-2).

NOTE 2. Computational feasibility depends on the users specific security requirements and environment.

[ISO-9797-1:1999]

2.34 ALGORITMO DE CIFRA

Ver:

- *Cifrado*
- *Algoritmo criptográfico*
- *Algoritmo criptográfico asimétrico*
- *Algoritmo criptográfico simétrico*
- *Algoritmo de descifrado*

2.34.1 ALGORITMO DE CIFRA

Conjunto finito de operaciones matemáticas (en ocasiones simplemente reglas o pasos) que permiten obtener un texto cifrado a partir de un texto en claro y de ciertos parámetros iniciales, por ejemplo, la clave criptográfica y el vector de inicialización.

Es término sinónimo de "algoritmo de cifrado" y "algoritmo criptográfico".

[Ribagorda:1997]

2.34.2 ALGORITMO DE CIFRA

Conjunto de operaciones o secuencia de reglas o pasos utilizado para obtener, a partir de un texto claro y en función de una determinada clave, un texto cifrado, o viceversa. [CESID:1997]

2.34.3 ALGORITMO NACIONAL DE CIFRA

Medio o procedimiento de cifra, material o no material, cuya realización, propiedad y garantía de seguridad pertenece al Estado Español.

El órgano con que cuenta el Ministerio de Defensa para establecer esta garantía de seguridad es el Centro Superior de Información de la Defensa, según el Real Decreto 1883/1996 (BOE n° 156 de 8 de agosto de 1996). [CESID:1997]

2.34.4 ALGORITMO PERSONALIZABLE

Ver Algoritmo privatizable. [CESID:1997]

2.34.5 ALGORITMO PRIVATIZABLE O PERSONALIZABLE

Algoritmo de cifra en el que el usuario puede seleccionar determinados parámetros de su funcionamiento a fin de individualizarlo para su red. [CESID:1997]

2.34.6 (EN) ENCRYPTION ALGORITHM

Set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key. [CNSSI_4009:2010]

2.34.7 (EN) ENCRYPTION ALGORITHM

process which transforms plaintext into ciphertext. [ISO-18033-1:2005]

2.34.8 (FR) ALGORITHME DE CHIFFREMENT

Technique cryptographique utilisée pour assurer la confidentialité des données. L'algorithme de chiffrement est constitué de deux processus:

- Le cryptage ou chiffrement qui transforme des données en clair en données chiffrées
- Le décryptage ou déchiffrement qui transforme les données chiffrées en données en clair.

[ISO-18033-1:2005]

2.35 ALGORITMO DE DESCIFRADO

Ver:

- *Descifrado*
- *Algoritmo criptográfico*
- *Algoritmo de cifra*

2.35.1 ALGORITMO DE DESCIFRADO

Proceso que transforma textro cifrado en texto en claro.

2.35.2 (EN) DECRYPTION ALGORITHM

process which transforms ciphertext into plaintext. [ISO-18033-1:2005]

2.36 ALGORITMO DIFFIE-HELLMAN

Acrónimos: DH

Ver:

- *Criptografía de clave pública*
- *Negociación de claves*
- http://www.ietf.org/rfc/rfc2631

2.36.1 INTERCAMBIO EXPONENCIAL DIFFIE-HELLMAN

Primer algoritmo de clave pública, enunciado por W. Diffie y M. Hellman en 1976, que basa su seguridad en la dificultad de calcular logaritmos discretos en un campo finito. Se emplea para distribución de claves pero no para cifrar y descifrar. [CESID:1997]

2.36.2 (EN) DIFFIE-HELLMAN / DIFFIE-HELLMAN-MERKLE

(N) A key-agreement algorithm published in 1976 by Whitfield Diffie and Martin Hellman [DH76, R2631]. [RFC4949:2007]

2.36.3 (EN) DIFFIE-HELLMAN ALGORITHM

A key agreement algorithm published in 1976 by Whitfield Diffie and Martin Hellman.

Diffie -Hellman does key establishment, not encryption. However, the key that it produces may be used for encryption, for further key management operations, or for any other cryptography.

2.36.4 (EN) DIFFIE-HELLMAN

A key agreement algorithm published in 1976 by Whitfield Diffie and Martin Hellman. Diffie-Hellman does key establishment, not encryption. However, the key that it produces may be used for encryption, for further key management operations, or for any other cryptography.

http://www.sans.org/security-resources/glossary-of-terms/

2.37 ALGORITMO IRREVERSIBLE

Ver:

- *Función irreversible*
- *Algoritmo criptográfico*
- *Algoritmo reversible*

2.37.1 ALGORITMO IRREVERSIBLE

Véase: Función irreversible. [Ribagorda:1997]

2.37.2 ALGORITMO IRREVERSIBLE

Algoritmo que emplea o no clave y que se utiliza sólo en un sentido (p.e. algoritmos que proporcionan firma de claves, autenticación o integridad). (v. Algoritmo reversible). [CESID:1997]

2.38 ALGORITMO PÚBLICO

Ver:

- *Algoritmo criptográfico*
- *Algoritmo*
- *Algoritmo secreto*

2.38.1 ALGORITMO PÚBLICO

Algoritmo de cifra cuyo funcionamiento no se considera información a proteger y es de general conocimiento. [CESID:1997]

2.38.2 (EN) PUBLIC ALGORITHM

Cryptographic algorithm that is not secret; it is open to public inspection.

2.39 ALGORITMO REVERSIBLE

Ver:

- *Algoritmo*
- *Algoritmo criptográfico*

2.39.1 CIFRADO REVERSIBLE

Aquél basado en un algoritmo invertible en algún sentido. En ocasiones, caso del cifrado asimétrico, el algoritmo inverso se obtiene con el concurso de un parámetro, clave privada, distinto del empleado para el algoritmo directo, clave pública. En el cifrado simétrico, el mismo parámetro, denominado clave secreta, se emplea para el algoritmo directo y el inverso. [Ribagorda:1997]

2.39.2 ALGORITMO REVERSIBLE

Algoritmo de cifra que se utiliza para cifrar y descifrar. [CESID:1997]

2.39.3 (EN) REVERSIBLE ENCRYPTION

Reversible encryption refers to any form of encryption that also can be decrypted.

2.40 ALGORITMO SECRETO

Ver:

- *Algoritmo criptográfico*
- *Algoritmo*
- *Algoritmo público*

2.40.1 ALGORITMO SECRETO

Algoritmo de cifra cuyo funcionamiento interno es considerado por el fabricante o el usuario información a proteger. (v. Algoritmo público). [CESID:1997]

2.40.2 (EN) SECRET ALGORITHM

Cryptographic algorithm that is kept secret.

2.41 ALTA DISPONIBILIDAD

2.41.1 ALTA DISPONIBILIDAD

Configuración de los sistemas de forma que garantizan un servicio continuo incluso cuando alguno de sus componentes no se encuentra plenamente disponible.

2.41.2 ALTA DISPONIBILIDAD

(Diseño del Servicio) Una aproximación o Diseño que minimiza u oculta a los Usuarios de un Servicio de TI los efectos del Fallo de un Elemento de Configuración. Las soluciones de Alta disponibilidad se diseñan para alcanzar los niveles acordados de disponibilidad y para hacer uso de técnicas como la Tolerancia a Fallos, Resistencia y recuperación rápida para reducir el número de Incidentes y el Impacto de los mismos. [ITIL:2007]

2.41.3 (EN) HIGH AVAILABILITY

Configuration of clusters or redundant servers to provide continuous access to a network resource application, such as a VPN, firewall or Web server. The servers are continuously synchronized to provide automatic failover. High availability solutions enable redundant server to detect when the primary server is unavailable and transparently switch to a secondary server.

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.41.4 (EN) HIGH AVAILABILITY

(Service Design) An approach or Design that minimises or hides the effects of Configuration Item Failure on the Users of an IT Service. High Availability solutions are Designed to achieve an agreed level of Availability and make use of techniques such as Fault Tolerance, Resilience and fast Recovery to reduce the number of Incidents, and the Impact of Incidents. [ITIL:2007]

2.41.5 (FR) HAUTE DISPONIBILITÉ

(Conception de services) Une approche ou un concept tendant à réduire (minimiser ?) ou à cacher les effets d'une défaillance d'un élément de configuration sur les utilisateurs d'un service des TI.

Les solutions à haute disponibilité sont conçues pour répondre à un niveau convenu de disponibilité et mettent en oeuvre des techniques telles que la tolérance de panne, la résilience et la reprise rapide afin de réduire le nombre d'incidents, ainsi que leur impact. [ITIL:2007]

2.42 AMENAZA

Ver:

- *Amenaza activa*
- *Amenaza pasiva*
- *Exploit*
- *Daño*
- *Vulnerabilidad*

2.42.1 AMENAZA:

Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. [UNE-ISO/IEC 27000:2014]

2.42.2 AMENAZA

Condición o actividad capaz de ocasionar que, intencional o accidentalmente, la información o recursos para el procesamiento de la información se pierdan, modifiquen, queden expuestos o vuelvan inaccesibles; o que sean afectados de algún otro modo en detrimento de la organización.

http://es.pcisecuritystandards.org

2.42.3 AMENAZA

Cualquier cosa que pueda aprovechar un Vulnerabilidad. Cualquier causa potencial de un Incidente puede ser considerada una Amenaza. Por ejemplo un fuego es una Amenaza que puede aprovechar la Vulnerabilidad de moquetas inflamables. Este término es comúnmente usado en la Gestión de la Información de Seguridad y la Gestión de Continuidad del Servicio de TI, pero también aplica a otras áreas tales como Gestión de la Disponibilidad y Problemas. [ITIL:2007]

2.42.4 AMENAZA

Cualquier circunstancia o evento que puede explotar, intentionadamente o no, una vulnerabilidad específica en un Sistema de las TIC resultando en una pérdida de confidencialidad, integridad o disponibilidad de la información manejada o de la integridad o disponibilidad del propio Sistema.

2.42.5 AMENAZA

Posible ataque a los bienes por parte de un elemento peligroso. [EBIOS:2005]

2.42.6 MOTIVACIÓN

Motivo de un elemento peligroso. Puede tener un carácter estratégico, ideológico, terrorista, codicioso, lúdico o vengador y varía según se trate de un acto accidental (curiosidad, aburrimiento) o deliberado (espionaje, afán de lucro, intención de perjudicar, ideología, juego, fraude, robo, piratería, desafío intelectual, venganza, chantaje, extorsión monetaria). [EBIOS:2005]

2.42.7 ELEMENTO PELIGROSO

Acción humana, elemento natural o ambiental que tiene consecuencias potenciales negativas para el sistema. Puede caracterizarse por su tipo (natural, humano o ambiental) y por su causa (accidental o deliberada). Cuando se trata de una causa accidental, puede caracterizarse también en función de la exposición y los recursos disponibles. Cuando se trata de una causa deliberada, puede caracterizarse también en función de la pericia, los recursos disponibles y la motivación. [EBIOS:2005]

2.42.8 AMENAZAS

Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos. [Magerit:2012]

2.42.9 AMENAZA

Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE-71504:2008]

2.42.10 AMENAZA

1. Acción o acontecimiento que puede atentar contra la seguridad (ITSEC).

2. Violación potencial de la seguridad del sistema (ISO-7498-2).

[Ribagorda:1997]

2.42.11 AMENAZA

Condición del entorno del sistema de información que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad.

Puede ser:

- Activa: Supone un cambio del estado del sistema.
- Pasiva: No varía el estado del sistema.

[CESID:1997]

2.42.12 AMENAZA

Violación potencial de la seguridad. [ISO-7498-2:1989]

2.42.13 (EN) THREAT

potential cause of an unwanted incident, which may result in harm to a system or organisation. [ISO/IEC 27000:2014]

2.42.14 (EN) THREAT

Condition or activity that has the potential to cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the organization.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.42.1 (EN) THREAT

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [CNSSI_4009:2010]

2.42.2 (EN) THREAT

Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm. [RiskIT-PG:2009]

2.42.3 (EN) THREAT EVENT

Any event where a threat element/actor acts against an asset in a manner that has the potential to directly result in harm. [RiskIT-PG:2009]

2.42.4 (EN) THREAT

natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property

Annotation: Threat as defined refers to an individual, entity, action, or occurrence; however, for the purpose of calculating risk, the threat of an intentional hazard is generally estimated as the likelihood of an attack (that accounts for both the intent and capability of the adversary) being attempted by an adversary; for other hazards, threat is generally estimated as the likelihood that a hazard will manifest.

DHS Risk Lexicon, September 2008

2.42.5 (EN) THREAT

1a. (I) A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm. (See: dangling threat, INFOCON level, threat action, threat agent, threat consequence. Compare: attack, vulnerability.)

1b. (N) Any circumstance or event with the potential to adversely affect a system through unauthorized access, destruction, disclosure, or modification of data, or denial of service. [C4009] (See: sensitive information.)

Usage: (a) Frequently misused with the meaning of either "threat action" or "vulnerability". (b) In some contexts, "threat" is used more narrowly to refer only to intelligent threats; for example, see definition 2 below. (c) In some contexts, "threat" is used more broadly to cover both definition 1 and other concepts, such as in definition 3 below.

Tutorial: A threat is a possible danger that might exploit a vulnerability. Thus, a threat may be intentional or not:

- "Intentional threat": A possibility of an attack by an intelligent entity (e.g., an individual cracker or a criminal organization).
- "Accidental threat": A possibility of human error or omission, unintended equipment malfunction, or natural disaster (e.g., fire, flood, earthquake, windstorm, and other causes listed in [FP031]).

The Common Criteria characterizes a threat in terms of (a) a threat agent, (b) a presumed method of attack, (c) any vulnerabilities that are the foundation for the attack, and (d) the system resource that is attacked. That characterization agrees with the definitions in this Glossary (see: diagram under "attack").

2. (O) The technical and operational ability of a hostile entity to detect, exploit, or subvert a friendly system and the demonstrated, presumed, or inferred intent of that entity to conduct such activity.

Tutorial: To be likely to launch an attack, an adversary must have (a) a motive to attack, (b) a method or technical ability to make the attack, and (c) an opportunity to appropriately access the targeted system.

3. (D) "An indication of an impending undesirable event." [Park]

Deprecated Definition: IDOCs SHOULD NOT use this term with definition 3 because the definition is ambiguous; the definition was intended to include the following three meanings:

- "Potential threat": A possible security violation; i.e., the same as definition 1.
- "Active threat": An expression of intent to violate security. (Context usually distinguishes this meaning from the previous one.)
- "Accomplished threat" or "actualized threat": That is, a threat action.

Deprecated Usage: IDOCs SHOULD NOT use the term "threat" with this meaning; instead, use "threat action".

[RFC4949:2007]

2.42.6 (EN) THREAT ACTION

(I) A realization of a threat, i.e., an occurrence in which system security is assaulted as the result of either an accidental event or an intentional act. (See: attack, threat, threat consequence.)

Tutorial: A complete security architecture deals with both intentional acts (i.e., attacks) and accidental events [FP031]. (See: various kinds of threat actions defined under the four kinds of "threat consequence".)

[RFC4949:2007]

2.42.7 (EN) THREAT AGENT

(I) A system entity that performs a threat action, or an event that results in a threat action. [RFC4949:2007]

2.42.8 (EN) THREAT ANALYSIS

(I) An analysis of the threat actions that might affect a system, primarily emphasizing their probability of occurrence but also considering their resulting threat consequences. Example: RFC 3833. (Compare: risk analysis.) [RFC4949:2007]

2.42.9 (EN) THREAT

capabilities, intentions and attack methods of adversaries, or any circumstance or event, whether originating externally or internally, that has the potential to cause harm to information or a program or system or cause those to harm others. [ISO-21827:2007]

2.42.10 (EN) THREAT AGENT

the originator and/or the initiator of deliberate or accidental man-m ade threats. [ISO-21827:2007]

2.42.11 (EN) THREAT

Anything that might exploit a Vulnerability. Any potential cause of an Incident can be considered to be a Threat. For example a fire is a Threat that could exploit the Vulnerability of flammable floor coverings. This term is commonly used in Information Security Management and IT Service Continuity Management, but also applies to other areas such as Problem and Availability Management. [ITIL:2007]

2.42.12 (EN) THREAT

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. [FIPS-200:2006]

2.42.13 (EN) THREAT

Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [NIST-SP800-53:2013]

2.42.14 (EN) MOTIVATION

Motive of a threat agent. It may arise from strategy, ideology, terrorism, greed, amusement or revenge and may be an accidental action (arising from curiosity, boredom, etc.) or a deliberate action (arising from spying, the lure of gain, the intention to harm, ideology, amusement, fraud, theft, piracy, intellectual challenge, revenge, blackmailing, extortion of money, etc.) [EBIOS:2005]

2.42.15 (EN) THREAT

The potential source of an adverse event. [NIST-SP800-61:2004]

2.42.16 (EN) THREAT

Any circumstance or event with the potential to intentionally or unintentionally exploit a specific vulnerability in an information system resulting in a loss of confidentiality, integrity, or availability. [NIST-SP800-60V2:2004]

2.42.17 (EN) THREAT

An activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity. [TDIR:2003]

2.42.18 (EN) THREAT

The potential for a threat source (defined below) to exploit (intentional) or trigger (accidental) a specific vulnerability. [NIST-SP800-33:2001]

2.42.19 (EN) THREAT

Any circumstance or event that could harm a critical asset through unauthorized access, compromise of data integrity, denial or disruption of service, or physical destruction or impairment. [CIAO:2000]

2.42.20 (EN) THREAT

an action or event that might prejudice security. [ITSEC:1991]

2.42.21 (EN) THREAT

A potential violation of security. [ISO-7498-2:1989]

2.42.22 (EN) THREAT

An actor or agent who exploits security vulnerabilities and risks.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/risk/248-BSI.html

2.42.23 (EN) THREAT

A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, data modification, and/or Denial of Service (DoS).

http://www.symantec.com/avcenter/refa.html

2.42.24 (EN) THREAT

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

http://www.sans.org/security-resources/glossary-of-terms/

2.42.25 (EN) THREAT ANALYSIS

The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment. [NIST-SP800-33:2001]

2.42.26 (EN) THREAT ASSESSMENT

process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations and/or property

DHS Risk Lexicon, September 2008

2.42.27 (EN) THREAT ASSESSMENT

A threat assessment is the identification of types of threats that an organization might be exposed to.

http://www.sans.org/security-resources/glossary-of-terms/

(en) threat source

The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability. [CNSSI_4009:2010]

2.42.28 (EN) THREAT SOURCE

The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent. [FIPS-200:2006]

2.42.29 (EN) THREAT AGENT

Human action, natural or environmental element that has potentially negative consequences on the system. It can be characterised by its type (natural, human or environmental) and by its cause (accidental or deliberate). In the case of an accidental cause, it is also characterised by exposure and available resources. In the case of a deliberate cause, it is also characterised by expertise, available resources and motivation. [EBIOS:2005]

2.42.30 (EN) THREAT SOURCE

Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) the situation and method that may accidentally trigger a vulnerability. [NIST-SP800-33:2001]

2.42.31 (EN) THREAT MODEL

A threat model is used to describe a given threat and the harm it could to do a system if it has a vulnerability.

http://www.sans.org/security-resources/glossary-of-terms/

2.42.32 (EN) THREAT VECTOR

The method a threat uses to get to the target.

http://www.sans.org/security-resources/glossary-of-terms/

2.42.33 (EN) THREAT

A threat is an actor or an agent that is a source of danger to the system under consideration or the assets to which it has access. The threat can be a person that abuses the software, a program running on a compromised system, or even a non-sentient event such as a hardware failure. A threat exploits a vulnerability in software to attack it.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/attack/590-BSI.html

2.42.34 (EN) THREAT

An event or act, deliberate or accidental, that could cause injury to people, information, assets or services.

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

2.42.35 (EN) MENACE

Situation ouactivité susceptible d'entraîner la perte, la modification, l'exposition ou l'indisponibilité intentionnelle ou accidentelle d'informations ou de ressources de traitement des informations, ou de les affecter au détriment de l'organisation.

http://fr.pcisecuritystandards.org/

2.42.36 (FR) MENACE

Tout ce qui peut exploiter la vulnérabilité. Toute cause potentielle d'incident peut être considérée comme une menace. Par exemple, un incendie est une menace pouvant exploiter la vulnérabilité des revêtements de sol inflammables. Ce terme est communément utilisé par la Gestion de la Sécurité de l'Information (ISM) et la Gestion de la continuité du service des TI (ITSCM), mais s'applique aussi à d'autres domaines tels que la gestion des problèmes et la gestion de la disponibilité. [ITIL:2007]

2.42.37 (FR) MENACE

Attaque possible d'un élément menaçant sur des biens. [EBIOS:2005]

2.42.38 (FR) MOTIVATION

Motif d'un élément menaçant. Elle peut avoir un caractère stratégique, idéologique, terroriste, cupide, ludique ou vengeur et diffère selon qu'il s'agit d'un acte accidentel (curiosité, ennui...) ou délibéré (espionnage, appât du gain, volonté de nuire, idéologie, jeu, fraude, vol, piratage, défi intellectuel, vengeance, chantage, extorsion de fonds...). [EBIOS:2005]

2.42.39 (FR) ÉLÉMENT MENAÇANT

Action humaine, élément naturel ou environnemental qui a des conséquences potentielles négatives sur le système. Elle peut être caractérisée par son type (naturel, humain, ou environnemental) et par sa cause (accidentelle ou délibérée). Dans le cas d'une cause accidentelle, elle est aussi caractérisée par une exposition et des ressources disponibles. Dans le cas d'une cause délibérée, elle est aussi caractérisée par une expertise, des ressources disponibles et une motivation. [EBIOS:2005]

2.42.40 (FR) MENACE

Violation potentielle de la sécurité. [ISO-7498-2:1989]

2.42.41 (FR) SOURCE DE MENACE

Chose ou personne à l'origine de menaces. Elle peut être caractérisée par son type (humain ou environnemental), par sa cause (accidentelle ou délibérée) et selon le cas par ses ressources disponibles, son expertise, sa motivation... [EBIOS:2010]

2.42.42 (FR) MENACE

Événement ou acte délibéré ou accidentel qui pourrait porter préjudice aux personnes, à l'information, aux biens ou aux services.

http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578

2.43 AMENAZA ACTIVA

Ver:

- *Amenaza*

2.43.1 AMENAZA ACTIVA

Amenaza de un cambio no autorizado y deliberado del estado de un sistema (ISO-7498-2).

Las amenazas activas suponen, de materializarse, la intrusión y posterior interacción con un sistema de información. Ejemplos de amenazas activas son la interrupción, modificación o fabricación de recursos. [Ribagorda:1997]

2.43.2 AMENAZA ACTIVA

Amenaza de un cambio deliberado y no autorizado del estado del sistema.

NOTA. Como ejemplos de amenazas activas relativas a la seguridad cabe citar: la modificación de mensajes, la reproducción de mensajes, la inserción de mensajes espurios, la usurpación de identidad (o impostura) de una entidad autorizada y la negación (o denegación) de servicio.

[ISO-7498-2:1989]

2.43.3 (EN) ACTIVE THREAT

The threat of a deliberate unauthorized change to the state of the system.

NOTE. Examples of security-relevant active threats may be: modification of messages, replay of messages, insertion of spurious messages, masquerading as an authorized entity and denial of service.

[ISO-7498-2:1989]

2.43.4 (FR) MENACE ACTIVE

Menace de modification non autorisée et délibérée de l'état du système.

Remarque. La modification et la répétition de messages, l'insertion de faux messages, le déguisement d'une entité autorisée et le déni de service sont des exemples de menaces actives.

[ISO-7498-2:1989]

2.44 AMENAZA EXTERNA

Ver:

- *Amenaza*

2.44.1 AMENAZA EXTERNA

Entidad no autorizada fuera del dominio de seguridad que tiene el potencial de dañar un sistema de información a través de la destrucción, divulgación, modificación de datos y / o denegación de servicio.

2.44.2 (EN) OUTSIDE(R) THREAT

An unauthorized entity outside the security domain that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service. [CNSSI_4009:2010]

2.45 AMENAZA INTERNA

Ver:

- *Amenaza*

2.45.1 AMENAZA INTERNA

Entidad con acceso autorizado (es decir, en el dominio de seguridad) que tiene el potencial de dañar un sistema de información o de la empresa a través de la destrucción, divulgación, modificación de datos y / o denegación de servicio.

2.45.2 (EN) INSIDE(R) THREAT

An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service. [CNSSI_4009:2010]

2.45.1 (EN) INTERNAL THREAT

A threat that originates within an organization.

http://www.symantec.com/avcenter/refa.html

2.46 AMENAZA PASIVA

Ver:

- *Amenaza*

2.46.1 AMENAZA PASIVA

1. de revelación no autorizada de información sin cambiar el estado del sistema (ISO-7498-2)

2. Amenaza a la confidencialidad de la información que, de materializarse, no cambia el esta del sistema. Por ejemplo, la interceptación de un canal de transmisión de datos.

Estas amenazas, de materializarse, son más difíciles de detectar que las activas y la recuperación del daño frecuentemente imposible.

[Ribagorda:1997]

2.46.2 AMENAZA PASIVA

Amenaza de revelación no autorizada de la información sin modificar el estado del sistema. [ISO-7498-2:1989]

2.46.3 (EN) PASSIVE THREAT

The threat of unauthorized disclosure of information without changing the state of the system. [ISO-7498-2:1989]

2.46.4 (FR) MENACE PASSIVE

Menace d'une divulgation non autorisée des informations, sans que l'état du système ne soit modifié. [ISO-7498-2:1989]

2.47 AMENAZAS AVANZADAS PERSISTENTES (APT)

Acrónimos: APT

Ver:

- *Amenaza*

2.47.1 AMENAZAS AVANZADAS PERSISTENTES (APT)

La definición ampliamente aceptada de amenaza persistente avanzada es que se trata de un ataque selectivo de ciberespionaje o cibersabotaje llevado a cabo bajo el auspicio o la dirección de un país, por razones que van más allá de las meramente financieras/delictivas o de protesta política. No todos los ataques de este tipo son muy avanzados y sofisticados, del mismo modo que no todos los ataques selectivos complejos y bien estructurados son una amenaza persistente avanzada. La motivación del adversario, y no tanto el nivel de sofisticación o el impacto, es el principal diferenciador de un ataque APT de otro llevado a cabo por ciberdelincuentes o hacktivistas.

McAfee. Predicciones de amenazas para 2011.

2.47.2 (EN) ADVANCED PERSISTENT THREAT (APT)

An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives using multiple attack vectors (NIST SP800-61)

Scope Note: The APT:

1. pursues its objectives repeatedly over an extended period of time
2. adapts to defenders' efforts to resist it
3. is determined to maintain the level of interaction needed to execute its objectives

ISACA, Cybersecurity Glossary, 2014

2.47.3 (EN) ADVANCED PERSISTENT THREAT

The Advanced Persistent Threat (APT) refers to a class of cyber threat designed to infiltrate a network, remain persistent through evasion and propagation techniques. APTs are typically used to establish and maintain an external command and control channel through which the attacker can continuously exfiltrate data. [knapp:2014]

2.47.4 (EN) ADVANCED PERSISTENT THREAT (APT)

An advanced persistent threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. APT attacks target organizations in sectors with high-value information, such as national defense, manufacturing and the financial industry.

In a simple attack, the intruder tries to get in and out as quickly as possible in order to avoid detection by the network's intrusion detection system (IDS). In an APT attack, however, the goal is not to get in and out but to achieve ongoing access. To maintain access without discovery, the intruder must continuously rewrite code and employ sophisticated evasion techniques. Some APTs are so complex that they require a full time administrator.

http://searchsecurity.techtarget.com/

2.47.5 (EN) ADVANCED PERSISTENT THREATS (APT)

Advanced Persistent Threats (APT) are computer attacks usually driven by government agencies or terrorist organizations conducting espionage or trying to take valuable data for non financial purposes. Rarely are APTs led by political or commercial organizations. However, in some cases, marginal threats do arise from obsessed individuals and legitimate commercial organizations since the value of data goes well beyond just the financial value. Incidents like Project Aurora and Wikileaks highlights that data also has both political and military value.

http://www.imperva.com/resources/glossary/glossary.html

2.47.6 (EN) ADVANCED PERSISTENT THREAT (APT)

usually refers to a group, such as a foreign government, with both the capability and the intent to persistently and effectively target a specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage, but applies equally to other threats such as that of traditional espionage or attack. Other recognised attack vectors include infected media, supply chain compromise, and social engineering. Individuals, such as an individual hacker, are not usually referred to as an APT as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target.

http://en.wikipedia.org/wiki/Advanced_persistent_threat

2.47.7 (EN) APT: ADVANCED PERSISTENT THREAT.

An Internet-borne attack usually perpetrated by a group of individuals with significant resources, such as organized crime or a rogue nation-statesuch as organized crime or a rogue nation-state.

Cybersecurity for Dummies, Palo Alto Networks Edition, 2014

2.48 AMPLIACIÓN

Ver:

- *Criterios comunes*

2.48.1 AMPLIACIÓN

La adición de uno o más requisitos a un paquete. [CC:2006]

2.48.2 (EN) AUGMENTATION

the addition of one or more requirement(s) to a package. [CC:2006]

2.49 ANÁLISIS DE FALLOS

Acrónimo: SFA

Ver:

- *Ataque por canal colateral*

2.49.1 ANÁLISIS DE FALLOS

Análisis de la respuesta de un dispositivo criptográficos antes diferentes fallos provocados, con el objeto de inferir información acerca de las claves usadas.

2.49.2 (EN) SECURITY FAULT ANALYSIS (SFA)

An assessment usually performed on information system hardware, to determine the security properties of a device when hardware fault is encountered. [CNSSI_4009:2010]

2.49.3 (EN) SECURITY FAULT ANALYSIS

(I) A security analysis, usually performed on hardware at the level of gate logic, gate-by-gate, to determine the security properties of a device when a hardware fault is encountered. [RFC4949:2007]

2.49.4 (EN) FAULT ANALYSIS

Attempting to induce faults, monitor the results and infer information on the secret data.

2.49.5 (EN) FAULT ANALYSIS

Attempting to induce faults, monitor the results and infer information on the secret data.

http://www.discretix.com/glossary.shtml

2.50 ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA)

Acrónimos: BIA

Ver:

- *Continuidad*

2.50.1 ANÁLISIS DE IMPACTO DEL NEGOCIO (BIA)

(Estrategia del Servicio) BIA es la Actividad de la Gestión de la Continuidad del Negocio que identifica las Funciones Vitales del Negocio y sus dependencias. Estas dependencias pueden incluir Proveedores, personas, otros Procesos de Negocio, Servicios TI, etc.

BIA define los requerimientos de recuperación para los Servicios TI. Dichos requerimientos incluyen Objetivos de Tiempos de Recuperación, Objetivos del Punto de Recuperación y los Objetivos de Nivel de Servicio mínimos para cada Servicio TI.

[ITIL:2007]

2.50.2 ANÁLISIS DE IMPACTO

Estudio de las consecuencias que tendría una parada de X tiempo sobre la Organización. [Magerit:2012]

2.50.3 ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA)

Estudio y evaluación de las pérdidas producidas por un ataque real o simulado. [Ribagorda:1997]

2.50.4 (EN) BUSINESS IMPACT ANALYSIS (BIA)

An analysis of an enterprise's requirements, processes, and interdependencies used to characterize information system contingency requirements and priorities in the event of a significant disruption. [CNSSI_4009:2010]

2.50.5 (EN) BUSINESS IMPACT ANALYSIS (BIA)

(Service Strategy) BIA is the Activity in Business Continuity Management that identifies Vital Business Functions and their dependencies. These dependencies may include Suppliers, people, other Business Processes, IT Services etc.

BIA defines the recovery requirements for IT Services. These requirements include Recovery Time Objectives, Recovery Point Objectives and minimum Service Level Targets for each IT Service.

[ITIL:2007]

2.50.6 (EN) BUSINESS IMPACT ANALYSIS

process of analysing business functions and the effect that a business disruption might have upon them. [BS25999-1:2006]

2.50.7 (EN) WHAT IS A BUSINESS IMPACT ANALYSIS (BIA)?

The BIA is a critical step to understanding the information systems components, interdependencies, and potential downtime impacts. The contingency plan strategy and procedures should be designed specifically around the results of the BIA. A BIA is conducted by identifying the systems

critical resources. Each critical resource is then further examined to determine how long functionality of the resource could be withheld from the information system before an unacceptable impact is experienced. [NIST-SP800-100:2006]

2.50.8 (EN) BUSINESS IMPACT ANALYSIS (BIA)

An activity performed by a sponsor to determine if a re-evaluation of a changed Target of Evaluation is necessary. [ITSEM:1993]

2.50.9 (EN) BUSINESS IMPACT ANALYSIS (BIA)

The process of identifying the potential impact of uncontrolled, non-specific events on an institution's business processes.

http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-b-glossary.aspx

2.50.10 (EN) BUSINESS IMPACT ANALYSIS (BIA)

A Business Impact Analysis determines what levels of impact to a system are tolerable.

http://www.sans.org/security-resources/glossary-of-terms/

2.50.11 (FR) ANALYSE D'IMPACT SUR LE BUSINESS (BIA)

(Stratégie de Services) La BIA est l'activité de la gestion de la continuité du business qui identifie les fonctions business vitales et leurs dépendances. Ces dépendances peuvent inclure des sous-traitants, des gens, d'autres processus business, des services informatiques, etc.

La BIA définit les besoins de la reprise des services des TI. Ces besoins incluent les objectifs de temps de reprise, les objectifs de point de reprise et les cibles de niveau de service minimum pour chacun des services informatiques.

[ITIL:2007]

2.51 ANÁLISIS DE PAQUETES TCP

2.51.1 ANÁLISIS DE PAQUETES TCP

Técnica útil para detectar qué sistema operativo se usa en un cierto equipo remoto. Consiste en analizar los paquetes TCP que envía buscando características signulares peculiares de un cierto sistema.

2.51.2 (EN) PASSIVE FINGERPRINTING

Analyzing packet headers for certain unusual characteristics or combinations of characteristics that are exhibited by particular operating systems or applications. [NIST-SP800-94:2007]

2.51.3 (EN) TCP FINGERPRINTING

TCP fingerprinting is the user of odd packet header combinations to determine a remote operating system.

http://www.sans.org/security-resources/glossary-of-terms/

2.52 ANÁLISIS DE RIESGOS

Ver:

- *Riesgo*

2.52.1 ANÁLISIS DEL RIESGO

Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo. [UNE-ISO GUÍA 73:2010]

NOTA 1 El análisis del riesgo proporciona las bases para la evaluación del riesgo y para tomar las decisiones relativas al tratamiento del riesgo.

NOTA 2 El análisis del riesgo incluye la estimación del riesgo.

[UNE-ISO/IEC 27000:2014]

2.52.2 ANÁLISIS DE RIESGOS.

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos. [ENS:2010]

2.52.3 ANÁLISIS DEL RIESGO

Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo. [UNE Guía 73:2010]

2.52.4 ANÁLISIS DE RIESGOS

Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. [Magerit:2012]

2.52.5 ANÁLISIS DE RIESGOS

Estudio de los bienes, sus vulnerabilidades y las probabilidades de materialización de amenazas, con el propósito de determinar la exposición anual al riesgo de cada bien ante cada amenaza.

Puede ser cuantitativo, cuando esta exposición se expresa en unidades monetarias, o cualitativo, cuando se expresa en una escala relativa de gravedad, por ejemplo del 1 al 10. Dada la dificultad que entraña el cálculo preciso de las probabilidades citadas, se suele elegir esta último.

[Ribagorda:1997]

2.52.6 (EN) RISK ANALYSIS

process to comprehend the nature of risk and to determine the level of risk [ISO Guide 73:2009]

NOTE 1: Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

NOTE: Risk analysis includes risk estimation

[ISO/IEC 27000:2014]

2.52.7 (EN) RISK ANALYSIS

process to comprehend the nature of risk and to determine the level of risk. [ISO Guide 73:2009]

2.52.1 (EN) RISK ANALYSIS

Examination of information to identify the risk to an information system. [CNSSI_4009:2010]

2.52.2 (EN) RISK ANALYSIS

A process by which frequency and magnitude of IT risk scenarios are estimated. [RiskIT-PG:2009]

2.52.3 (EN) RISK ANALYSIS:

systematic examination of the components and characteristics of risk

Annotation: In practice, risk analysis is generally conducted to produce a risk assessment. Risk analysis can also involve aggregation of the results of risk assessments to produce a valuation of risks for the purpose of informing decisions. In addition, risk analysis can be done on proposed alternative risk management strategies to determine the likely impact of the strategies on the overall risk.

DHS Risk Lexicon, September 2008

2.52.4 (EN) RISK ANALYSIS

(I) An assessment process that systematically (a) identifies valuable system resources and threats to those resources, (b) quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence, and (c) (optionally) recommends how to allocate available resources to countermeasures so as to minimize total exposure. (See: risk management, business-case analysis. Compare: threat analysis.) [RFC4949:2007]

2.52.5 (EN) RISK ANALYSIS

An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence. [TDIR:2003]

2.52.6 (EN) RISK ANALYSIS

The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment. [NIST-SP800-33:2001]

2.52.7 (EN) RISK ANALYSIS

A documented assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI, and an estimation of the security measures sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level. Risk analysis involves determining what requires protection, what it should be protected from, and how to protect it.

http://www.hipaa.yale.edu/overview/glossary.html

2.52.8 (EN) RISK ANALYSIS

Risk analysis involves analyzing target software for vulnerabilities and characterizing their nature and potential impact. Microsoft calls this threat modeling. Risk analysis attempts to identify, prioritize, and plan appropriate mitigation for the risks facing a piece of software.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/attack/590-BSI.html

2.52.9 (FR) ANALYSE DU RISQUE

processus mis en oeuvre pour comprendre la nature d'un risque et pour déterminer le niveau de risque [ISO Guide 73:2009]

2.53 ANÁLISIS DE TIEMPOS

Ver:

- *Ataque por canal colateral*

2.53.1 ANÁLISIS DE TIEMPOS

Análisis del tiempo de procesamiento empleado por un dispositivo criptográfico para tratar diferentes entradas, con el objeto de inferir información acerca de las claves usadas.

2.53.2 (EN) TIMING ANALYSIS

Attempting to infer secret information by measuring processing time of different inputs.

http://www.discretix.com/glossary.shtml

2.54 ANÁLISIS DE TRÁFICO

Ver:

- *Confidencialidad del tráfico de datos*
- *Rellenado de tráfico*

2.54.1 ANÁLISIS DE TRÁFICO

Observación del tráfico de datos (presencia, ausencia, dirección, volumen y frecuencia) en un canal de transmisión para inferir información (ISO-7498-2). Cuando la dificultad de descifrar los datos transmitidos por un canal es grande, este tipo de ataque puede proporcionar interesantes conjeturas sobre los mismos. [Ribagorda:1997]

2.54.2 ANÁLISIS DEL TRÁFICO

Inferencia de información a partir de la observación de flujos de tráfico (presencia, ausencia, cantidad, sentido y frecuencia). [ISO-7498-2:1989]

(en) traffic analysis

Gaining knowledge of information by inference from observable characteristics of a data flow, even if the information is not directly available (e.g., when the data is encrypted). These characteristics include the identities and locations of the source(s) and destination(s) of the flow, and the flow's presence, amount, frequency, and duration of occurrence. [CNSSI_4009:2010]

2.54.3 (EN) TRAFFIC ANALYSIS

1. (I) Gaining knowledge of information by inference from observable characteristics of a data flow, even if the information is not directly available (e.g., when the data is encrypted).

These characteristics include the identities and locations of the source(s) and destination(s) of the flow, and the flow's presence, amount, frequency, and duration of occurrence. The object of the analysis might be information in SDUs, information in the PCI, or both. (See: inference, traffic-flow confidentiality, wiretapping. Compare: signal analysis.)

2. (O) "The inference of information from observation of traffic flows (presence, absence, amount, direction, and frequency)." [ISO-7498-2]

[RFC4949:2007]

2.54.4 (EN) TRAFFIC ANALYSIS

The inference of information from observation of traffic flows (presence, absence, amount, direction, and frequency). [NIST-SP800-33:2001]

2.54.5 (EN) TRAFFIC ANALYSIS

The inference of information from observation of traffic flows (presence, absence, amount, direction and frequency). [ISO-7498-2:1989]

2.54.6 (FR) ANALYSE DU TRAFIC

Déduction d'informations à partir de l'observation des flux de données (présence, absence, quantité, direction, fréquence). [ISO-7498-2:1989]

2.55 ANÁLISIS DE VULNERABILIDADES

Ver:

- *Vulnerabilidad*
- *Evaluación de vulnerabilidad*
- *Escáner de vulnerabilidades*

2.56 ANÁLISIS DIFERENCIAL DE CONSUMO

Ver:

- *Análisis simple de consumo*
- *Ataque por canal colateral*

2.56.1 ANÁLISIS DIFERENCIAL DE CONSUMO

Análisis del consumo de energía realizado por un módulo criptográfico con el objetivo de extraer información relacionada con las claves criptográficas con las que trabaja.

A diferencia del análisis simple, aquí se estudian estadísticamente las variaciones de las observaciones realizadas con diferentes datos de entrada.

2.56.2 (EN) DIFFERENTIAL POWER ANALYSIS (DPA)

an analysis of the variations of the electrical power consumption of a cryptographic module, for the purpose of extracting information correlated to cryptographic operation. [ISO-19790:2006]

2.56.3 (EN) DIFFERENTIAL POWER ANALYSIS

An analysis of the variations of the electrical power consumption of a cryptographic module, using advanced statistical methods and/or other techniques, for the purpose of extracting information correlated to cryptographic keys used in a cryptographic algorithm. [FIPS-140-2:2001]

2.57 ANÁLISIS FORENSE

2.57.1 HERRAMIENTAS FORENSES

También se denomina “ciencia forense informática”. Cuando se trata de la seguridad de la información, se refiere a la aplicación de herramientas de investigación y técnicas de análisis para recolectar evidencia a partir de recursos informáticos a fin de determinar la causa del riesgo de los datos.

http://es.pcisecuritystandards.org

2.57.2 ANÁLISIS FORENSE

El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperabilidad del sistema, el análisis se denomina análisis postmortem.

http://es.wikipedia.org/wiki/Auditor%C3%ADa_de_seguridad_de_sistemas_de_informaci%C3%B3n

2.57.3 (EN) COMPUTER FORENSICS

The application of the scientific method to digital media to establish factual information for judicial review.

Scope Note: This process often involves investigating computer systems to determine whether they are or have been used for illegal or unauthorized activities As a discipline it combines elements of la and have been used for illegal or unauthorized activities. As a discipline, it combines elements of law and computer science to collect and analyze data from information systems (e.g., personal computers, networks, wireless communication and digital storage devices) in a way that is admissible as evidence in a court of law.

ISACA, Cybersecurity Glossary, 2014

2.57.4 (EN) DIGITAL FORENSICS

The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings

ISACA, Cybersecurity Glossary, 2014

2.57.5 (EN) FORENSIC EXAMINATION

The process of collecting, assessing, classifying and documenting digital evidence to assist in the identification of an offender and the method of compromise

ISACA, Cybersecurity Glossary, 2014

2.57.6 (EN) FORENSICS

The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. [CNSSI_4009:2010]

2.57.7 (EN) COMPUTER FORENSICS

The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. [CNSSI_4009:2010]

2.57.8 (EN) FORENSIC COPY

An accurate bit-for-bit reproduction of the information contained on an electronic device or associated media, whose validity and integrity has been verified using an accepted algorithm. [CNSSI_4009:2010]

2.57.9 (EN) COMPUTER FORENSICS

The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. [NIST-SP800-61:2004]

2.57.10 (EN) FORENSICS

Also referred to as “computer forensics.” As it relates to information security, the application of investigative tools and analysis techniques to gather evidence from computer resources to determine the cause of data compromises.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.57.11 (EN) COMPUTER FORENSICS

Computer forensics is application of the scientific method to digital media in order to establish factual information for judicial review. This process often involves investigating computer systems to determine whether they are or have been used for illegal or unauthorized activities. Mostly, computer forensics experts investigate data storage devices, either fixed like hard disks or removable like compact disks and solid state devices. Computer forensics experts:

- Identify sources of documentary or other digital evidence.
- Preserve the evidence.
- Analyze the evidence. Present the findings.

Computer forensics is done in a fashion that adheres to the standards of evidence that are admissible in a court of law.

http://en.wikipedia.org/wiki/Computer_forensics

2.57.12 (EN) FORENSIC-ENABLED INTELLIGENCE

The intelligence resulting from the integration of scientifically examined materials and other information to establish full characterization, attribution, and the linkage of events, locations, items, signatures, nefarious intent, and persons of interest. Also called FEI. [JP2-0:2013]

2.57.13 (FR) INFORMATIQUE LÉGALE

Également dénommé «expertise judiciaire en informatique». S'appliquant à la sécurité des informations, les outils d'investigation et de techniquesd'analysepermettent de rassembler des preuves à partir des ressources informatiques afin de déterminer la cause de la compromission des données.

http://fr.pcisecuritystandards.org/

2.58 ANÁLISIS HEURÍSTICO

Ver:

- *Sistema de detección de intrusiones*

2.58.1 ANÁLISIS HEURÍSTICO

Se hace cuando, a fin de detectar la presencia de virus, se estudia el comportamiento de los programas. El comportamiento anómalo permite inferir la infección.

2.58.2 (EN) HEURISTIC ANALYSIS

Analysis of how a program behaves, rather than looking for a know virus signature in order it identity a virus.

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.59 ANÁLISIS SIMPLE DE CONSUMO

Ver:

- *Análisis diferencial de consumo*
- *Ataque por canal colateral*

2.59.1 ANÁLISIS SIMPLE DE CONSUMO

Análisis del consumo de energía realizado por un módulo criptográfico dispositivo criptográfico para tratar diferentes entradas, con el objeto de inferir información acerca de las claves usadas.

2.59.2 (EN) SIMPLE POWER ANALYSIS (SPA)

a direct (primarily visual) analysis of patterns of instruction execution (or execution of individual instructions), obtained through monitoring the variations in electrical power consumption of a cryptographic module, for the purpose of revealing the features and implementations of cryptographic algorithms and subsequently the values of cryptographic keys. [ISO-19790:2006]

2.59.3 (EN) SIMPLE POWER ANALYSIS

Attempting to infer information by visual inspection of instantaneous power consumption.

2.60 ANONIMATO

Ver:

- *Perfilado*
- *Anonymizer*
- *Anonymous remailer*

2.60.1 ANONIMATO

Carácter o condición de anónimo.

DRAE. Diccionario de la Lengua Española.

2.60.2 ANÓNIMO

1. Dicho de una obra o de un escrito: Que no lleva el nombre del autor.

2. Dicho de un autor: Cuyo nombre se desconoce.

DRAE. Diccionario de la Lengua Española.

2.60.3 (EN) ANONYMITY

the state of remaining unknown to most other people

Oxford Advanced Learner's Dictionary.

2.60.4 (EN) ANONYMITY

(I) The condition of an identity being unknown or concealed. (See: alias, anonymizer, anonymous credential, anonymous login, identity, onion routing, persona certificate. Compare: privacy.) [RFC4949:2007]

2.60.5 (EN) ANONYMITY

(also see Pseudonymity and Pseudonymous profiling)

A condition in which your true identity is not known. Your online service provider may allow you, as a subscriber, to participate in online activities anonymously (not known at all) or pseudonymously (taking on a different identity).

http://www.consumerprivacyguide.org/glossary/

2.61 ANONYMIZER

Ver:

- *Anonimato*
- *Anonymous remailer*

2.61.1 ANONYMIZER

Servicio, dispositivo o aplicación interpuestos que impiden a los servidores web ver la dirección IP de sus usuarios.

2.61.2 (EN) ANONYMIZER

(I) An internetwork service, usually provided via a proxy server, that provides anonymity and privacy for clients. That is, the service enables a client to access servers (a) without allowing anyone to gather information about which servers the client accesses and (b) without allowing the accessed servers to gather information about the client, such as its IP address. [RFC4949:2007]

2.61.3 (EN) ANONYMIZER (ALSO SEE ANONYMOUS REMAILER)

An anonymizer is essentially a shield between your computer and the Internet that relays Web traffic through an intermediary server. It hides personally identifying informationsuch as IP address, browser software used, surfing patterns, etc.from any Web site you visit, and prevents sites from adding any cookies or other files to your computer.

http://www.consumerprivacyguide.org/glossary/

2.61.4 (EN) ANONYMIZER

An intermediary service, device, or software which prevents Web sites from seeing a users Internet Protocol (IP) address.

http://iab.com/

2.61.5 (EN) ANONYMIZATION AND DE-IDENTIFICATION

Anonymization refers to irreversibly severing a data set from the identity of the data contributor in a study to prevent any future re-identification, even by the study organizers under any condition. De-identification is also a severing of a data set from the identity of the data contributor, but may include preserving identifying information which could only be re-linked by a trusted party in certain situations.

https://en.wikipedia.org/wiki/De-identification#Anonymization_and_de-identification

2.61.6 (EN) DE-IDENTIFICATION

De-identification is the process by which a collection of data is stripped of information which would allow the identification of the source of the data. Common uses of de-identification include human subject research for the sake of privacy for research participants. Common strategies for de-identifying datasets are deleting or masking personal identifiers, such as name and social security number, and suppressing or generalizing quasi-identifiers, such as date of birth and zip code.

The reverse process of defeating de-identification to identify individuals is known as re-identification.

https://en.wikipedia.org/wiki/De-identification#Anonymization_and_de-identification

2.61.7 (FR) ANONYMISEUR

Serveur relais, en général sur Internet, qui permet de naviguer tout en restant (relativement) anonyme. L'anonymiseur a pour rôle de modifier et de supprimer les traces au cours de la navigation rendant ainsi plus difficile l'identification de l'internaute sur le réseau.

http://www.cases.public.lu/functions/glossaire/

2.62 ANONYMOUS REMAILER

Ver:

- *Anonimato*
- *Anonymizer*

2.62.1 ANONYMOUS REMAILER

Servidor intermedio de mensajería electrónica cuya función es reenviar los mensajes recibidos habiendo eliminado previamente la identificación del remitente.

2.62.2 (EN) ANONYMOUS REMAILER (ALSO SEE ANONYMIZER)

An anonymous remailer is a special email server that acts as a middleman. It strips your outgoing email of all personally identifying information (except any information you might type in the body of the message), then forwards it to its destination, usually with the IP address of the remailer attached. Some remailers allow users to use their real name on the message.

http://www.consumerprivacyguide.org/glossary/

2.63 ANTI AUTOMATIZACIÓN

Ver:

- *Verificación visual*

2.63.1 ANTI AUTOMATIZACIÓN

Medida de seguridad de los servidores web que impiden el acceso automatizado. La técnica consiste en exigir al usuario que demuestre ser humano pasándole una prueba de difícil resolución por un robot.

2.63.2 (EN) ANTI-AUTOMATION

Security measure that prevents automated programs from exercising web site functionality by administering the Turing Test to a user, which only a human could pass.

http://www.webappsec.org/projects/glossary/

2.64 ANTI-SPAM

Ver:

- *Spam*

2.64.1 ANTI-SPAM

Contramedida cuyo objetivo es la contención de correo electrónico no solicitado (spam). [CCN-STIC-400:2006]

2.64.2 (EN) ANTI-SPAM

Measures to counter spam abuse.

2.65 ANTI-SPOOF

Ver:

- *Spoof*

2.65.1 ANTI-SPOOF

Medidas para prevenir el abuso de datos de identificación y autenticación, impidiendo que alguien se haga pasar por quien no es.

2.65.2 (EN) ANTI-SPOOF

Countermeasures taken to prevent the unauthorized use of legitimate Identification & Authentication (I&A) data, however it was obtained, to mimic a subject different from the attacker. [CNSSI_4009:2010]

2.66 ANTI-SPYWARE

Ver:

- *Spyware*

2.66.1 ANTI-SPYWARE

Contramedida cuyo objetivo es evitar la infección por código malicioso de tipo spyware. [CCN-STIC-400:2006]

2.66.2 (EN) ANTI-SPYWARE

Measures to counter spyware.

2.66.3 (FR) ANTISPYWARE

Utilitaire capable de rechercher et d'éliminer les espiogiciels. Il s'agit le plus souvent d'un scanner à la demande utilisant une analyse par signatures pour identifier les espiogiciels connus et les désinstaller. Un antispyware est utile pour s'assurer qu'aucun espiogiciel n'est présent sur un ordinateur, ou pour éliminer un espiogiciel récalcitrant lorsque l'utilisateur ne souhaite plus utiliser le

logiciel associé. Par contre, l'utilisation de certains antispywares qui permettent de bloquer ou de neutraliser un spyware tout en continuant à utiliser son logiciel associé est assimilable à du piratage, les contrats de licence faisant généralement du spyware une contrepartie obligatoire à l'utilisation gratuite du logiciel associé.

http://www.secuser.com/glossaire/

2.67 ANTI-VIRUS

2.67.1 ANTIVIRUS

Aplicación informática cuya finalidad es la detección, detención y eliminación de virus y demás códigos maliciosos.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.67.2 ANTIVIRUS

Programa o software capaz de detectar y eliminar los diferentes tipos de programas maliciosos (también conocidos como "malware"), incluidos virus, gusanos, troyanos o caballos troyanos, spyware, adware y rootkits, y de proteger su computadora contra estos.

http://es.pcisecuritystandards.org

2.67.3 (EN) ANTIVIRUS SOFTWARE

A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents. [NIST-SP800-94:2007] [NIST-SP800-83:2005]

2.67.4 (EN) ANTI-VIRUS

Program or software capable of detecting, removing, and protecting against various forms of malicious software (also called “malware”) including viruses, worms, Trojans or Trojan horses, spyware, adware, and rootkits.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.67.5 (EN) ANTI-VIRUS

A class od software that attempts to prevent, detect, and remove malware from computers.

2.67.6 (FR) ANTIVIRUS

Programme ou logiciel capable de détecter, de supprimer et d’assurer une protection contre diverses formes de codes ou de logiciels malveillants (également appelés «maliciels»), notamment les virus, vers, chevaux de Troie, spywares ou logiciels espions, adware ou publiciel et outils de dissimulation d’activité

http://fr.pcisecuritystandards.org/

2.67.7 (FR) ANTIVIRUS

Logiciel capable de rechercher, d'identifier et de supprimer les virus informatiques et autres codes malicieux.

http://www.cases.public.lu/functions/glossaire/

2.67.8 (FR) ANTIVIRUS

Utilitaire capable de rechercher et d'éliminer les virus informatiques et autres malwares. La détection se fait selon deux principes: une analyse par signatures qui permet de détecter avec d'excellents résultats les virus connus pour peu que les définitions de virus soient régulièrement mises à jour, ou une analyse heuristique qui permet de détecter avec des résultats variables les virus inconnus à partir de leur logique de programmation et le cas échéant de leur comportement à l'exécution. Les antivirus fonctionnent eux-même selon deux principes: un scanner qui permet à l'utilisateur de lancer une analyse d'un disque ou d'un fichier lorsqu'il le souhaite ("on demand"), ou un moniteur qui surveille le système en temps réel ("on access") et empêche l'utilisateur d'ouvrir un fichier infecté. La plupart des antivirus comportent un scanner et un moniteur, mais il existe des produits analysant seulement "à la demande" (ex.: antivirus en ligne) voire ne disposant que d'un moniteur (ex.: antivirus génériques).

http://www.secuser.com/glossaire/

2.68 AOSTIC

Acrónimos: AOSTIC (es)

2.69 APÉNDICE

Ver:

- *Firma digital*

2.69.1 APÉNDICE

Bits formados por la signatura y una cadena de texto opcional.

2.69.2 (EN) APPENDIX

String of bits formed by the signature and an optional text field. [ISO-14888-1:1998]

2.70 APLICACIÓN

2.70.1 APLICACIÓN

Programa informático que realiza una determinada función, directamente para el usuario sin requerir privilegios especiales.

2.70.2 (EN) APPLICATION

Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges. [CNSSI_4009:2010]

2.71 APRECIACIÓN DE LOS RIESGOS

Ver:

- *Riesgo*
- *Evaluación de riesgos*

2.71.1 APRECIACIÓN DEL RIESGO

proceso global que comprende la identificación del riesgo, el análisis del riesgo y la evaluación del riesgo. [UNE-ISO GUÍA 73:2010]

[UNE-ISO/IEC 27000:2014]

2.71.2 APRECIACIÓN DEL RIESGO

Proceso global que comprende la identificación del riesgo, el análisis del riesgo y la evaluación del riesgo [UNE Guía 73:2010]

2.71.3 ANÁLISIS DE RIESGOS / EVALUACIÓN DE RIESGOS

Proceso que identifica los recursos valiosos de un sistema y sus amenazas; cuantifica la exposición a pérdida (es decir, el potencial de pérdida) según frecuencias estimadas y costos derivados por siniestros; y, opcionalmente, recomienda el modo de asignar recursos como medidas preventivas que minimicen el índice total de exposición.

http://es.pcisecuritystandards.org

2.71.4 GRAVAMEN DE RIESGO

Los pasos iniciales de la Gestión de Riesgos. Al analizar el valor de los Activos del negocio, identificando Amenazas a esos Activos, y evaluando cuan Vulnerable cada Activo es a esas Amenazas. El Gravamen de Riesgo puede ser cuantitativo (basado en información numérica) o cualitativa. [ITIL:2007]

2.71.5 (EN) RISK ASSESSMENT

overall process of risk identification, risk analysis and risk evaluation [ISO Guide 73:2009]

[ISO/IEC 27000:2014]

2.71.6 (EN) RISK ASSESSMENT

overall process of risk identification, risk analysis and risk evaluation [ISO Guide 73:2009]

2.71.7 (EN) RISK ASSESSMENT

The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. [NIST-SP800-53:2013]

2.71.1 (EN) RISK ASSESSMENT

The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated, potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF).

NIST SP 800-53: The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system.

Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

[CNSSI_4009:2010]

2.71.2 (EN) RISK ASSESSMENT

product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making

Extended Definition: appraisal of the risks facing an entity, asset, system, network, geographic area or other grouping Annotation: A risk assessment can be the resulting product created through analysis of the component parts of risk.

DHS Risk Lexicon, September 2008

2.71.3 (EN) QUALITATIVE RISK ASSESSMENT METHODOLOGY

set of methods, principles, or rules for assessing risk based on non-numerical categories or levels

DHS Risk Lexicon, September 2008

2.71.4 (EN) QUANTITATIVE RISK ASSESSMENT METHODOLOGY

set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment

Annotation: While a semi-quantitative methodology also involves the use of numbers, only a purely quantitative methodology uses numbers in a way that allows for the consistent use of values outside the context of the assessment.

DHS Risk Lexicon, September 2008

2.71.5 (EN) SEMI-QUANTITATIVE RISK ASSESSMENT METHODOLOGY

Definition: set of methods, principles, or rules to assess risk that uses bins, scales, or representative numbers whose values and meanings are not maintained in other contexts

Example: By giving the "low risk, "medium risk," and "high risk" categories corresponding numerical values, the assessor used a semi-quantitative risk assessment methodology.

Annotation: While numbers may be used in a semi-quantitative methodology, the values are not applicable outside of the methodology, and numerical results from one methodology cannot be compared with those from other methodologies.

DHS Risk Lexicon, September 2008

2.71.6 (EN) RISK ASSESSMENT

The initial steps of Risk Management. Analysing the value of Assets to the business, identifying Threats to those Assets, and evaluating how Vulnerable each Asset is to those Threats. Risk Assessment can be quantitative (based on numerical data) or qualitative. [ITIL:2007]

2.71.7 (EN) RISK ASSESSMENT

A study of vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures. The process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations. [TDIR:2003]

2.71.8 (EN) RISK ANALYSIS / RISK ASSESSMENT:

Process that identifies valuable system resources and threats; quantifies loss exposures (that is, loss potential) based on estimated frequencies and costs of occurrence; and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.71.9 (EN) RISK ASSESSMENT

Process of evaluating the risks of information loss based on an analysis of threats to, and vulnerabilities of, a system, operation or activity.

http://www.ioss.gov/docs/definitions.html

2.71.10 RISK ANALYSIS

For the purpose of this handbook, risk analysis is defined as the probabilistic assessment of performance such that the probability of not meeting a particular performance commitment can be quantified.

NASA Risk Management Handbook, NASA/SP-2011-3422, Version 1.0, November 2011

2.71.11 (FR) APPRÉCIATION DU RISQUE

ensemble du processus d'identification des risques, d'analyse du risque et d'évaluation du risque [ISO Guide 73:2009]

2.71.12 (FR) ANALYSE / ÉVALUATION DES RISQUES

Processus identifiant systématiquement les ressources système précieuses et les menaces qui leur sont associées. Ce processus quantifie l'exposition aux pertes (pertes éventuelles) en fonction de

la fréquence et des coûts d'occurrence estimés, et (en option) recommande la manière d'affecter des ressources aux contre-mesures dans le but de réduire l'exposition totale.

http://fr.pcisecuritystandards.org/

2.72 ÁRBOLES DE ATAQUE

Ver:

- *Ataque*

2.72.1 ÁRBOL DE ATAQUE

Estructura de datos en forma de árbol donde a partir de un objetivo final (representado como la raíz) se identifican (como ramificaciones) objetivos secundarios que nos permitirían alcanzar el objetivo final. Los árboles de ataque se utilizan para modelar las posibles vías por las que puede perpetrarse un ataque.

2.72.2 (EN) ATTACK TREE

(I) A branching, hierarchical data structure that represents a set of potential approaches to achieving an event in which system security is penetrated or compromised in a specified way. [Moor]

Tutorial: Attack trees are special cases of fault trees. The security incident that is the goal of the attack is represented as the root node of the tree, and the ways that an attacker could reach that goal are iteratively and incrementally represented as branches and subnodes of the tree. Each subnode defines a subgoal, and each subgoal may have its own set of further subgoals, etc. The final nodes on the paths outward from the root, i.e., the leaf nodes, represent different ways to initiate an attack. Each node other than a leaf is either an AND-node or an OR-node. To achieve the goal represented by an AND-node, the subgoals represented by all of that node's subnodes must be achieved; and for an OR-node, at least one of the subgoals must be achieved. Branches can be labeled with values representing difficulty, cost, or other attack attributes, so that alternative attacks can be compared.

[RFC4949:2007]

2.72.3 (EN) ATTACK TREE

Attack trees (known as threat trees by Microsoft) provide a formal, methodical way of describing the security of systems based on various attacks [Schneier 99]. The root node of the tree is the attackers goal (known as threat by Microsoft), and the children of each node describe a lower-level way of achieving the goal of the parent node. In this manner, the leaf nodes generally contain relatively low-level tasks such as install a key logger on target machine, and the root node contains a goal such as obtain administrators password.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/attack/590-BSI.html

2.73 ÁRBOL DE LLAMADAS

Ver:

- *Emergencia*

2.73.1 ÁRBOL DE LLAMADAS

Relación de personas que deben ser contactadas en caso de declaración de emergencia.

2.73.2 (EN) CALL TREE

A documented list of employees and external entities that should be contacted in the event of an emergency declaration.

http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-b-glossary.aspx

2.74 ÁREA CONFIDENCIAL

2.74.1 ÁREA CONFIDENCIAL

Todo centro de datos, sala de servidores o cualquier área que aloje sistemas que almacenan, procesen o transmiten datos de titulares de tarjetas. No se incluyen las áreas en las que se encuentran presentes terminales de punto de venta, tales como el área de cajas en un comercio.

http://es.pcisecuritystandards.org/

2.74.2 (EN) SENSITIVE AREA:

Any data center, server room or any area that houses systems that stores, processes, or transmits cardholder data. This excludes the areas where only point-of-sale terminals are present such as the cashier areas in a retail store.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.74.3 (FR) ZONE SENSIBLE

Tout centre de données, salle de serveur ou zone abritant des systèmes qui stockent, traitent ou transmettent des données de titulaires de cartes. Ceci exclut les zones où ne sont installés que des terminaux de point de vente, comme les zones de caisse dans un magasin.

http://fr.pcisecuritystandards.org/

2.75 ÁREA DE ACCESO CONTROLADO

2.75.1 ÁREA DE ACCESO CONTROLADO

Área o espacio para los que la organización tiene la confianza de que las protecciones físicas y de procedimiento previstas son suficientes para cumplir los requisitos establecidos para la protección de la información y/o del sistema de información.

2.75.2 (EN) CONTROLLED AREA

Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. [NIST-SP800-53:2013]

2.75.3 (EN) CONTROLLED ACCESS AREA

Physical area (e.g., building, room, etc.) to which only authorized personnel are granted unrestricted access. All other personnel are either escorted by authorized personnel or are under continuous surveillance. [CNSSI_4009:2010]

2.75.4 (EN) CONTROLLED AREA

Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. [CNSSI_4009:2010]

2.76 ARQUITECTURA DE SEGURIDAD

Ver:

- *Seguridad*

2.76.1 ARQUITECTURA DE SEGURIDAD

Un planteamiento y un plan que cubre: (a) los servicios de seguridad que se le exigen a un sistema, (b) los componentes necesarios para proporcionar dichos servicios y (c) las características que se requieren de dichos componentes para enfrentarse eficazmante a las amenazas previsibles. [RFC4949:2007]

2.76.2 (EN) SECURITY ARCHITECTURE

(I) A plan and set of principles that describe (a) the security services that a system is required to provide to meet the needs of its users, (b) the system components required to implement the services, and (c) the performance levels required in the components to deal with the threat environment (e.g., [R2179]). (See: defense in depth, IATF, OSIRM Security Architecture, security controls, Tutorial under "security policy".) [RFC4949:2007]

2.76.3 (EN) IT SECURITY ARCHITECTURE

A description of security principles and an overall approach for complying with the principles that drive the system design; i.e., guidelines on the placement and implementation of specific security services within various distributed computing environments. [NIST-SP800-33:2001]

2.77 ASN.1 - ABSTRACT SYNTAX NOTATION ONE

Acrónimos: ASN.1

Ver:

- *BER - Basic Encoding Rules*
- *CER - Canonical Encoding Rules*
- *DER - Distinguished Encoding Rules*
- *PER - Packet Encoding Rules*
- *XER - XML Encoding Rules*

2.77.1 ASN.1 - ABSTRACT SYNTAX NOTATION ONE

http://es.wikipedia.org/wiki/ASN.1

2.77.2 (EN) ASN.1 - ABSTRACT SYNTAX NOTATION ONE

http://en.wikipedia.org/wiki/ASN.1

2.78 ASOCIACIÓN DE SEGURIDAD (SA)

Ver:

- *IPsec - IP security*
- *IKE - Internet Key Exchange*
- *ISAKMP - Internet Security Association Key Management Protocol*

2.78.1 ASOCIACIÓN DE SEGURIDAD (SA)

Relación establecida entre dos entidades que les permite proteger la información que intercambian.

2.78.2 (EN) SECURITY ASSOCIATION

A relationship established between two or more entities to enable them to protect data they exchange. [CNSSI_4009:2010]

2.78.3 (EN) SECURITY ASSOCIATION

1. (I) A relationship established between two or more entities to enable them to protect data they exchange. (See: association, ISAKMP, SAD. Compare: session.)

2. (I) /IPsec/ A simplex (uni-directional) logical connection created for security purposes and implemented with either AH or ESP (but not both). The security services offered by a security association depend on the protocol (AH or ESP), the IPsec mode (transport or tunnel), the endpoints, and the election of optional services within the protocol. A security association is identified by a triple consisting of (a) a destination IP address, (b) a protocol (AH or ESP) identifier, and (c) a Security Parameter Index.

3. (O) "A set of policy and cryptographic keys that provide security services to network traffic that matches that policy". [R3740] (See: cryptographic association, group security association.)

4. (O) "The totality of communications and security mechanisms and functions (e.g., communications protocols, security protocols, security mechanisms and functions) that securely binds together two security contexts in different end systems or relay systems supporting the same information domain." [DoD6]

[RFC4949:2007]

2.78.4 (EN) SECURITY ASSOCIATION (SA)

In Internet Protocol Security (IPSec), settings that establish policy and encryption keys used to protect communications between two end points in a Virtual Private Network (VPN). Security associations are negotiated between two computers during the first phase of establishing an Internet Key Exchange (IKE) connection.

http://www.watchguard.com/glossary/

2.79 ASYMMETRIC_CIPHER

Ver:

- *Cifrado asimétrico*

2.79.1 (EN) ASYMMETRIC CIPHER

system based on asymmetric cryptographic techniques whose public transformation is used foren-cryption and whose private transformation is used for decryption.[ISO-18033-1:2005]

2.79.2 (EN) ASYMMETRIC CIPHER

alternative term for asymmetric encryption system. [ISO-18033-1:2005]

2.80 ATAQUE

Ver:

- *Ataque distribuido*
- *Potencial de ataque*
- *Patrón de un ataque*
- *Árboles de ataque*

2.80.1 ATAQUE

Tentativa de destruir, exponer, alterar, inhabilitar, robar, acceder sin autorización o hacer un uso no autorizado de un activo [UNE-ISO/IEC 27000:2014]

2.80.2 ATAQUE

Intento de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja, o violar alguna política de seguridad de alguna otra manera. [ISO-18043:2006]

2.80.3 ATAQUE

Explotación de una o varias vulnerabilidades utilizando un método de ataque con una oportunidad dada.

Ejemplos:

- gran oportunidad de uso de software falsificado o copiado debido a la ausencia total de concienciación o de información sobre la legislación referida a los derechos de autor;
- alteración del software por un virus debido a la facilidad para introducir programas de efectos dañinos en la red ofimática del organismo;
- ...

[EBIOS:2005]

2.80.4 ATAQUE

Acción que puede violar los sistemas y mecanismos de seguridad de un sistema de información.

Tradicionalmente los ataques se dividen, según el efecto que producen, en: interrupción, interceptación, modificación y fabricación. Si se categorizan por el modo de actuación, se clasifican en: pasivos (no modifican el estado atacando) y activos (alteran el sistema atacado).

[Ribagorda:1997]

2.80.5 ATAQUE

1. Acciones encaminadas a descubrir las claves secreta o privada de un criptosistema.

2. Cualquier acción deliberada encaminada a violar los mecanismos de seguridad de un sistema de información.

[CESID:1997]

2.80.6 (EN) ATTACK

attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset [ISO/IEC 27000:2014]

2.80.1 (EN) ATTACK

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself . [CNSSI_4009:2010]

2.80.2 (EN) ATTACK

1. (I) An intentional act by which an entity attempts to evade security services and violate the security policy of a system. That is, an actual assault on system security that derives from an intelligent threat. (See: penetration, violation, vulnerability.)

2. (I) A method or technique used in an assault (e.g., masquerade).

Tutorial: Attacks can be characterized according to intent:

- An "active attack" attempts to alter system resources or affect their operation.
- A "passive attack" attempts to learn or make use of information from a system but does not affect system resources of that system. (See: wiretapping.)

The object of a passive attack might be to obtain data that is needed for an off-line attack.

- An "off-line attack" is one in which the attacker obtains data from the target system and then analyzes the data on a different system of the attacker's own choosing, possibly in preparation for a second stage of attack on the target.

Attacks can be characterized according to point of initiation:

- An "inside attack" is one that is initiated by an entity inside the security perimeter (an "insider"), i.e., an entity that is authorized to access system resources but uses them in a way not approved by the party that granted the authorization.
- An "outside attack" is initiated from outside the security perimeter, by an unauthorized or illegitimate user of the system (an "outsider"). In the Internet, potential outside

attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

Attacks can be characterized according to method of delivery:

- In a "direct attack", the attacker addresses attacking packets to the intended victim(s). In an "indirect attack", the attacker addresses packets to a third party, and the packets either have the address(es) of the intended victim(s) as their source address(es) or indicate the intended victim(s) in some other way. The third party responds by sending one or more attacking packets to the intended victims. The attacker can use third parties as attack amplifiers by providing a broadcast address as the victim address (e.g., "smurf attack"). (See: reflector attack. Compare: reflection attack, replay attack.)

[RFC4949:2007]

2.80.3 (EN) ATTACKER

Any person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources. [ISO-18028-1:2006]

2.80.4 (EN) ATTACK

Attempts to destroy, expose, alter, or disable an Information System and/or information within it or otherwise breach the security policy. [ISO-18043:2006]

2.80.5 (EN) ATTACK

The activities undertaken to bypass or exploit deficiencies in a system's security mechanisms. By a direct attack on a system they exploit deficiencies in the underlying algorithms, principles, or properties of a security mechanism. Indirect attacks are performed when they bypass the mechanism, or when they make the system use the mechanism incorrectly. [H.235:2005]

2.80.6 (EN) ATTACK

Exploiting one or more vulnerabilities using an attack method with a given opportunity.

Examples:

- strong opportunity of using counterfeit or copied software resulting from total absence of awareness or information concerning copyright legislation;
- software damaged by a virus through easy loading of malicious programmes onto the organisation's office network;
- etc.

[EBIOS:2005]

2.80.1 (EN) ATTACK

An attack is the act of carrying out an exploit.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/attack/590-BSI.html

2.80.2 (EN) ATTACK PATH

steps that an adversary takes or may take to plan, prepare for, and execute an attack

Annotation: An attack path may include recruitment, radicalization, and training of operatives, selection and surveillance of the target, construction or procurement of weapons, funding, deployment of operatives to the target, execution of the attack, and related post-attack activities.

DHS Risk Lexicon, September 2008

2.80.3 (EN) ATTACK PATH

An attack path is a path in an attack tree from a leaf node to the root node. An attack path can be a simplistic representation of an attack pattern.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/attack/590-BSI.html

2.80.4 (EN) ATTACK PATTERN

An attack pattern is a general framework for carrying out a particular type of attack such as a particular method for exploiting a buffer overflow or an interposition attack that leverages architectural weaknesses. In this paper, an attack pattern describes the approach used by attackers to generate an exploit against software.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/attack/590-BSI.html

2.80.5 (EN) ATTACKER

An attacker is the person that actually executes an attack. Attackers may range from very unskilled individuals leveraging automated attacks developed by others (script kiddies) to well-funded government agencies or even large international organized crime syndicates with highly skilled software experts.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/attack/590-BSI.html

2.80.6 (EN) ATTACK

An attempt by an unauthorized individual to fool a Verifier or a Relying Party into believing that the unauthorized individual in question is the Subscriber. [NIST SP-800-63:2013]

2.80.7 (EN) ATTACKER

A party who acts with malicious intent to compromise an information system. [NIST SP-800-63:2013]

2.80.8 (EN) OFF-LINE ATTACK

An attack where the Attacker obtains some data (typically by eavesdropping on an authentication protocol run or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing. [NIST SP-800-63:2013]

2.80.9 (EN) ONLINE ATTACK

An attack against an authentication protocol where the Attacker either assumes the role of a Claimant with a genuine Verifier or actively alters the authentication channel. [NIST SP-800-63:2013]

2.80.10 (EN) ATTACK SURFACE

The attack surface of a system or asset refers to the collectively exposed portions of that system or asset. A large attack surface means that there are many exposed areas that an attack could target, while a small attack surface means that the target is relatively unexposed. [knapp:2014]

2.80.11 (EN) ATTACK VECTOR

An attack vector is the direction(s) through which an attack occurs, often referring to specific vulnerabilities that are used by an attacker at any given stage of an attack.[knapp:2014]

2.80.12 (FR) ATTAQUE

Exploitation d'une ou plusieurs vulnérabilités à l'aide d'une méthode d'attaque avec une opportunité donnée.

Exemples:

- forte opportunité d'utilisation de logiciels contrefaits ou copiés du fait de l'absence totale de sensibilisation ou d'information sur la législation des droits d'auteur ;
- altération du logiciel par un virus du fait de la facilité d'introduire des logiciels à effets malicieux sur le réseau bureautique de l'organisme ;
- ...

[EBIOS:2005]

2.80.13 (FR) ATTAQUE

Une tentative d'exploitation d'une vulnérabilité d'un système IT [ISO-15947:2002]

2.81 ATAQUE ACTIVO

2.81.1 ATAQUE ACTIVO

Ataque que altera el sistema o los datos.

2.81.1 (EN) ACTIVE ATTACK

An attack that alters a system or data. [CNSSI_4009:2010]

2.81.1 (EN) ACTIVE ATTACK

An attack on the authentication protocol where the Attacker transmits data to the Claimant, Credential Service Provider, Verifier, or Relying Party. Examples of active attacks include man-in-the-middle, impersonation, and session hijacking. [NIST SP-800-63:2013]

2.82 ATAQUE "ENCONTRARSE EN EL MEDIO"

Ver:

- *Ataques a la criptografía*
- *Criptoanálisis*

2.82.1 ATAQUE "ENCONTRARSE EN EL MEDIO"

Ataque contra sistemas de doble cifrado. Para buscar las dos claves, se cifra el texto en claro con una clave, mientras se descifra el texto cifrado con otra clave. Si los resultados coinciden es que hemos hallado ambas claves.

2.82.2 (EN) MEET IN THE MIDDLE ATTACK

A known plaintext attack against double encryption with two separate keys where the attacker encrypts a plaintext with a key and ``decrypts" the original ciphertext with another key and hopes to get the same value.

http://www.rsasecurity.com/rsalabs/faq

2.83 ATAQUE CON SÓLO TEXTO CIFRADO

Ver:

- *Ataques a la criptografía*
- *Criptoanálisis*

2.83.1 ATAQUE CON SÓLO TEXTO CIFRADO

Variante de análisis criptográfico donde el atacante sólo dispone de texto cifrado.

2.83.2 (EN) CIPHERTEXT-ONLY ATTACK

(I) A cryptanalysis technique in which the analyst tries to determine the key solely from knowledge of intercepted cipher text (although the analyst may also know other clues, such as the cryptographic algorithm, the language in which the plain text was written, the subject matter of the plain text, and some probable plaintext words.) [RFC4949:2007]

2.83.3 (EN) CYPHERTEXT ONLY ATTACK

A form of cryptanalysis where the cryptanalyst has some ciphertext but nothing else.

http://www.rsasecurity.com/rsalabs/faq

2.84 ATAQUE CON TEXTO CIFRADO ESCOGIDO

Ver:

- *Ataques a la criptografía*
- *Criptoanálisis*

2.84.1 ATAQUE CON TEXTO CIFRADO ESCOGIDO

Método criptoanalítico en el cual el atacante puede obtener el texto en claro correspondiente a cualquier texto cifrado por él elegido. [Ribagorda:1997]

2.84.2 (EN) CHOSEN-CIPHERTEXT ATTACK

(I) A cryptanalysis technique in which the analyst tries to determine the key from knowledge of plain text that corresponds to cipher text selected (i.e., dictated) by the analyst. [RFC4949:2007]

2.84.3 (EN) CHOSEN CYPHERTEXT ATTACK

A chosen-ciphertext attack (CCA) is an attack model for cryptanalysis in which the cryptanalyst chooses a ciphertext and causes it to be decrypted with an unknown key. Specific forms of this attack are sometimes termed "lunchtime" or "midnight" attacks, referring to a scenario in which an attacker gains access to an unattended decryption machine. A device which provides decryptions of chosen ciphertexts (either by accident or by design) is generically referred to as a "decryption oracle".

http://en.wikipedia.org/wiki/Chosen_ciphertext_attack

2.85 ATAQUE CON TEXTO EN CLARO CONOCIDO

Ver:

- *Ataques a la criptografía*
- *Criptoanálisis*

2.85.1 ATAQUE CON TEXTO EN CLARO CONOCIDO

Agresión al cifrado que pretende averiguar la clave criptográfica usada a partir del conocimiento de un, o varios, texto cifrado y el texto en claro del, o de los, que procede, así como del algoritmo de cifra usado. Es el ataque usual a mensajes cifrados con algoritmos conocidos y transmitidos mediante protocolos normalizados (por ejemplo, EDI). [Ribagorda:1997]

2.85.2 (EN) KNOWN-PLAINTEXT ATTACK

(I) A cryptanalysis technique in which the analyst tries to determine the key from knowledge of some plaintext-ciphertext pairs (although the analyst may also have other clues, such as knowing the cryptographic algorithm). [RFC4949:2007]

2.85.3 (EN) KNOWN PLAINTEXT ATTACK

A form of cryptanalysis where the cryptanalyst knows both the plaintext and the associated ciphertext.

http://www.rsasecurity.com/rsalabs/faq

2.86 ATAQUE CON TEXTO EN CLARO ESCOGIDO

Ver:

- *Ataques a la criptografía*

- *Criptoanálisis*

2.86.1 ATAQUE CON TEXTO EN CLARO ESCOGIDO

Ataque consistente en elegir un texto en claro y comparar aquél con el texto cifrado obtenido, para así tratar de hallar la clave criptográfica que se está empleando. Presupone el conocimiento del algoritmo de cifra usado, o al menos el acceso al dispositivo en que está implementado. Un ejemplo típico se tiene en el usuario de un criptosistema asimétrico, que conoce por tanto la clave pública del mismo. También en el usuario de un ordenador con acceso a la tabla de contraseñas cifradas. Cambiando repetidamente su contraseña y examinando en cada ocasión la misma cifrada puede recopilar gran cantidad de pares contraseña en claro-contraseña cifrada. [Ribagorda:1997]

2.86.2 (EN) CHOSEN-PLAINTEXT ATTACK

(I) A cryptanalysis technique in which the analyst tries to determine the key from knowledge of cipher text that corresponds to plain text selected (i.e., dictated) by the analyst. [RFC4949:2007]

2.86.3 (EN) CHOSEN PLAINTEXT ATTACK

A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of the attack is to gain some further information which reduces the security of the encryption scheme. In the worst case, a chosen-plaintext attack could reveal the scheme's secret key.

http://en.wikipedia.org/wiki/Chosen-plaintext_attack

2.87 ATAQUE CONTROLADO

Ver:

- *Pruebas de penetración*
- *Escáner de vulnerabilidades*

2.87.1 ATAQUE CONTROLADO

Ataque a un sistema autorizado y controlado por el propietario del sistema. Tiene como objeto adelantarse a ataques reales para descubrir vulnerabilidades antes de que sean explotadas.

2.87.2 HACKING ÉTICO

Se denomina a la realización de un análisis de seguridad de una infraestructura TIC ayudándose de técnicas de hacking, su finalidad es la realización de ataque controlados cuyo fin es conocer la seguridad de los sistemas y aplicaciones, así como los fallos o brechas de seguridad para que puedan ser corregidas.

http://www.inteco.es/glossary/Formacion/Glosario/

2.87.3 (EN) WHITE HAT

White hat describes a hacker (or, if you prefer, cracker) who identifies a security weakness in a computer system or network but, instead of taking malicious advantage of it, exposes the weakness in a way that will allow the system's owners to fix the breach before it can be taken advantage by others (such as black hat hackers.) Methods of telling the owners about it range from a simple phone call through sending an e-mail note to a Webmaster or administrator all the way to leaving an electronic "calling card" in the system that makes it obvious that security has been breached.

http://searchsecurity.techtarget.com/

2.87.4 (EN) ETHICAL HACKER

An ethical hacker is a computer and network expert who attacks a security system on behalf of its owners, seeking vulnerabilities that a malicious hacker could exploit. To test a security system, ethical hackers use the same methods as their less principled counterparts, but report problems instead of taking advantage of them. Ethical hacking is also known as penetration testing, intrusion testing, and red teaming. An ethical hacker is sometimes called a white hat, a term that comes from old Western movies, where the "good guy" wore a white hat and the "bad guy" wore a black hat.

http://searchsoftwarequality.techtarget.com/glossary/

2.87.5 (EN) WHITE HAT

A white hat is a computer hacker who works to find and fix computer security risks. White hat consultants are often hired to attempt to break into their client's network to see if all security holes have been addressed.

http://cyber.law.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas

2.88 ATAQUE DEL CUMPLEAÑOS

Ver:

- *Ataques a la criptografía*
- *Criptoanálisis*

2.88.1 ATAQUE DEL CUMPLEAÑOS

Ataque de fuerza bruta que busca colisiones probando todas las combinaciones posibles de 2 textos.

Se basa en la paradoja del cumpleaños, que se puede resumir diciendo que la probabilidad de que dos o más personas en un grupo de individuos hayan nacido el mismo día, es superior al 50% cuando el número de personas es igual o mayor que 23 sujetos.

2.88.2 (EN) BIRTHDAY ATTACK

(I) A class of attacks against cryptographic functions, including both encryption functions and hash functions. The attacks take advantage of a statistical property: Given a cryptographic function having an N-bit output, the probability is greater than 1/2 that for 2**(N/2) randomly chosen inputs, the function will produce at least two outputs that are identical. (See: Tutorial under "hash function".) [RFC4949:2007]

2.88.3 (EN) BIRTHDAY ATTACK

A brute-force attack used to find collisions. It gets its name from the surprising result that the probability of two or more people in a group of 23 sharing the same birthday is greater than 1/2.

http://www.rsasecurity.com/rsalabs/faq

2.89 ATAQUE DIRIGIDO

2.89.1 ATAQUE DIRIGIDO

Son aquellos ataques realizados normalmente de manera silenciosa e imperceptible, cuyo objetivo es una persona, empresa o grupos de ambas. No son ataques masivos, porque su objetivo no es alcanzar al mayor número posible de ordenadores. Su peligro estriba precisamente en que son ataques personalizados, diseñados especialmente para engañar a las potenciales víctimas.

http://tecnologia.glosario.net/

2.89.1 (EN) TARGETED ATTACKS

A targeted attack occurs when attackers target a specific entity/organization over a long time span. Often the objective of targeted attacks is either data exfiltration or gaining persistent access and control of the target system. This kind of attack consists of an information gathering phase and the use of advanced techniques to fulfil the attacker's goals. The first phase can possibly involve specially crafted e-mails (spearphishing), infected media and social engineering techniques, whereas the second phase involves advanced and sophisticated exploitation techniques.

ENISA Threat Landscape [Deliverable – 2012-09-28]

2.90 ATAQUE DISTRIBUIDO

Ver:

- *Ataque*
- *Zombi*

2.90.1 ATAQUE DISTRIBUIDO

Ataque realizado mediante múltiples agentes desde diferentes lugares.

2.90.2 (EN) DISTRIBUTED ATTACK

1a. (I) An attack that is implemented with distributed computing. (See: zombie.)

1b. (I) An attack that deploys multiple threat agents.

[RFC4949:2007]

2.91 ATAQUE EXHAUSTIVO

Ver:

- *Ataque por fuerza bruta*
- *Criptoanálisis*

2.92 ATAQUE PASIVO

2.92.1 ATAQUE PASIVO

Se dice cuando el atacante accede a la información, pero la deja como estaba sin alterar su contenido.

2.92.1 (EN) PASSIVE ATTACK

An attack against an authentication protocol where the Attacker intercepts data traveling along the network between the Claimant and Verifier, but does not alter the data (i.e., eavesdropping). [NIST SP-800-63:2013]

2.92.2 (EN) PASSIVE ATTACK

An attack that does not alter systems or data. [CNSSI_4009:2010]

2.93 ATAQUE POR ARRANQUE EN FRIO

2.93.1 ATAQUE POR ARRANQUE EN FRIO

Un ataque de arranque en frío es un proceso para acceder a las claves de cifrado almacenadas en los chips de memoria RAM del equipo.

2.93.2 COLD BOOT ATTACK

A cold boot attack is a process for obtaining unauthorized access to encryption keys stored in the dynamic random access memory (DRAM) chips of a computer system.

http://searchsecurity.techtarget.com/

2.94 ATAQUE POR CANAL COLATERAL

Ver:

- *Análisis de tiempos*
- *Análisis de fallos*
- *Análisis simple de consumo*
- *Análisis diferencial de consumo*

2.95 ATAQUE POR DESLIZAMIENTO

Ver:

- *Ataques a la criptografía*
- *Criptoanálisis*

2.95.1 ATAQUE POR DESLIZAMIENTO

Ataque a algoritmos de cifra que utilizan varios ciclos similares de cifrado elemental. El ataque busca debilidades en la generación de sub-claves para cada ciclo.

2.95.2 (EN) SLIDE STTACK

The slide attack is a form of cryptanalysis designed to deal with the prevailing idea that even weak ciphers can become very strong by increasing the number of rounds, which can ward off a differential attack. The slide attack works in such a way as to make the number of rounds in a cipher irrelevant. Rather than looking at the data-randomizing aspects of the block cipher the slide attack works by analyzing the key schedule and exploiting weaknesses in it to break the cipher. The most common one is the keys repeating in a cyclic manner.

http://en.wikipedia.org/wiki/Slide_attack

2.96 ATAQUE POR DICCIONARIO

Ver:

- *Ataques a la criptografía*
- *Criptoanálisis*
- *Ataque por fuerza bruta*
- http://en.wikipedia.org/wiki/Dictionary_attack

2.96.1 ATAQUE DE DICCIONARIO

Método empleado para romper la seguridad de los sistemas basados en contraseñas (password) en la que el atacante intenta dar con la clave adecuada probando todas (o casi todas) las palabras posibles o recogidas en un diccionario idiomático. Generalmente se emplean programas especiales que se encargan de ello.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.96.2 (EN) DICTIONARY ATTACK

(I) An attack that uses a brute-force technique of successively trying all the words in some large, exhaustive list. [RFC4949:2007]

2.96.3 (EN) DICTIONARY ATTACK

A brute force attack that tries passwords and or keys from a precompiled list of values. This is often done as a precomputation attack.

http://www.rsasecurity.com/rsalabs/faq

2.96.4 (EN) DICTIONARY ATTACKS

A dictionary attack is a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a password. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypted message or document.

Dictionary attacks work because many computer users and businesses insist on using ordinary words as passwords. Dictionary attacks are rarely successful against systems that employ multiple-word phrases, and unsuccessful against systems that employ random combinations of uppercase and lowercase letters mixed up with numerals. In those systems, the brute-force method of attack (in which every possible combination of characters and spaces is tried up to a certain maximum length) can sometimes be effective, although this approach can take a long time to produce results.

Vulnerability to password or decryption-key assaults can be reduced to near zero by limiting the number of attempts allowed within a given period of time, and by wisely choosing the password or key. For example, if only three attempts are allowed and then a period of 15 minutes must elapse before the next three attempts are allowed, and if the password or key is a long, meaningless jumble of letters and numerals, a system can be rendered immune to dictionary attacks and practically immune to brute-force attacks.

A form of dictionary attack is often used by spammers. A message is sent to every e-mail address consisting of a word in the dictionary, followed by the at symbol (@), followed by the name of a particular domain. Lists of given names (such as frank, george, judith, or donna) can produce amazing results. So can individual letters of the alphabet followed by surnames (such as csmith, jwilson, or pthomas). E-mail users can minimize their vulnerability to this type of spam by choosing usernames according to the same rules that apply to passwords and decryption keys -- long, meaningless sequences of letters interspersed with numerals.

http://searchsoftwarequality.techtarget.com/glossary/

2.96.5 (EN) DICTIONARY ATTACK

An attack that tries all of the phrases or words in a dictionary, trying to crack a password or key. A dictionary attack uses a predefined list of words compared to a brute force attack that tries all possible combinations.

http://www.sans.org/security-resources/glossary-of-terms/

2.96.6 (FR) DICTIONNAIRE (ATTAQUE PAR)

Méthode visant à découvrir en peu de temps des mots de passe utilisateurs en utilisant comme base de départ des mots d'un dictionnaire et en les comparant une fois chiffrés avec le mot de passe chiffré que l'on souhaite découvrir. Les attaques par dictionnaires se font généralement plus vite que des attaques exhaustives qui visent à tester successivement toutes les combinaisons de caractères pour trouver le mot de passe. Les pirates se basent sur la probabilité que le mot de passe choisi peut être un mot courant du dictionnaire et donc plus facile et rapide à découvrir en lançant une attaque par dictionnaire qu'en effectuant une recherche exhaustive.

http://www.cases.public.lu/functions/glossaire/

2.97 ATAQUE POR FUERZA BRUTA

Ver:

- *Ataques a la criptografía*
- *Criptoanálisis*
- *Ataque exhaustivo*
- http://en.wikipedia.org/wiki/Brute_force_attack

2.97.1 ATAQUE EXHAUSTIVO

1. Caso particular de ataque sólo al texto cifrado en el que el criptoanalista, cociendo el algoritmo de cifra, intenta su descifrado probando con cada clave del espacio de claves. Si el cardinal de este último es un número muy grande, el tiempo invertido en recorrer el citado espacio es fabuloso, y las probabilidades de éxito escasísimas.

2. Aplicación de una función resumen (supuesto conocida) a todos los posibles mensajes de un espacio de ellos, para encontrar aquél cuyo resumen coincide con uno dado.

[Ribagorda:1997]

2.97.2 (EN) BRUTE FORCE

(I) A cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries a large number of possible solutions to the problem. (See: impossible, strength, work factor.) [RFC4949:2007]

2.97.3 (EN) BRUTE FORCE ATTACK

This attack requires trying all (or a large fraction of all) possible values till the right value is found; also called an exhaustive search.

http://www.rsasecurity.com/rsalabs/faq

2.97.4 (EN) BRUTE FORCE

An attacker gains unauthorised access to the hashed or encrypted password, runs a program offline to encrypt or hash a database of possible passwords and compares the results with the hashed or encrypted password. The brute force attack may be conducted through dictionary or exhaustion attacks or pre-calculated hashed or encrypted databases. Alternatively another (and more time-consuming) attack comprises the unauthorised user running a program online to try many passwords until a match is found though this can be countered by limiting the number of retries allowed A similar attack may be carried out against a file of hashed biometrics templates though exploitation of recovered biometrics may be more difficult.

2.97.5 (EN) BRUTE FORCE

An automated process of trial and error used to guess the secret protecting a system. Examples of these secrets include usernames, passwords or cryptographic keys.

http://www.webappsec.org/projects/glossary/

2.97.6 (EN) BRUTE FORCE

A cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries all possibilities, one-by-one.

http://www.sans.org/security-resources/glossary-of-terms/

2.98 ATAQUE POR MICROFRAGMENTOS DE TCP/IP

2.98.1 ATAQUE POR MICROFRAGMENTOS DE TCP/IP

Ataque consistente en fragmentar los paquetes TCP en partes IP tan pequeñas como para dividir la cabecera y engañar a los filtros que analizan la información en la cabecera para tomar decisiones respecto de los paquetes TCP.

2.98.2 (EN) TINY FRAGMENT ATTACK

With many IP implementations it is possible to impose an unusually small fragment size on outgoing packets. If the fragment size is made small enough to force some of a TCP packet's TCP header fields into the second fragment, filter rules that specify patterns for those fields will not match. If the filtering implementation does not enforce a minimum fragment size, a disallowed packet might be passed because it didn't hit a match in the filter.

STD 5, RFC 791 states: Every Internet module must be able to forward a datagram of 68 octets without further fragmentation. This is because an Internet header may be up to 60 octets, and the minimum fragment is 8 octets.

http://www.sans.org/security-resources/glossary-of-terms/

2.99 ATAQUE POR SUPERPOSICIÓN DE FRAGMENTOS TCP

2.99.1 ATAQUE POR SUPERPOSICIÓN DE FRAGMENTOS TCP

Ataque basado en la característica de las trasmisiones IP en las que se permite la fragmentación de los paquetes para una transmisión más eficiente. El ataque consiste en alterar la posición relativa del segundo fragmento de forma que al reconstruirse se deteriora interesadamente el destino.

2.99.2 (EN) FRAGMENT OVERLAP ATTACK

A TCP/IP Fragmentation Attack that is possible because IP allows packets to be broken down into fragments for more efficient transport across various media. The TCP packet (and its header) are carried in the IP packet. In this attack the second fragment contains incorrect offset. When packet is reconstructed, the port number will be overwritten.

http://www.sans.org/security-resources/glossary-of-terms/

2.100 ATAQUES A LA CRIPTOGRAFÍA

Ver:

- *Texto cifrado elegido dinámicamente*
- *Texto en claro elegido dinámicamente*
- *Ataques algebraicos*
- *Ataque del cumpleaños*
- *Ataque por fuerza bruta*
- *Ataque con texto cifrado escogido*
- *Ataque con texto en claro escogido*
- *Ataque con sólo texto cifrado*
- *Ataque por diccionario*
- *Criptoanálisis diferencial*
- *Ataque con texto en claro conocido*
- *Criptoanálisis lineal*
- *Ataque "encontrarse en el medio"*
- *Ataque por deslizamiento*

2.101 ATAQUES A LA VALIDACIÓN DE DATOS

2.101.1 ATAQUES A LA VALIDACIÓN DE DATOS

Ataques en los que el atacante introduce deliberadamente datos erróneaos con el fin de confundir a la aplicación.

2.101.2 (EN) INPUT VALIDATION ATTACKS

Input Validations Attacks are where an attacker intentionally sends unusual input in the hopes of confusing an application.

http://www.sans.org/security-resources/glossary-of-terms/

2.102 ATAQUES ALGEBRAICOS

Ver:

- *Ataques a la criptografía*
- *Criptoanálisis*

2.102.1 ATAQUES ALGEBRAICOS

Ataque basado en las propiedades algebraicas del un algoritmo de cifra.

2.102.2 (EN) ALGEBRAIC ATTACK

algebraic attack A method of cryptanalytic attack used against block ciphers that exhibit a significant amount of mathematical structure.

http://www.rsasecurity.com/rsalabs/faq

2.103 ATAQUES DE REPRODUCCIÓN

Ver:

- http://en.wikipedia.org/wiki/Replay_attack

2.103.1 ATAQUES DE REPRODUCCIÓN

Ataque consistente en capturar una transmisión de datos correcta y reproducirla posteriormente. Es un ataque típico para capturar secuencias de autenticación correctas y reproducirlas luego para que el atacante logre los mismos derechos de acceso.

2.103.2 (EN) REPLAY ATTACK

An attack in which the Attacker is able to replay previously captured messages (between a legitimate Claimant and a Verifier) to masquerade as that Claimant to the Verifier or vice versa.[NIST-SP800-63:2013]

2.103.3 (EN) REPLAY ATTACK

An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access. [CNSSI_4009:2010]

2.103.4 (EN) REPLAY ATTACK

(I) An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by a third party who intercepts the data and retransmits it, possibly as part of a masquerade attack. (See: active wiretapping, fresh, liveness, nonce. Compare: indirect attack, reflection attack.) [RFC949:2007]

2.103.5 (EN) REPLAY ATTACKS

Where dialogue between the authentication system and main system is intercepted and replayed into the main system by an attacker at a later date. This includes for instance an attacker connecting a PC that appears to perform a password hashing function but in fact merely transmits a previously intercepted hash value.

2.103.6 (EN) REPLAY ATTACK

A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).

http://en.wikipedia.org/wiki/Replay_attack

2.104 ATAQUES POR INFERENCIA

2.104.1 INFERIR

Sacar una consecuencia o deducir algo de otra cosa.

DRAE. Diccionario de la Lengua Española.

2.104.2 ATAQUES POR INFERENCIA

Ataques que se basan en información deducida lógicamente a partir de piezas aparentemente inconexas.

2.104.3 (EN) INFERENCE

something that you can find out indirectly from what you already know.

Oxford Advanced Learner's Dictionary.

2.104.4 (EN) INFERENCE ATTACKS

Inference Attacks rely on the user to make logical connections between seemingly unrelated pieces of information.

http://www.sans.org/security-resources/glossary-of-terms/

2.105 ATAQUES POR MONITORIZACIÓN

Ver:

- *Ataque*

2.105.1 ATAQUES POR MONITORIZACIÓN

Familia de métodos de ataque que se refiere a técnicas pasivas de análisis del comportamiento de un dispositivo criptográfico mientras se ejecutan tareas normales.

2.105.2 (EN) MONITORING ATTACKS

a generic category of attack methods that includes passive analysis techniques aiming at disclosure of sensitive internal data of the TOE by operating the TOE in the way that corresponds to the guidance documents.

TOE - Target of Evaluation

[CC:2006]

2.106 ATRIBUTO

Ver:

- *Certificado de atributo*

2.106.1 ATRIBUTO

Una propiedad de una entidad, física o abstracta.

2.106.2 (EN) ATTRIBUTE

(N) Information of a particular type concerning an identifiable system entity or object. An "attribute type" is the component of an attribute that indicates the class of information given by the attribute; and an "attribute value" is a particular instance of the class of information indicated by an attribute type. (See: attribute certificate.) [RFC4949:2007]

2.106.3 (EN) ATTRIBUTE

Information associated with a key that is not used in cryptographic algorithms but is required to implement applications and applications protocols. [NIST-SP800-57:2007]

2.106.4 (EN) ATTRIBUTE

Information concerning a managed object used to describe (either in part or in whole) that managed object. This information consists of an attribute type and its corresponding attribute value (single-valued) or values (multi-valued). [X.790:1995]

2.107 ATRIBUTO DE SEGURIDAD

2.107.1 ATRIBUTO DE SEGURIDAD

Una abstracción que representa las propiedades básicas o características de una entidad con respecto a la protección de la información; típicamente asociados con estructuras de datos internas (por ejemplo, registros, buffers, archivos, etc.). Estos atributos típicamente se utilizan como soporte del control de acceso, políticas de control de flujo, reglas especiales de difusión, etc. En general, para implementar políticas de seguridad de la información.

2.107.2 (EN) SECURITY ATTRIBUTE

An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the information system which are used to enable the implementation of access control and flow control policies; reflect special dissemination, handling, or distribution instructions; or support other aspects of the information security policy. [CNSSI_4009:2010]

2.108 AUDITORÍA

Ver:

- *Recogida de pistas de auditoría*
- *Registro de auditoría*
- *Pista de auditoría*
- *Auditoría de seguridad*
- *Certificación*
- *Valoración*

2.108.1 AUDITAR

Examinar la gestión económica de una entidad a fin de comprobar si se ajusta a lo establecido por ley o costumbre.

DRAE. Diccionario de la Lengua Española. .

2.108.2 AUDITORÍA

Proceso sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.

NOTA 1: Una auditoría puede ser interna (de primera parte), o externa (de segunda o tercera parte), y puede ser combinada (combinando dos o más disciplinas).

[ISO Anexo SL] [UNE-ISO/IEC 27000:2014]

2.108.3 AUDITORÍA

Inspección formal para verificar si un Estándar o un conjunto de Guías se está siguiendo, que sus Registros son precisos, o que las metas de Eficiencia y Efectividad se están cumpliendo. Una Auditoría la puede realizar tanto un grupo interno como uno externo. Ver Certificación, Evaluación. [ITIL:2007]

2.108.4 AUDITORÍA

La auditoría consiste en la revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse, según la definición dada por la Real Academia de la Lengua Española.

El origen etimológico de la palabra es el verbo latino "audire", que significa "oír". Esta denominación proviene de su origen histórico, ya que los primeros auditores ejercían su función juzgando la verdad o falsedad de lo que les era sometido a su verificación principalmente oyendo.

http://es.wikipedia.org/wiki/Auditor%C3%ADa

2.108.5 AUDITORÍA

proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoría

NOTA. Las auditorías internas, denominadas en algunos casos como auditorías de primera parte, se realizan por, o en nombre de, la propia organización para fines internos y puede constituir la base para la auto-declaración de conformidad de una organización.

[ISO-9000_es:2000]

2.108.6 AUDITORÍA DE SISTEMAS DE INFORMACIÓN

La auditoría de sistemas de información es realizada para verificar ya sea por un equipo interno o externo que analiza el funcionamiento y la distribución de los controles en los procesos de información de una empresa, organización o cualquier sistema que utilice medios de información, principalmente se realizan para encontrar fallas, en el sistema a analizar, que permitan optimizar, homogenizar, acercar, y proteger los procesos informáticos, ya que el flujo de la información se facilita en cuanto se automatiza reduciendo el error humano, el termino de informático se trata como sinónimo ya que en la actualidad no podemos hablar de sistemas de información sin hablar de informática.

http://es.wikipedia.org/wiki/Auditor%C3%ADa_de_sistemas_de_informaci%C3%B3n

2.108.7 (EN) AUDIT

systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

NOTE 1: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

[ISO/IEC 27000:2014]

2.108.1 (EN) AUDIT

Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures . [CNSSI_4009:2010]

2.108.2 (EN) AUDIT

A review of system security (or software security) in order to provide assurance that the system's security posture is adequate. Comprehensive auditing is a good security practice, but specific kinds of auditing may also be mandated by government, regulatory, or contractual considerations. During software development, this term is often used to refer to a code review or to an architectural risk assessment. In an operational environment, auditing refers to a review of security logs or other data collected during ongoing monitoring of operations to identify actual or attempted security breaches and to evaluate the quality of a system?s security. Such auditing should be done frequently, but, unlike intrusion detection approaches, auditing is typically not expected to be a real-time activity.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/risk/248-BSI.html

2.108.3 (EN) AUDIT

Formal inspection and verification to check whether a Standard or set of Guidelines is being followed, that Records are accurate, or that Efficiency and Effectiveness targets are being met. An Audit may be carried out by internal or external groups. See Certification, Assessment. [ITIL:2007]

2.108.4 (EN) AUDIT

Formal inquiry, formal examination, or verification of facts against expectations, for compliance and conformity. [ISO-18028-1:2006]

2.108.5 (EN) AUDIT AND AUDIT TRAILS

Audits are conducted to support operational assurance and examine whether systems are meeting stated or implied security requirements, including system and organization policies.

Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.

Audit trails may be used as either a support for regular system operations, or as a kind of insurance policy, or as both of these. As insurance, audit trails are maintained but are not used unless needed, such as after a system outage. As a support for operations, audit trails are used to help system administrators ensure that the system or resources have not been harmed by hackers, insiders, or technical problems.

Mobile Security Reference Architecture, May 23, 2013

2.108.6 (EN) AUDIT TOOLS

automated tools to aid the analysis of the contents of audit logs. [ISO-18028-1:2006]

2.108.7 (EN) AUDITING

Auditing is the information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities.

http://www.sans.org/security-resources/glossary-of-terms/

2.108.8 (EN) AUDITOR

A third party independent organization or person(s) that performs audits.

http://iab.com/

2.108.9 (FR) AUDIT

Inspection et vérification formelle permettant de s'assurer qu'un standard ou un ensemble de principes a bien été suivi, que les enregistrements sont précis ou que les objectifs d'efficience et d'efficacité ont été atteints. Un audit peut être effectué par des groupes internes ou externes. Voir Certification, Évaluation. [ITIL:2007]

2.108.10 (FR) AUDIT

L'audit est un processus méthodique, indépendant et documenté permettant d'effectuer une revue et une inspection des activités et des enregistrements des événements systèmes à un instant t. Il permet de valider l'adéquation des contrôles mis en place pour assurer la conformité, l'adéquation et l'efficacité des politiques et des procédures opérationnelles garantissant la conformité et la sécurité des données. Au final, l'audit apporte des recommandations pour des changements nécessaires dans les contrôles, les politiques ou les procédures.

http://www.cases.public.lu/functions/glossaire/

2.109 AUDITORÍA DE SEGURIDAD

Ver:

- *Auditoría*

2.109.1 AUDITORÍA DE LA SEGURIDAD.

Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos. [ENS:2010]

2.109.2 AUDITORÍA DE SEGURIDAD

Estudio y examen independiente del historial y actividades de un sistema de información, con la finalidad de comprobar la idoneidad de los controles del sistema, asegurar su conformidad con la estructura de seguridad y procedimientos operativos establecidos, a fin de detectar brechas en la

seguridad y recomendar cambios en los procedimientos, controles y estructuras de seguridad. [Magerit:2012]

2.109.3 AUDITORÍA DE SEGURIDAD

Revisión y examen independiente de los registros y actividades de un sistema, a fin de verificar la fiabilidad de sus controles de seguridad (para asegurar el cumplimento de la política y procedimientos de seguridad) y detectar sus vulnerabilidades. Como consecuencia, debe recomendar las modificaciones oportunas de dicha política, procedimientos y controles (ISO-7498-2)

La citada norma lo reconoce como un mecanismo de seguridad, cuya acción es disuasoria para cualquier potencial atacante, que se arriesga a ser delatado por el anterior mecanismo.

[Ribagorda:1997]

2.109.4 AUDITORÍA DE SEGURIDAD

Estudio y examen independiente del historial y actividades de un sistema de información, con la finalidad de comprobar la idoneidad de los controles del sistema, asegurar su conformidad con la estructura de seguridad y procedimientos operativos establecidos, a fin de detectar brechas en la seguridad y recomendar cambios en los procedimientos, controles y estructuras de seguridad. [CESID:1997]

2.109.5 AUDITORÍA DE SEGURIDAD

Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos. [ISO-7498-2:1989]

2.109.6 AUDITORÍA DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN

Una auditoría de seguridad informática o auditoría de seguridad de sistemas de información (SI) es el estudio que comprende el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Las auditoras de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

http://es.wikipedia.org/wiki/Auditor%C3%ADa_de_seguridad_de_sistemas_de_informaci%C3%B3n

2.109.7 (EN) SECURITY AUDIT

(I) An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures. [ISO-7498-2, NCS01] (Compare: accounting, intrusion detection.) [RFC4949:2007]

2.109.8 (EN) SECURITY AUDIT

An independent review and examination of data processing system records and activities to test for adequacy of system controls, to ensure compliance with established security policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, security policy, and procedures. [ISO-2382-8:1998]

2.109.9 (EN) SECURITY AUDIT

An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures. [ISO-7498-2:1989]

2.109.10 (FR) AUDIT DE SÉCURITÉ

Revue indépendante et examen des enregistrements et des activités du système afin de vérifier l'exactitude des contrôles du système pour s'assurer de leur concordance avec la politique de sécurité établie et les procédures d'exploitation, pour détecter les infractions à la sécurité et pour recommander les modifications appropriées des contrôles, de la politique et des procédures. [ISO-7498-2:1989]

2.110 AUTENTICACIÓN

Ver:

- *Autenticar*
- *Servicio de autenticación*
- *Autenticidad del origen de la información*
- *Autenticación de una entidad*
- *Autenticación de la otra parte*
- *Intercambio de autenticación*
- *Método asimétrico de autenticación*
- *Método simétrico de autenticación*
- *Autenticador*
- *Certificado de autenticación*
- *AAA - Autenticación, Autorización y Registro*
- *Verificación visual*
- *Identificación*

2.110.1 AUTENTICACIÓN

Acción y efecto de autenticar.

Autenticar. Acreditar. Dar fe de la verdad de un hecho o documento con autoridad legal.

DRAE. Diccionario de la Lengua Española.

2.110.2 AUTENTICACIÓN

Proceso para verificar la identidad de un individuo, dispositivo o proceso. Por lo general, la autenticación ocurre a través del uso de uno o más factores de autenticación, tales como:

- Algo que el usuario sepa, como una contraseña o frase de seguridad
- Algo que el usuario tenga, como un dispositivo token o una tarjeta inteligente
- Algo que el usuario sea, como un rasgo biométrico

http://es.pcisecuritystandards.org

2.110.3 AUTENTICACIÓN

Aportación de garantías de que son correctas las características que para sí reivindica una entidad]UNE-ISO/IEC 27000:2014]

2.110.4 AUTENTICACIÓN

«autenticación», un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico; [PE-CONS 60/14]

2.110.5 AUTENTICACIÓN

Servicio de seguridad que permite verificar la identidad. [CCN-STIC-405:2006]

2.110.6 AUTENTICACIÓN

El acto de verificar la identidad de un usuario y su elegibilidad para acceder a la información computarizada. La autenticación está diseñada para proteger contra conexiones de acceso fraudulentas. [COBIT:2006]

2.110.7 AUTENTICACIÓN

Proceso utilizado en los mecanismos de control de acceso con el objetivo de verificar la identidad de un usuario, dispositivo o sistema mediante la comprobación de credenciales de acceso. [CCN-STIC-400:2006]

2.110.8 AUTENTICACIÓN

Procedimiento de comprobación de la identidad de un usuario.

Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

2.110.9 AUTENTICACIÓN

1. Proceso ejecutado entre un emisor y un receptor de un canal de transmisión para garantizar la integridad de los datos y la autenticidad del origen de los mismos (ISO-8732).

Es importante notar que esta definición, en la actualidad, es poco usada por equívoca, pues en el presente el término autenticación se refiere, exclusivamente, a entidades y sujetos (en su acepción de comprobación por encontrarse en textos no actualizados.

2. Servicio de seguridad que se puede referir al origen de datos o a una entidad homóloga (ISO-7498-2)

Garantiza que el origen de datos, o la entidad homóloga, son quienes afirman ser.

[Ribagorda:1997]

2.110.10 AUTENTICACIÓN SIMPLE

Autenticación mediante contraseñas (ISO/IEC 9594-8, ITU-T X.509) [Ribagorda:1997]

2.110.11 AUTENTIFICACIÓN

Sinónimo de Autenticación, siendo esta última la preferida por la Real Academia de la Lengua Española. [Ribagorda:1997]

2.110.12 AUTENTICACIÓN (SIMPLE) O AUTENTIFICACIÓN

Servicio de seguridad que previene contra transmisiones fraudulentas. Puede determinar la validez de la pareja de corresponsales (peer-entity) o del origen del mensaje recibido.

Como mecanismo de seguridad, es el procedimiento que presta dicho servicio, para conseguir la autenticidad de la información (técnicas criptográficas, empleo de características o propiedades del corresponsal, contraseñas certificadas, sincronización de relojes y referencias horarias, etc.).

[CESID:1997]

2.110.13 AUTENTICACIÓN

Véanse «autenticación de origen de los datos» y «autenticación de entidad par». [ISO-7498-2:1989]

2.110.1 DATOS CONFIDENCIALES DE AUTENTICACIÓN

Información de seguridad (entre otra, códigos o valores de validación de tarjetas, datos completos de la pista [de la banda magnética o su equivalente en un chip], PIN y bloqueos de PIN) utilizada en la autenticación de titulares de tarjetas o en la autorización de transacciones realizadas con tarjeta de pago.

http://es.pcisecuritystandards.org

2.110.2 (EN) AUTHENTICATION

'authentication' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed; [PE-CONS 60/14]

2.110.3 (EN) AUTHENTICATE

To prove that something is genuine, real or true.

Oxford Advanced Learner's Dictionary.

2.110.1 (EN) AUTHENTICATION

provision of assurance that a claimed characteristic of an entity is correct [ISO/IEC 27000:2014]

2.110.2 (EN) AUTHENTICATION

The process of establishing confidence in the identity of users or information systems.[NIST-SP800-63:2013]

2.110.3 (EN) AUTHENTICATION PROTOCOL

A defined sequence of messages between a Claimant and a Verifier that demonstrates that the Claimant has possession and control of a valid token to establish his/her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier. [NIST-SP800-63:2013]

2.110.4 (EN) AUTHENTICATE

To verify the identity of a user, user device, or other entity. [CNSSI_4009:2010]

2.110.1 (EN) AUTHENTICATION

The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data.

NIST SP 800-53: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

[CNSSI_4009:2010]

2.110.2 (EN) AUTHENTICATION MECHANISM

Hardware or software-based algorithm that forces users, devices, or processes to prove their identity before accessing data on an information system. [CNSSI_4009:2010]

2.110.3 (EN) AUTHENTICATION PROTOCOL

A well specified message exchange process between a claimant and a verifier that enables the verifier to confirm the claimant’s identity. [CNSSI_4009:2010]

2.110.4 (EN) AUTHENTICATION

(I) The process of verifying a claim that a system entity or system resource has a certain attribute value. (See: attribute, authenticate, authentication exchange, authentication information, credential, data origin authentication, peer entity authentication, "relationship between data integrity service and authentication services" under "data integrity service", simple authentication, strong authentication, verification, X.509.)

Tutorial: Security services frequently depend on authentication of the identity of users, but authentication may involve any type of attribute that is recognized by a system. A claim may be made by a subject about itself (e.g., at login, a user typically asserts its identity) or a claim may be made on behalf of a subject or object by some other system entity (e.g., a user may claim that a data object originates from a specific source, or that a data object is classified at a specific security level).

An authentication process consists of two basic steps:

- Identification step: Presenting the claimed attribute value (e.g., a user identifier) to the authentication subsystem.
- Verification step: Presenting or generating authentication information (e.g., a value signed with a private key) that acts as evidence to prove the binding between the attribute and that for which it is claimed. (See: verification.)

[RFC4949:2007]

2.110.5 (EN) AUTHENTICATION

Process of verifying identity of an individual, device, or process. Authentication typically occurs through the use of one or more authentication factors such as:

- Something you know, such as a password or passphrase
- Something you have, such as a token device or smart card
- Something you are, such as a biometric

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.110.6 (EN) AUTHENTICATION

A process that establishes the origin of information, or determines an entitys identity. [NIST-SP800-57:2007]

2.110.7 (EN) AUTHENTICATION

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. [FIPS-200:2006]

2.110.8 (EN) AUTHENTICATION

The act of verifying the identity of a user and the user's elegibility to access computarised information. Authentication is designed to protect against fraudulent logon. [COBIT:2006]

2.110.9 (EN) AUTHENTICATION

provision of assurance of the claimed identity of an entity.

In case of user authentication, users are identified either by knowledge (e.g., password), by possession (e.g., token) or by a personal characteristic (biometrics). Strong authentication is either based on strong mechanisms (e.g., biometrics) or makes use of at least two of these factors (so-called multi-factor authentication). [ISO-18028-4:2005]

2.110.10 (EN) SIMPLE AUTHENTICATION

Authentication by means of simple password arrangements. [X.509:2005]

2.110.11 (EN) AUTHENTICATION

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system. [NIST-SP800-27:2004]

2.110.12 (EN) AUTHENTICATION

Security control designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NIST-SP800-60V2:2004]

2.110.13 (EN) AUTHENTICATION

The Authentication Security Dimension serves to confirm the identities of communicating entities. Authentication ensures the validity of the claimed identities of the entities participating in communication (e.g. person, device, service or application) and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication. [X.805:2003]

2.110.14 (EN) AUTHENTICATION

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system. [NIST-SP800-33:2001]

2.110.15 (EN) MUTUAL ENTITY AUTHENTICATION

Entity authentication which provides both entities with assurance of each other's identity. [ISO-11770-3:2008]

2.110.16 (EN) AUTHENTICATED IDENTITY

A distinguishing identifier of a principal that has been assured through authentication. [ISO-10181-2:1996]

2.110.17 (EN) AUTHENTICATION

the verification of a claimed identity. [ITSEM:1993]

2.110.18 (EN) AUTHENTICATION

the provision of assurance of the claimed identity of an entity. [ISO-10181-2:1996]

2.110.19 (EN) AUTHENTICATION

See data origin authentication, and peer entity authentication. [ISO-7498-2:1989]

2.110.20 (EN) SENSITIVE AUTHENTICATION DATA:

Security-related information (including but not limited to card validation codes/values, full magnetic-stripe data, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.110.21 (EN) AUTHENTICATION

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. The weakness in this system for transactions that are significant (such as the exchange of money) is that passwords can often be stolen, accidentally revealed, or forgotten.

http://searchsecurity.techtarget.com/

2.110.22 (EN) AUTHENTICATION

The process for verifying that someone or something is who or what it claims to be.

http://www.getsafeonline.org/

2.110.23 (EN) AUTHENTICATION

The assurance that a party to some computerized transaction is not an impostor. Authentication typically involves using a password, certificate, PIN, or other information that can be used to validate the identity over a computer network.

http://www.symantec.com/avcenter/refa.html

2.110.24 (EN) AUTHENTICATION

Authentication is the process of confirming the correctness of the claimed identity.

http://www.sans.org/security-resources/glossary-of-terms/

2.110.25 (EN)AUTHENTICATION AND AUTHORIZATION

Authentication is the process of verifying an identity. Electronic authentication (e-authentication) is the process of establishing confidence in identities electronically presented to an information system.

Authentication precedes authorization. Authorization is the defining of privileges on a system. Authorization can be tied to identities or to roles and can control the actions of a user, executable code, or a data element, but authorization only succeeds if paired with authentication to validate which privileges should be assigned based on validating the identity being granted the privileges.

Mutual authentication is a higher level of authentication. In mutual authentication, both the authentication target and the authentication requestor verify the identity of the other end of the exchange. As an example, mutual authentication may occur between a user and a bank. The bank requires authentication of the requesting user to prove that the requestor should be granted access to a particular bank account. At the same time, the requesting userswant proof that they are connected to the actual bank web presence and not a “spoof” of the bank, to be sure they are not sharing their authentication credentials with a potential bad actor.

Mobile Security Reference Architecture, May 23, 2013

2.110.26 (FR) AUTHENTIFICATION

"authentification", un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique; [PE-CONS 60/14]

2.110.27 (FR) AUTHENTIFICATION

Processus de vérification de l'identité d'une personne, d'un dispositif ou d'un processus. L'authentification se fait généralement par l'utilisation d'un ou plusieurs facteurs d'authentification, tels que:

- Quelque chose de connu du seul utilisateur, comme un mot de passe ou une locution de passage;
- Quelque chose de détenu par l'utilisateur, comme un dispositif de jeton ou une carte à puce;
- Quelque chose concernant l'utilisateur, comme une mesure biométrique.

http://fr.pcisecuritystandards.org/

2.110.28 (FR) AUTHENTIFICATION MUTUELLE

Authentification d'entités qui garantie que chacun des entités a l'assurance de l'identité de chacune des autres entités. [ISO-9798-1:1997]

2.110.29 (FR) AUTHENTIFICATION

Voir «authentification de l'origine des données» et «authentification de l'entité homologue» [ISO-7498-2:1989]

2.110.30 (FR) AUTHENTIFICATION

Service de sécurité dont l'objectif est de valider l'identité d'une entité (utilisateur ou équipement). Il existe classiquement trois méthodes d'authentification permettant de prouver l'identité d'une entité:

- Authentification basée sur la connaissance d'un secret (ex.: mot de passe).
- Authentification basée sur la possession d'un objet (ex.: carte à puce, jeton).
- Authentification basée sur la biométrie.

http://securit.free.fr/glossaire.htm

2.111 AUTENTICACIÓN CON 2 ELEMENTOS

Ver:

- *Autenticación con tres elementos*
- *Autenticación*

2.111.1 AUTENTICACIÓN CON 2 ELEMENTOS

Utilización de dos elementos de autenticación independientes. Por ejemplo: una tarjeta inteligente activada por un PIN. La idea es que la combinación de elementos es más robusta que cada elemento por independiente.

2.111.2 AUTENTICACIÓN DE DOS FACTORES

Método de autenticación de un usuario mediante la comprobación de dos o más factores. Estos factores incluyen algo que el usuario posee (como un token de hardware o software), algo que sabe (como una contraseña, frase de seguridad o PIN) o algo que el usuario es o algo que hace (como las huellas dactilares y otros elementos biométricos).

http://es.pcisecuritystandards.org

2.111.3 (EN) TWO-FACTOR AUTHENTICATION

Method of authenticating a user whereby two or more factors are verified. These factors include something the user has (such as hardware or software token), something the user knows (such as a password, passphrase, or PIN) or something the user is or does (such as fingerprints or other forms of biometrics).

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.111.4 (EN) TWO-FACTOR AUTHENTICATION

The use of two independent mechanisms for authentication; for example, requiring a smart card and a password. The combination is less likely to allow abuse than either component alone.

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.111.5 (FR) AUTHENTIFICATION À DEUX FACTEURS

Méthode d'authentification d'un utilisateur par la vérification de deux ou plusieurs facteurs. Ces facteurs sont constitués d'un élément que possède l'utilisateur (comme un token matériel ou logiciel), d'un élément que l'utilisateur connaît (comme un mot de passe, une locution de passage ou un code PIN), ou d'un élément qui identifie ou que fait l'utilisateur effectue (comme une empreinte digitale ou autre forme de mesure biométrique).

http://fr.pcisecuritystandards.org/

2.112 AUTENTICACIÓN CON TRES ELEMENTOS

Ver:

- *Autenticación con 2 elementos*
- *Autenticación*

2.112.1 AUTENTICACIÓN CON TRES ELEMENTOS

Utilización de tres elementos de autenticación independientes. Por ejemplo: una tarjeta inteligente activada por un PIN, con verificación biométrica. La idea es que la combinación de elementos es más robusta que cada elemento por independiente.

2.112.2 (EN) THREE-FACTOR AUTHENTICATION

The use of three independent mechanisms for authentication; for example, requiring a smart card, a password, and a biometric identifier. This provides superior security.

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.113 AUTENTICACIÓN DE LA OTRA PARTE

Ver:

- *Autenticación*
- *Entidad*

2.113.1 AUTENTICACIÓN DE LA OTRA PARTE

Corroboración de que entidad con la que se establece una asociación de seguridad es la que alega ser.

2.113.2 AUTENTICACIÓN DE ENTIDAD PAR

Corroboración de que una entidad par en una asociación es la pretendida. [ISO-7498-2:1989]

2.113.3 (EN) PEER-ENTITY AUTHENTICATION

corroboration that a peer entity in an association is the one claimed. [ISO-18028-2:2006]

2.113.4 (EN) PEER-ENTITY AUTHENTICATION

The corroboration that a peer entity in an association is the one claimed. [ISO-7498-2:1989]

2.113.5 (FR) AUTHENTIFICATION DE L'ENTITÉ HOMOLOGUE

Confirmation qu'une entité homologue d'une association est bien l'entité déclarée. [ISO-7498-2:1989]

2.114 AUTENTICACIÓN DE UNA ENTIDAD

Ver:

- *Autenticación*
- *Entidad*

2.114.1 AUTENTICACIÓN DE UNA ENTIDAD

Comprobación de que una entidad es la que alega ser (ISO/IEC ISO-9798-1).

… de una prueba que permite a un sistema de información identificar fehacientemente a una entidad.

[Ribagorda:1997]

2.114.2 AUTENTICACIÓN DE UNA ENTIDAD HOMOLOGADA

Comprobación de que una de las entidades homólogas de una asociación es la alegada (ISO-7498-2). [Ribagorda:1997]

2.114.3 (EN) ENTITY AUTHENTICATION

The corroboration that an entity is the one claimed. [ISO-9798-1:1997]

2.114.4 (EN) UNILATERAL AUTHENTICATION

Entity authentication that provides one entity with assurance of the other's identity but not vice versa.[ISO-9798-1:1997]

2.114.5 (EN) MUTUAL AUTHENTICATION (TWO-WAY AUTHENTICATION)

Entity authentication which provides both entities with assurance of each other's identity. [ISO-9798-1:1997]

2.115 AUTENTICACIÓN FUERTE

Ver:

- *Autenticación*
- *Autenticación simple*

2.115.1 AUTENTICACIÓN FUERTE

Autenticación por medio de credenciales derivadas criptográficamente. [X.509:2005]

2.115.1 AUTENTICACIÓN FUERTE

Autenticación mediante credenciales obtenidas por técnicas criptográficas simétricas o asimétricas (ISO/IEC 9594-8, ITU-T X.509).

La autenticación fuerte puede ser de un sentido, de dos o de tres. En la primera, un usuario, A, se identifica y autentica, mediante credenciales, ante otro, B, sin que éste haga lo mismo frente a A. En la segunda, la autenticación es mutua de A ante B y de éste ante aquel. Finalmente, en la tercera, el proceso es como el descrito para dos sentidos, con la adición de un último paso en el que A remite a B una credencial más que evita estampillar el tiempo en las credenciales anteriores.

[Ribagorda:1997]

2.115.2 AUTENTICACIÓN COMPLEJA O FUERTE (STRONG)

Tipo de autenticación utilizado en algunas aplicaciones que no se basa únicamente en la demostración de la identidad por una contraseña, sino que intercambia más información ofreciendo más seguridad. En general uno de los corresponsales genera un código que transmite y el otro corresponsal debe devolverlo procesado de un modo preestablecido. Puede ser:

- de un sentido (one-way): el receptor establece la identidad del emisor y que él generó el código por el que se auténtica, verifica que el mensaje va dirigido a él y la integridad y originalidad (no haber sido utilizado anteriormente) del código utilizado, todo ello con control de tiempo,
- de dos sentidos (two-way): establece todo lo anterior para códigos generados por los dos corresponsales,
- o de tres sentidos (three-way): incluye una nueva transmisión en la que el emisor devuelve el código generado por el receptor para que éste compruebe su integridad, no haciendo control de tiempo.

[CESID:1997]

(en) strong authentication

The requirement to use multiple factors for authentication and advanced technology, such as dynamic passwords or digital certificates, to verify an entity's identity. [CNSSI_4009:2010]

2.115.3 (EN) STRONG AUTHENTICATION

Authentication by means of cryptographically derived credentials. [X.509:2005]

2.115.4 (FR) AUTHENTIFICATION FORTE

authentification utilisant des justificatifs obtenus par des moyens de chiffrement. [X.509:2005]

2.116 AUTENTICACIÓN MULTIFACTOR

Ver:

- *Autenticador*

2.116.1 AUTENTICACIÓN MULTIFACTOR

Autenticación multifactor Autenticación utilizando dos o más factores. Por ejemplo:

- (i) algo que se sabe (como una contraseña o un PIN)
- (ii) algo que se tiene (como un dispositivo criptográfico de identificación) o
- (iii) algo que se es (o sea, características biométricas).

2.116.2 (EN) MULTI-FACTOR

A characteristic of an authentication system or a token that uses more than one authentication factor.

The three types of authentication factors are something you know, something you have, and something you are.

[NIST-SP800-63:2013]

2.116.3 (EN) MULTIFACTOR AUTHENTICATION

Authentication using two or more factors to achieve authentication. Factors include:

- (i) something you know (e.g. password/PIN);

- (ii) something you have (e.g., cryptographic identification device, token); or
- (iii) something you are (e.g., biometric).

[NIST-SP800-53:2013]

2.117 AUTENTICACIÓN SIMPLE

Ver:

- *Autenticación*
- *Autenticación fuerte*

2.117.1 AUTENTICACIÓN SIMPLE

Autenticación por medio de arreglos de contraseñas simples. [X.509:2005]

2.117.2 (EN) SIMPLE AUTHENTICATION

Authentication by means of simple password arrangements. [X.509:2005]

2.117.3 (FR) AUTHENTIFICATION SIMPLE

authentification utilisant de simples accords de mot de passe. [X.509:2005]

2.118 AUTENTICADOR

Ver:

- *Autenticación*
- *Autenticación multifactor*

2.118.1 AUTENTICADOR

Término en desuso (por el motivo expuesto en autenticación) referido a la integridad de los datos. Es preferible el empleo de los vocablos sinónimos abajo indicados. [Ribagorda:1997]

2.118.2 (EN) AUTHENTICATOR

The means used to confirm the identity of a user, processor, or device (e.g., user password or token). [NIST-SP800-53:2013]

2.118.3 (EN) AUTHENTICATOR

The means used to confirm the identity of a user, process, or device (e.g., user password or token). [CNSSI_4009:2010]

2.119 AUTENTICAR

Ver:

- *Autenticación*

2.119.1 AUTENTICAR

(De auténtico).

- Autorizar o legalizar algo.
- Acreditar; dar fe de la verdad de un hecho o documento con autoridad legal.

2.119.2 (EN) AUTHENTICATE

To verify the identity of a user, user device, or other entity. [CNSSI_4009:2010]

2.119.3 (EN) AUTHENTICATE

(I) Verify (i.e., establish the truth of) an attribute value claimed by or for a system entity or system resource. (See: authentication, validate vs. verify, "relationship between data integrity service and authentication services" under "data integrity service".) [RFC4949:2007]

2.119.4 (EN) AUTHENTICATE

To verify the identity of a user, device, or othe r entity in a computer system, often as a prerequisite to allowin g access to resources in a system. [IRM-5239-8:1995]

2.119.5 (EN) AUTHENTICATE

To establish the validity of a claimed identity. [TCSEC:1985]

2.120 AUTENTICIDAD

Ver:

- *Autenticación*

2.120.1 AUTÉNTICO

Certificación con que se testifica la identidad y verdad de algo.

DRAE. Diccionario de la Lengua Española.

2.120.2 AUTENTICIDAD

Propiedad consistente en que una entidad es lo que dice ser [UNE-ISO/IEC 27000:2014]

2.120.3 AUTENTICIDAD

Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE-71504:2008]

2.120.4 (EN) AUTHENTICITY

The quality of being genuine or true.

Oxford Advanced Learner's Dictionary.

2.120.5 (EN) AUTHENTICITY

property that an entity is what it claims to be [ISO/IEC 27000:2014]

2.120.6 (EN) AUTHENTICITY

(I) The property of being genuine and able to be verified and be trusted.

(See: authenticate, authentication, validate vs. verify.)

[RFC4949:2007]

2.120.7 (EN) AUTHENTICITY

The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. [NIST-SP800-53:2013]

2.120.8 (EN) AUTHENTICITY

Having an undisputed identity or origin.

http://www.ioss.gov/docs/definitions.html

2.120.9 (EN) AUTHENTICITY

The property of being genuine and able to be verified and be trusted. [NIST-SP800-60V2:2004]

2.120.10 (EN) AUTHENTICITY

Authenticity is the validity and conformance of the original information.

http://www.sans.org/security-resources/glossary-of-terms/

2.120.11 (FR) AUTHENTICITÉ

La propriété qui assure de l'identité d'un sujet ou d'une ressource qui est bien celle pour laquelle elle est clamée et s'applique aux entités telles que les utilisateurs, les process, les systèmes et les informations. [ISO-7498-2:1989]

2.121 AUTENTICIDAD DEL ORIGEN DE LA INFORMACIÓN

Ver:

- *Datos*
- *Autenticación*

2.121.1 AUTENTICACIÓN DE ORIGEN DE DATOS

Comprobación de que la fuente de los datos recibidos es la alegada (ISO-7498-2) [Ribagorda:1997]

2.121.2 AUTENTICACIÓN DEL ORIGEN DE LOS DATOS

Confirmación de que la fuente de los datos recibidos es la alegada. [ISO-7498-2:1989]

2.121.3 (EN) DATA ORIGIN AUTHENTICATION

The process of verifying that the source of the data is as claimed and that the data has not been modified. [CNSSI_4009:2010]

2.121.4 (EN) DATA ORIGIN AUTHENTICATION

(I) "The corroboration that the source of data received is as claimed." [ISO-7498-2] (See: authentication.) [RFC4949:2007]

2.121.5 (EN) DATA ORIGIN AUTHENTICATION

corroboration that the source of data received is as claimed. [ISO-18028-2:2006]

2.121.6 (EN) DATA ORIGIN AUTHENTICATION

The verification that the source of data received is as claimed. [NIST-SP800-33:2001]

2.121.7 (EN) DATA ORIGIN AUTHENTICATION

corroboration that the source of data received is as claimed. [ISO-7498-2:1989]

2.121.8 (FR) AUTHENTIFICATION DE L'ORIGINE DES DONNEES

Confirmation que la source des données reçues est telle que déclarée. [ISO-7498-2:1989]

2.122 AUTORIDAD

Ver:

- *Autoridad de certificación (AC)*
- *Autoridad de atributo*
- *Autoridad de registro*
- *Autoridad de validación*

2.122.1 AUTORIDAD

Entidad responsable de la expedición de certificados. En esta Especificación se definen dos tipos; la autoridad de certificación que expide certificados de clave pública y la autoridad de atributo que expide certificados de atributo. [X.509:2005]

2.122.2 (EN) AUTHORITY

An entity, responsible for the issuance of certificates. Two types are defined in this Specification; certification authority which issues public-key certificates and attribute authority which issues attribute certificates. [X.509:2005]

2.122.3 (FR) AUTORITÉ

entité responsable de l'émission de certificats. La présente Spécification définit les deux types suivants: les autorités de certification émettant des certificats de clé publique et les autorités d'attribut émettant des certificats d'attribut. [X.509:2005]

2.123 AUTORIDAD DE ATRIBUTO

Acrónimos: AA

Ver:

- *Autoridad*
- *Certificado de atributo*
- *Autoridad de certificación (AC)*

2.123.1 AUTORIDAD DE ATRIBUTO

Una AA es una entidad autorizada para emitir certificados de atributos.

2.123.2 AUTORIDAD DE ATRIBUTO (AA, ATTRIBUTE AUTHORITY)

Autoridad que asigna privilegios expidiendo certificados de atributo. [X.509:2005]

2.123.3 (EN) ATTRIBUTE AUTHORITY (AA)

1. (N) A CA that issues attribute certificates.

2. (O) "An authority [that] assigns privileges by issuing attribute certificates." [X509]

[RFC4949:2007]

2.123.4 (EN) ATTRIBUTE AUTHORITY

An authority which assigns privileges by issuing attribute certificates. [X.509:2005]

2.123.5 (EN) ATTRIBUTE AUTHORITY (AA)

An entity trusted by one or more entities to create and sign attribute certificates. Note that a CA may also be an AA. [ISO-14516:2002]

2.123.6 (FR) AUTORITÉ D'ATTRIBUT (AA)

autorité qui attribue des privilèges par l'émission de certificats d'attribut. [X.509:2005]

2.124 AUTORIDAD DE CERTIFICACIÓN (AC)

Acrónimos: AC (es), AC (fr), CA

Ver:

- *Certificado X.509*
- *Autoridad*
- *Tercera parte de confianza*

2.124.1 AUTORIDAD DE CERTIFICACIÓN

Entidad perteneciente a un Prestador de Servicios de Certificación encargada, fundamentalmente, de la emisión de certificados electrónicos. En una estructura jerárquica de autoridades de certificación (PKI jerárquica), la que inicia la jerarquía es la autoridad de certificación **raíz**, y las que actúan bajo ella se denominan autoridades de certificación **subordinadas**. [CCN-STIC-405:2006]

2.124.2 AUTORIDAD DE CERTIFICACIÓN

Autoridad a la cual uno o más usuarios han confiado la creación y asignación de certificados de clave pública. Facultativamente, la autoridad de certificación puede crear las claves de los usuarios. [X.509:2005]

2.124.3 AUTORIDAD DE CERTIFICACIÓN (AC)

Autoridad confiable para uno o más usuarios, que crea y asigna certificados. Opcionalmente, la Autoridad de Certificación puede también crear claves criptográficas de usuario (ISO/IEC 9594-8, ITU-T X.509). [Ribagorda:1997]

2.124.4 AUTORIDAD DE CERTIFICACIÓN

Centro confiable para dos o más entidades para la creación y asignación de certificados. [CE-SID:1997]

2.124.5 AUTORIDAD DE CERTIFICACIÓN

Una autoridad que es confiable (en el contexto de una política de seguridad) para crear certificados de seguridad que contienen una o más clases de datos pertinentes a la seguridad. [X.810:1995]

2.124.1 (EN) CERTIFICATION AUTHORITY (CA)

1. For Certification and Accreditation (C&A) (C&A Assessment): Official responsible for performing the comprehensive evaluation of the security features of an information system and determining the degree to which it meets its security requirements.

2. For Public Key Infrastructure (PKI): A trusted third party that issues digital certificates and verifies the identity of the holder of the digital certificate

[CNSSI_4009:2010]

2.124.2 (EN) CERTIFICATION AUTHORITY (CA)

1. (I) An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.

2. (O) "An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the user's keys." [X509]

[RFC4949:2007]

2.124.3 (EN) CERTIFICATION AUTHORITY

The entity in a Public Key Infrastructure (PKI) that is responsible for issuing certificates, and exacting compliance to a PKI policy. [NIST-SP800-57:2007]

2.124.4 (EN) CERTIFICATION AUTHORITY

authority trusted by one or more users to create and assign public-key certificates

NOTE. Optionally, the certification authority may create the user' keys.

[ISO-9594-8:2005]

2.124.5 (EN) CERTIFICATION AUTHORITY

A CA is an authority trusted by one or more users to create and assign public-key certificates. Optionally the certification authority may create the users' keys. [X.509:2005]

2.124.6 (EN) CERTIFICATION AUTHORITY

An entity that is trusted (in the context of a security policy) to create security certificates containing one or more classes of security-relevant data. [X.810:1995]

2.124.7 (FR) AUTORITÉ DE CERTIFICATION

autorité jouissant de la confiance d'un ou de plusieurs utilisateurs pour la création et l'attribution de certificats. L'autorité de certification peut, de manière optionnelle, créer les clés des utilisateurs. [X.509:2005]

2.124.8 (FR) AUTORITÉ DE CERTIFICATION

entité habilitée à laquelle il est fait confiance (dans le contexte d'une politique de sécurité) pour créer des certificats de sécurité contenant une ou plusieurs classes de données relatives à la sécurité. [X.810:1995]

2.124.9 (FR) AC (AUTORITE DE CERTIFICATION)

Organisation en charge de la gestion des certificats électroniques dans le cadre d'une PKI (Public Key Infrastructure) / ICP (Infrastructure à Clé Publique). On parlera également de "tiers de confiance".

http://www.cases.public.lu/functions/glossaire/

2.124.10 (FR) AUTORITE DE CERTIFICATION

Autorité chargée par un ou plusieurs utilisateurs de créer et d'attribuer des certificats. Cette autorité peut, facultativement, créer des clés d'utilisateur. [X.509:2005]

2.125 AUTORIDAD DE CERTIFICACIÓN RAÍZ

Ver:

- *Autoridad de certificación (AC)*

2.125.1 AUTORIDAD DE CERTIFICACIÓN RAÍZ

En una estructura jerárquica de infraestructura de clave pública, es la autoridad de certificación origen de las rutas de confianza. Es decir, el origen de la confianza.

2.125.2 (EN) ROOT CERTIFICATION AUTHORITY

In a hierarchical Public Key Infrastructure, the Certification Authority whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain. [CNSSI_4009:2010]

2.126 AUTORIDAD DE DOMINIO DE SEGURIDAD

Ver:

- *Dominio de seguridad*
- *Autoridad de seguridad*

2.126.1 AUTORIDAD DE DOMINIO DE SEGURIDAD

Autoridad de seguridad que es responsable de la aplicación de una política de seguridad para un dominio de seguridad. [X.810:1995]

2.126.2 (EN) SECURITY DOMAIN AUTHORITY

A security authority that is responsible for the implementation of a security policy for a security domain. [X.810:1995]

2.126.3 (FR) AUTORITE DU DOMAINE DE SECURITE

autorité de sécurité qui est responsable de la mise en oeuvre d'une politique de sécurité pour un domaine de sécurité. [X.810:1995]

2.127 AUTORIDAD DE EVALUACIÓN

Ver:

- *Criterios comunes*

2.127.1 AUTORIDAD DE EVALUACIÓN

Organismo que implementa los CC para una comunidad específica mediante un esquema de evaluación por el que se establecen las normas y se supervisa la calidad de las evaluaciones realizadas por organismos de dicha comunidad. [CC:2006]

2.127.2 (EN) EVALUATION AUTHORITY

a body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community. [CC:2006]

2.128 AUTORIDAD DE REGISTRO

Acrónimos: RA

Ver:

- *Entidad final*
- *Infraestructura de clave pública*
- http://www.ietf.org/rfc/rfc4210

2.128.1 AUTORIDAD DE REGISTRO

Componente opcional dentro de una PKI. Ayuda a la autoridad de certificación en sus relaciones con la entidad final: identificación del titular, distribución de certificados y distribución de CRL.

2.128.2 (EN) REGISTRATION AUTHORITY (RA)

A trusted entity that establishes and vouches for the identity of a subscriber to a Credentials Service Provider (CSP). The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s). [CNSSI_4009:2010]

2.128.3 (EN) REGISTRATION AUTHORITY (RA)

1. (I) An optional PKI entity (separate from the CAs) that does not sign either digital certificates or CRLs but has responsibility for recording or verifying some or all of the information (particularly the identities of subjects) needed by a CA to issue certificates and CRLs and to perform other certificate management functions. (See: ORA, registration.)

2. (I) /PKIX/ An optional PKI component, separate from the CA(s). The functions that the RA performs will vary from case to case but may include identity authentication and name assignment, key generation and archiving of key pairs, token distribution, and revocation reporting. [R4210]

[RFC4949:2007]

2.128.4 (EN) REGISTRATION AUTHORITY

A trusted entity that establishes and vouches for the identity of a user. [NIST-SP800-57:2007]

2.128.5 (FR) AUTORITÉ D'ENREGISTREMENT

Composante d'une infrastructure de gestion de clés qui vérifie les données propres au demandeur ou porteur de certificat ainsi que les contraintes liées à l'usage d'un certificat, conformément à la politique de certification. L'autorité d'enregistrement dépend directement d'au moins une autorité de certification (SCSSI, PC2 v2.0). L'autorité d'enregistrement est l'interface entre l'utilisateur et l'autorité de certification. Elle joue les rôles suivants:

- Authentification des demandeurs ou porteurs de certificats.
- Application de la politique de certification vis-à-vis des requêtes des utilisateurs.
- Récupération de la clé publique du demandeur.
- Soumission des demandes de certificats à l'autorité de certification.

http://securit.free.fr/glossaire.htm

2.129 AUTORIDAD DE SEGURIDAD

2.129.1 AUTORIDAD DE SEGURIDAD

Entidad que es responsable de la definición, aplicación o cumplimiento de la política de seguridad. [X.810:1995]

2.129.2 (EN) SECURITY AUTHORITY

The entity accountable for the administration of a security policy within a security domain. [ISO-15816:2002]

2.129.3 (EN) SECURITY AUTHORITY

An entity that is responsible for the definition, implementation or enforcement of security policy. [X.810:1995]

2.129.4 (FR) AUTORITÉ DE SÉCURITÉ

entité qui est responsable de la définition, de la mise en oeuvre ou de l'application de la politique de sécurité. [X.810:1995]

2.130 AUTORIDAD DE SELLADO DE TIEMPO

Acrónimos: TSA

Ver:

- *Sello de tiempo*

2.130.1 AUTORIDAD DE SELLADO DE TIEMPO

Tercera parte confiable para prestar servicios de fechado electrónico.

[traducción de ISO/IEC 18014-1]

2.130.2 (EN) TIME-STAMPING AUTHORITY (TSA)

trusted third party trusted to provide a time-stamping service.

[ISO-18014-1:2002]

2.130.3 (EN) TIME-STAMPING AUTHORITY

A trusted third party trusted to provide evidence which includes the time when the secure time stamp is generated. [ISO-13888-1:2004]

2.131 AUTORIDAD DE VALIDACIÓN

Acrónimos: VA

Ver:

- *Autoridad*

- *Autoridad de certificación (AC)*

2.131.1 AUTORIDADES DE VALIDACIÓN

La Autoridad de Validación es el componente que tiene como tarea suministrar información sobre la vigencia de los certificados electrónicos que, a su vez, hayan sido registrados por una Autoridad de Registro y certificados por la Autoridad de Certificación.

http://www.dnielectronico.es/Autoridades_de_Validacion/

2.131.2 (EN) VALIDATION AUTHORITY

As part of the Public Key Infrastructure, the VA is a body that checks the validity of a electronic certificate by referring to a list of invalid certificates, and it confirms whether the electronic certificate was issued by a sufficiently trustworthy Certification Authority.

http://www.sdl.hitachi.co.jp/english/glossary/v/validation_authority.html

2.132 AUTORIZACIÓN

Ver:

- *AAA - Autenticación, Autorización y Registro*

2.132.1 AUTORIZACIÓN

En el contexto del control de acceso, la autorización es el otorgamiento de derechos de acceso u otros derechos similares a un usuario, programa o proceso. La autorización define lo que un individuo o programa puede hacer después de un proceso de autenticación satisfactorio.

En lo que se refiere a una transacción con tarjeta de pago, la autorización ocurre cuando un comerciante recibe la aprobación de la transacción después de que el adquirente valide la transacción con el emisor/procesador.

http://es.pcisecuritystandards.org

2.132.2 AUTORIZACIÓN

Definición granular de permisos de acceso concedidos a un determinado usuario, dispositivo o sistema, habitualmente implementado mediando listas de control de acceso (ACL). [CCN-STIC-400:2006]

2.132.3 AUTORIZACIÓN

1. Concesión o posesión de derechos (ISO-7498-2).

2. Proceso de concesión a una entidad, o sujeto, de los derechos de acceso, completos o restringidos, a un recurso y objeto.

[Ribagorda:1997]

2.132.4 AUTORIZACIÓN

Capacidad que da el administrador de un sistema de información a determinados individuos para aprobar intercambios, procedimientos y sistemas. [CESID:1997]

2.132.5 AUTORIZACIÓN

Atribución de derechos, que incluye la concesión de acceso basada en derechos de acceso.[ISO-7498-2:1989]

2.132.6 (EN) AUTHORIZATION

Granting of access or other rights to a user, program, or process. For a network, authorization defines what an individual or program can do after successful authentication. For the purposes of a payment card transaction authorization occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.132.7 (EN) AUTHORIZATION

Access privileges granted to a user, program, or process or the act of granting those privileges. [CNSSI_4009:2010]

2.132.8 (EN) AUTHORIZATION

1a. (I) An approval that is granted to a system entity to access a system resource. (Compare: permission, privilege.)

Usage: Some synonyms are "permission" and "privilege". Specific terms are preferred in certain contexts:

- /PKI/ "Authorization" SHOULD be used, to align with "certification authority" in the standard [X509].
- /role-based access control/ "Permission" SHOULD be used, to align with the standard [ANSI].
- /computer operating systems/ "Privilege" SHOULD be used, to align with the literature. (See: privileged process, privileged user.)

Tutorial: The semantics and granularity of authorizations depend on the application and implementation (see: "first law" under "Courtney's laws"). An authorization may specify a particular access mode -- such as read, write, or execute -- for one or more system resources.

1b. (I) A process for granting approval to a system entity to access a system resource.

2. (O) /SET/ "The process by which a properly appointed person or persons grants permission to perform some action on behalf of an organization. This process assesses transaction risk, confirms that a given transaction does not raise the account holder's debt above the account's credit limit, and reserves the specified amount of credit. (When a merchant obtains authorization, payment for the authorized amount is guaranteed -- provided, of course, that the merchant followed the rules associated with the authorization process.)" [SET2]

[RFC4949:2007]

2.132.9 (EN) AUTHORIZATION

Access privileges that are granted to an entity; conveying an official sanction to perform a security function or activity. [NIST-SP800-57:2007]

2.132.10 (EN) AUTHORISED USER

a user who may, in accordance with the SFRs, perform an operation.

SFR - Security Functional Requirement

[CC:2006]

2.132.11 (EN) AUTHORISATION

The granting of permission on the basis of authenticated identification. [H.235:2005]

2.132.12 (EN) AUTHORIZATION

The granting or denying of access rights to a user, program, or process. [NIST-SP800-27:2004]

2.132.13 (EN) AUTHORIZATION

The granting or denying of access rights to a user, program, or process. [NIST-SP800-33:2001]

2.132.14 (EN) AUTHORIZATION

The granting of rights, which includes the granting of access based on access rights. [ISO-7498-2:1989]

2.132.15 (EN) AUTHORIZED PERSON

A person who has a need-to-know for classified information in the performance of official duties and who has been granted a PCL at the required level. [DoD 5220:2006]

2.132.16 (EN) AUTHORIZATION

Authorization is the approval, permission, or empowerment for someone or something to do something.

http://www.sans.org/security-resources/glossary-of-terms/

2.132.17 (EN) AUTHORIZATION

Authorization is the process of giving someone permission to do or have something. In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use (such as access to which file directories, hours of access, amount of allocated storage space, and so forth). Assuming that someone has logged in to a computer operating system or application, the system or application may want to identify what resources the user can be given during this session. Thus, authorization is sometimes seen as both the preliminary setting up of permissions by a system administrator and the actual checking of the permission values that have been set up when a user is getting access.

http://searchsecurity.techtarget.com/

2.132.18 (FR) AUTORISATION

Attribution de droits, comprenant la permission d'accès sur la base de droits d'accès. [ISO-7498-2:1989]

2.132.19 (FR) AUTORISATION

Dans le contexte du contrôle d'accès, l'autorisation est la concession d'un droit d'accès ou d'autres droits à un utilisateur, programme ou processus. L'autorisation définit ce qu'une personne ou un programme peuvent effectuer après une authentification réussie.

Dans le cadre d'une transaction par carte de paiement, l'autorisation est donnée lorsque le commerçant reçoit l'approbation de la transaction une fois que l'acquéreur a validé la transaction avec l'émetteur/le processeur.

http://fr.pcisecuritystandards.org/

2.132.20 (FR) AUTORISATION

Service de sécurité visant à déterminer les droits d'une entité (utilisateur ou équipement) sur une ressource informatique (ex.: permissions sur un fichier). En général, ce service est lié avec le service d'authentification.

http://securit.free.fr/glossaire.htm

2.133 AUTORIZACIÓN PARA OPERAR

Ver:

- *Autorización*

2.133.1 AUTORIZACIÓN PARA OPERAR

Decisión formal de la autoridad por la que se autoriza la entrada en producción de un sistema de información, aceptando el riesgo residual al que esté expuesta.

2.133.2 (EN) AUTHORIZATION (TO OPERATE)

The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. [NIST-SP800-53:2013]

2.133.3 (EN) AUTHORIZATION BOUNDARY

All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected. [NIST-SP800-53:2013]

2.133.4 (EN) AUTHORIZING OFFICIAL

A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. [NIST-SP800-53:2013]

2.133.1 (EN) APPROVAL TO OPERATE (ATO)

The official management decision issued by a DAA or PAA to authorize operation of an information system and to explicitly accept the residual risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. See authorization to operate. [CNSSI_4009:2010]

2.133.2 (EN) AUTHORIZATION (TO OPERATE)

The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. [CNSSI_4009:2010]

2.133.3 (EN) INTERIM APPROVAL TO OPERATE (IATO)

Temporary authorization granted by a DAA for an information system to process information based on preliminary results of a security evaluation of the system. (To be replaced by ATO and POA&M) [CNSSI_4009:2010]

2.134 AUTOSERVICIO DE RECUPERACIÓN DE CONTRASEÑA

Ver:

- *Contraseña*

2.134.1 AUTOSERVICIO DE RECUPERACIÓN DE CONTRASEÑA

Procso que permite a los usuarios recuperar el acceso a un sistema tras haber perdido su contraseña, sin recurrir al centro de ayuda de usuarios.

Es habitual que el usuario proporcione una dirección de correo electrónico a la que le será enviada una contraseña temporal de desbloqueo. Mediante esta contrasñe temporal, y durante un periodo de tiempo reducido, el usuario puede acceder y establecer una nueva contraseña. El acceso al correo electrónico se usa de prueba de autenticidad del usuario.

Otros mecanismos más robustos pueden incluir mecanismos más robustos de autenticación alternativa.

2.134.2 (EN) SELF-SERVICE PASSWORD RESET (SSPR)

is defined as any process or technology that allows users who have either forgotten their password or triggered an intruder lockout to authenticate with an alternate factor, and repair their own problem, without calling the help desk. It is a common feature in identity management software and often bundled in the same software package as a password synchronization capability.

Typically users who have forgotten their password launch a self-service application from an extension to their workstation login prompt, using their own or another user's web browser, or through a telephone call. Users establish their identity, without using their forgotten or disabled password, by answering a series of personal questions, using a hardware authentication token, responding to a password notification e-mail or, less often, by providing a biometric sample. Users can then either specify a new, unlocked password, or ask that a randomly generated one be provided.

Self-service password reset expedites problem resolution for users "after the fact," and thus reduces help desk call volume. It can also be used to ensure that password problems are only resolved after adequate user authentication, eliminating an important weakness of many help desks: social engineering attacks, where an intruder calls the help desk, pretends to be the intended victim user, claims that he has forgotten his password, and asks for a new password.

http://en.wikipedia.org/wiki/Self-service_password_reset

2.135 BACKORIFICE

Ver:

- *Caballo de Troya*

2.135.1 BACKORIFICE

Back Orifice es un programa de control remoto de ordenadores que funciona bajo un servidor y un cliente. Si colocamos el servidor a otro ordenador remoto, es posible desde el cliente, gobernar cualquier función del ordenador remoto, entre los que destaca abrir y cerrar programas, controlar el CD, leer y modificar ficheros o borrar parte del disco duro. Para ello el servidor se autoejecuta y se borra cada vez que el ordenador ajeno se enciende, nuestro cliente escanea el puerto elegido y cuando este esta abierto actúa a través de él, desde un menú repleto de pestañas y opciones de control remoto. El sistema es bueno para controlar un ordenador u ordenadores dentro de nuestra red LAN, aunque dejar este puerta abierta para Windows es toda una amenaza.

http://es.wikipedia.org/wiki/Back_Orifice

2.135.2 (EN) BACKORIFICE

Back Orifice (often shortened to BO) is a controversial computer program designed for remote system administration. It enables a user to control a computer running the Microsoft Windows operating system from a remote location. The name is a pun on Microsoft BackOffice Server software.

Although Back Orifice has legitimate purposes, such as remote administration, there are other factors that make it suited for less benign business. The server can hide itself from cursory looks by users of the system. If wrapped inside a Trojan horse, it can be installed without trouble and used as an attack point or just to spy on or harass the unsuspecting user.

For those and other reasons, the antivirus industry immediately categorized the tool as malware and appended Back Orifice to their quarantine lists. Despite this fact, it was widely used by script kiddies because of its simple UI and ease of installation.

http://en.wikipedia.org/wiki/Back_Orifice

2.135.3 (EN) BACKORIFICE

A Trojan horse that installs itself as a server on a machine, and allows a user with the BackOrifice client to control the host remotely. Hackers often distribute seemingly harmless executables that also install BackOfifice. Once installed, a hacker can access all files, system passwords, key-strokes, ad other confidential information to further compromise the network.

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.136 BARRIDO DE PUERTOS

Ver:

- *Barrido IP*

2.136.1 ESCANEAR - PUERTOS, DIRECCIONES IP

Acción por la cual se chequean los puertos de comunicaciones y/o las direcciones IP de un ordenador, para localizarlos y obtener información sobre su estado.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.136.2 (EN) PORT SCANNING

Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports). [CNSSI_4009:2010]

2.136.3 (EN) SCANNING

Sending packets or requests to another system to gain information to be used in a subsequent attack. [CNSSI_4009:2010]

2.136.4 (EN) PORT SCAN

(I) A technique that sends client requests to a range of service port addresses on a host. (See: probe. Compare: ping sweep.) [RFC4949:2007]

2.136.5 (EN) PORT SCANNING

Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports). [NIST-SP800-61:2004]

2.136.6 (EN) PORT SCAN

A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well known" port number, the computer

provides. Port scanning, a favorite approach of computer cracker, gives the assailant an idea where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness.

http://www.sans.org/security-resources/glossary-of-terms/

2.136.7 (FR) PORT SCANNING

Opération consistant à passer en revue tous les ports d'une machine connectée à un réseau pour déterminer quels sont les ports ouverts et pour lesquels une application peut être en attente de données réseau. Le port scanning est souvent une étape préliminaire pour la recherche et la détection de vulnérabilités. Le port scanning est aussi bien utilisé par des pirates informatiques que par des administrateurs systèmes et réseaux mais dans des buts différents. Les premiers pour disposer d'informations pour mener des attaques, les seconds pour sécuriser leurs systèmes d'information et de communication.

http://www.cases.public.lu/functions/glossaire/

2.137 BARRIDO IP

Ver:

- *Barrido de puertos*

2.137.1 ESCANEAR - PUERTOS, DIRECCIONES IP

Acción por la cual se chequean los puertos de comunicaciones y/o las direcciones IP de un ordenador, para localizarlos y obtener información sobre su estado.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.137.2 (EN) PING SWEEP

(I) An attack that sends ICMP echo requests ("pings") to a range of IP addresses, with the goal of finding hosts that can be probed for vulnerabilities.

(See: ping of death. Compare: port scan.)

[RFC4949:2007]

2.138 BASE DE DATOS DE GESTIÓN DE LA CONFIGURACIÓN (CMDB)

Acrónimos: CMDB

Ver:

- *Configuración*

2.138.1 BASE DE DATOS DE GESTIÓN DE LA CONFIGURACIÓN (CMDB)

(Transición del Servicio) Base de Datos usada para almacenar Registros de Configuración durante todo su Ciclo de Vida. El Sistema de Gestión de la Configuración mantiene una o más CMDBs, y cada CMDB contiene Atributos de CIs, y Relaciones con otros CIs. [ITIL:2007]

2.138.2 (EN) CONFIGURATION MANAGEMENT DATABASE (CMDB)

(Service Transition) A database used to store Configuration Records throughout their Lifecycle. The Configuration Management System maintains one or more CMDBs, and each CMDB stores Attributes of CIs, and Relationships with other CIs. [ITIL:2007]

2.138.3 (FR) GESTION DES CONFIGURATIONS (CMDB)

(Transition de Services) Base de données servant à rassembler les enregistrements de configuration tout au long de leur cycle de vie. Le système de gestion des configurations tient à jour une ou plusieurs CMDB, chacune d'elles regroupant les attributs des CI, et leurs relations les uns avec les autres. [ITIL:2007]

2.139 BASE FIABLE DE PROCESAMIENTO

Acrónimos: TCB

Ver:

- http://en.wikipedia.org/wiki/Trusted_computing_base

2.139.1 BASE FIABLE DE CÁLCULO

En la terminología del TCSEC (libro naranja) estadounidense, mecanismos de protección, sean físicos, lógicos o ambos, que son responsables de la seguridad del sistema. [Ribagorda:1997]

2.139.2 (EN) TRUSTED COMPUTING BASE (TCB)

Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination responsible for enforcing a security policy. [CNSSI_4009:2010]

2.139.3 (EN) TRUSTED COMPUTING BASE (TCB)

(N) "The totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy." [NCS04]

(See: "trusted" under "trust". Compare: TPM.)

[RFC4949:2007]

2.139.4 (EN) TRUSTED COMPUTING BASE

The totality of protection mechanisms within a computer system -- including hardware, firmware, and software -- the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a trusted computing base to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy. [TCSEC:1985]

2.140 BASTIÓN

Ver:

- *Fortificar*
- *Bastionado*

2.140.1 BASTIÓN

Equipos de frontera que, situados fuera de la red interna, ofrecen servicios al exterior. Equipos hacen virtud de la necesidad de estar bien asegurados pues están muy expuestos a ataques externos.

Se dice que un equipo está "fortificado" cuando se le han aplicado todas las protecciones conocidas, de forma que no adolece de ninguna vulnerabilidad conocida.

2.140.2 (EN) BASTION HOST

A special purpose computer on a network specifically designed and configured to withstand attacks. [CNSSI_4009:2010]

2.140.3 (EN) BASTION HOST

(I) A strongly protected computer that is in a network protected by a firewall (or is part of a firewall) and is the only host (or one of only a few) in the network that can be directly accessed from networks on the other side of the firewall.

(See: firewall.)

[RFC4949:2007]

2.140.4 (EN) BASTION HOST

A computer placed outside a firewall to provide public services (such as World Wide Web access and FTP) to other Internet sites, hardened to withstand whatever attacks the Internet can throw at it.

Hardening is accomplished by making the box as single-purpose as possible, removing all unneeded services and potential security vulnerabilities. Bastion host is sometimes inaccurately generalized to refer to any host critical to the defense of a local network.

http://www.watchguard.com/glossary/

2.140.5 (EN) BASTION HOST

A bastion host has been hardened in anticipation of vulnerabilities that have not been discovered yet.

http://www.sans.org/security-resources/glossary-of-terms/

2.140.6 (FR) BASTION

Système sécurisé dans le but de supporter une application ou un service critique (ex.: firewall, serveur Web).

http://securit.free.fr/glossaire.htm

2.141 BASTIONADO

Ver:

- *Bastión*
- *Fortificar*

2.141.1 BASTIONADO

Implementar todas las medidas de seguridad posibles para proteger un sistema.

2.141.2 (EN) HARDEN

(I) To protect a system by configuring it to operate in a way that eliminates or mitigates known vulnerabilities. Example: [RSCG].

(See: default account.)

[RFC4949:2007]

2.141.3 (EN) HARDENING

Hardening is the process of identifying and fixing vulnerabilities on a system.

http://www.sans.org/security-resources/glossary-of-terms/

2.142 BASURA (BUSCAR ENTRE LA)

Ver:

- *Restos (buscar entre los)*

2.142.1 BASURA (BUSCAR ENTRE LA)

Obtención de información a base de rebuscar en los cubos de basura.

2.142.2 (EN) DUMPSTER DIVING

A method of social engineering in which criminals raid rubbish bins to gather telling personal information.

http://www.getsafeonline.org/

2.142.3 (EN) DUMPSTER DIVING

Dumpster Diving is obtaining passwords and corporate directories by searching through discarded media.

http://www.sans.org/security-resources/glossary-of-terms/

2.142.4 (EN) DUMPSTER DIVING

Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't

limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network. To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash.

http://searchsecurity.techtarget.com/

2.143 BASURING EN MEMORIA

Ver:

- *Restos (buscar entre los)*
- *Basura (buscar entre la)*

2.143.1 BASURING EN MEMORIA

Acceso a información residual en la memoria de los dispositivos o sistemas con el ánimo de acceder a secretos.

2.143.2 (EN) MEMORY SCAVENGING

The collection of residual information from data storage. [CNSSI_4009:2010]

2.144 BER - BASIC ENCODING RULES

Acrónimos: BER

Ver:

- *ASN.1 - Abstract Syntax Notation One*
- *CER - Canonical Encoding Rules*
- *DER - Distinguished Encoding Rules*
- *PER - Packet Encoding Rules*
- *XER - XML Encoding Rules*

2.144.1 BER - BASIC ENCODING RULES

Conjunto de reglas para formatear en binario datos descritos en ASN.1.

http://es.wikipedia.org/wiki/BER

2.144.2 (EN) BER - BASIC ENCODING RULES

a set of ASN.1 encoding rules for formatting data in binary.

http://en.wikipedia.org/wiki/Basic_Encoding_Rules

2.145 BIG ENDIAN

Ver:

- *Little endian*

2.145.1 BIG ENDIAN

Ordenación de los bytes en memoria: byte más significativo primero.

2.145.2 (EN) BIG ENDIAN

Byte ordering in RAM: the most significant byte is at the lowest address.

2.145.3 (EN) BIG-ENDIAN

a method of storage of multi-byte numbers with the most significant bytes at the lowest memory addresses. [ISO-10118-1:2000]

2.146 BIOMETRÍA

2.146.1 DISPOSITIVO BIOMÉTRICO

Dispositivo que utiliza parámetros biológicos característicos de las personas como la huella dactilar, el iris del ojo o la voz para la autenticación. [CCN-STIC-430:2006]

2.146.2 BIOMÉTRICO

Procedimiento de autenticación basado en la medición de alguna característica física o biológica de una persona. Por extensión, también se aplica a la autenticación mediante la comprobación de algún hábito o rasgo personal de un individuo. Por ejemplo, en sentido estricto son procedimientos biométricos: el reconocimiento de la huella dactilar, de la geometría de la mano, del patrón de venas del fondo del ojo, de la voz, de la faz, etc. En el sentido más lato, citado arriba, también lo son: la verificación de la firma autógrafa, de la cadencia y presión de las pulsaciones del teclado, etc. [Ribagorda:1997]

2.146.3 (EN) BIOMETRICS

The process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics. [JP2-0:2013]

2.146.4 (EN) BIOMETRICS

Automated recognition of individuals based on their behavioral and biological characteristics.

In this document, biometrics may be used to unlock authentication tokens and prevent repudiation of registration.

[NIST-SP800-63:2013]

2.146.1 (EN) BIOMETRICS

Measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity, of an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics. [CNSSI_4009:2010]

2.146.2 (EN) BIOMETRIC AUTHENTICATION

(I) A method of generating authentication information for a person by digitizing measurements of a physical or behavioral characteristic, such as a fingerprint, hand shape, retina pattern, voiceprint, handwriting style, or face. [RFC4949:2007]

2.146.3 (EN) BIOMETRICS

Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes.

http://searchsoftwarequality.techtarget.com/glossary/

2.146.4 (EN) BIOMETRIC VERIFICATION

Biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. Unique identifiers include fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures. The oldest form of biometric verification is fingerprinting. Historians have found examples of thumbprints being used as a means of unique identification on clay seals in ancient China. Biometric verification has advanced considerably with the advent of computerized databases and the digitization of analog data, allowing for almost instantaneous personal identification.

Iris-pattern and retina-pattern authentication methods are already employed in some bank automatic teller machines. Voice waveform recognition, a method of verification that has been used for many years with tape recordings in telephone wiretaps, is now being used for access to proprietary databanks in research facilities. Facial-recognition technology has been used by law enforcement to pick out individuals in large crowds with considerable reliability. Hand geometry is being used in industry to provide physical access to buildings. Earlobe geometry has been used to disprove the identity of individuals who claim to be someone they are not (identity theft). Signature comparison is not as reliable, all by itself, as the other biometric verification methods but offers an extra layer of verification when used in conjunction with one or more other methods.

http://searchsoftwarequality.techtarget.com/glossary/

2.146.5 (EN) BIOMETRICS-ENABLED INTELLIGENCE

The intelligence derived from the processing of biologic identity data and other all-source for information concerning persons of interest. Also called BEI. [JP2-0:2013]

2.146.6 (FR) BIOMÉTRIE

Technologie d' authentification portant sur les caractéristiques biologiques propres et uniques à chaque être humain comme par exemple les empreintes digitales ou l'image rétinienne.

http://www.cases.public.lu/functions/glossaire/

2.146.7 (FR) BIOMÉTRIE

La biométrie permet d'authentifier un individu sur la base de ces caractères physiologiques (ex.: empreintes digitales ou rétinienne) ou traits comportementaux (ex.: fréquence ou pression de frappe sur un clavier).

http://securit.free.fr/glossaire.htm

2.147 BLOWFISH

Ver:

- http://www.schneier.com/blowfish.html
- *Twofish*

2.147.1 BLOWFISH

Blowfish es un codificador de bloques simétricos, diseñado por Bruce Schneier en 1993 e incluido en un gran número de conjuntos de codificadores y productos de cifrado. Mientras que ningún analizador de cifrados de Blowfish efectivo ha sido encontrado hoy en día, se ha dado más atención de la decodificación de bloques con bloques más grandes, como AES y Twofish.

http://es.wikipedia.org/wiki/Blowfish

2.147.2 (EN) BLOWFISH

(N) A symmetric block cipher with variable-length key (32 to 448 bits) designed in 1993 by Bruce Schneier as an unpatented, license-free, royalty-free replacement for DES or IDEA. [Schn]

(See: Twofish.)

[RFC4949:2007]

2.147.3 (EN) BLOWFISH

Blowfish is a keyed, symmetric block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. While no effective cryptanalysis of Blowfish has been found to date, more attention is now given to block ciphers with a larger block size, such as AES or Twofish.

http://en.wikipedia.org/wiki/Blowfish_%28cipher%29

2.147.4 (FR) BLOWFISH

Blowfish est un algorithme de chiffrement candidat à l'AES, proposé par Bruce Schneier (auteur du fameux "Applied cryptography). Il s'agit d'un algorithme de chiffrement symétrique par blocs (bloc cipher), utilisant une clé symétrique de taille variable (de 32 à 448 bits).

http://securit.free.fr/glossaire.htm

2.148 BOMBA LÓGICA

Ver:

- *Código dañino*

2.148.1 BOMBA LÓGICA

Clase de virus que carece de la capacidad de replicación y que consiste en una cadena de código que se ejecuta cuando una determinada condición se produce, por ejemplo, tras encender el ordenador una serie de veces, o pasados una serie de días desde el momento en que la bomba lógica se instaló en nuestro ordenador.

http://www.inteco.es/glossary/Formacion/Glosario/

2.148.2 BOMBA LÓGICA

Segmento de un programa que comprueba constantemente el cumplimiento de alguna condición lógica (por ejemplo, número de accesos a una parte del disco) o temporal (satisfacción de una cierta fecha). Cuando ello ocurre desencadenen a alguna acción no autorizada. En ocasiones, si la condición a verificar es una cierta fecha, la bomba se denomina temporal. [Ribagorda:1997]

2.148.3 (EN) LOGIC BOMB:

Malware that is designed to initiate a malicious sequence of actions if specified conditions are met

The Tallinn Manual, 2013

2.148.1 (EN) LOGIC BOMB

A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. [CNSSI_4009:2010]

2.148.2 (EN) TIME BOMB

Resident computer program that triggers an unauthorized act at a predefined time. [CNSSI_4009:2010]

2.148.3 (EN) LOGIC BOMB

(I) Malicious logic that activates when specified conditions are met. Usually intended to cause denial of service or otherwise damage system resources. (See: Trojan horse, virus, worm.) [RFC4949:2007]

2.149 BORRADO

Ver:

- *Desmagnetizador*
- *Terminación de soportes de información*
- *Borrado seguro*

2.149.1 BORRADO

Eliminación de la información de un sistema de información, sus equipos de almacenamiento y demás periféricos. El borrado debe ser sistemático y garantizar que la información no es recupe-

rable por medio alguno. Por si fuera posible recuperar información de equipos teóricamente borrados, los soportes de información no deberían ser reutilizados sino con información del mismo nivel o superior.

2.149.2 BORRADO

Proceso que se encarga de eliminar restos de magnetismo en soportes electrónicos de información.

2.149.3 (EN) ERASURE

Process intended to render magnetically stored information irretrievable by normal means. [CNSSI_4009:2010]

2.149.4 (EN) CLEARING

Removal of data from an information system, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (i.e., through the keyboard); however, the data may be reconstructed using laboratory methods. [CNSSI_4009:2010]

2.149.1 (EN) ERASURE

Process intended to render magnetically stored information irretrievable by normal means. [NIST-SP800-88:2006]

2.150 BORRADO SEGURO

2.150.1 LIMPIEZA SEGURA

También llamado "borrado seguro", es un método de sobrescritura de los datos que se encuentran en un disco duro o en otro medio digital, lo que impide la recuperación de los datos.

http://es.pcisecuritystandards.org/

2.150.2 (EN) SECURE WIPE:

Also called “secure delete,” a program utility used to delete specific files permanently from a computer system.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.151 BOTNET

Ver:

- *Zombi*
- *Denegación de servicio distribuida*

2.151.1 BOTNET

Red de equipos infectados por un atacante remoto. Los equipos quedan a su merced cuando desee lanzar un ataque masivo, tal como envío de spam o denegación [distribuida] de servicio.

2.151.2 BOTNET

Conjunto de ordenadores controlados remótamente por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de span, ataques de DDOS, etc.

http://www.inteco.es/glossary/Formacion/Glosario/

2.151.3 BOTNET

El término botnet se refiere a una red de ordenadores que han sido infectados por programas nocivos (virus informáticos). Esta red de ordenadores afectados (zombies) puede ser activada para realizar determinadas acciones como ataques a los sistemas de información (ciberataques). Los zombies pueden ser controlados – con frecuencia sin el conocimiento de los usuarios de los ordenadores afectados – por otro ordenador. El ordenador «controlador» también se conoce como el «centro de dirección y control». Las personas que controlan este centro incurren en una infracción penal, ya que utilizan los ordenadores afectados para lanzar ataques contra los sistemas de información. Es muy difícil rastrear a los autores porque los ordenadores que forman el botnet y realizan el ataque pueden encontrarse en un lugar diferente del propio infractor.

Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a los ataques contra los sistemas de información, por la que se deroga la Decisión marco 2005/222/JAI del Consejo, Bruselas, 30.9.2010, COM(2010) 517 final, 2010/0273 (COD)

2.151.4 (EN) BOTNET

A term derived from “robot network;” is a large automated and distributed network of previously compromised computers that can be simultaneously controlled to launch large-scale attacks such as a denial-of-service attack on selected victims

ISACA, Cybersecurity Glossary, 2014

2.151.5 (EN) BOTNETS

A botnet is a set of compromised computers which are under control of an attacker. These compromised systems are called bots (or ‘zombies’) and they communicate with the bot master that can maliciously direct them. Botnets are multiple usage tools that can be used for spamming, identity theft as well as for infecting other systems and distribute malware.

ENISA Threat Landscape [Deliverable – 2012-09-28]

2.151.6 (EN) BOTNET:

A network of compromised computers, ‘the bots’, remotely controlled by an intruder, ‘the botherder’, used to conduct coordinated cyber operations or cyber crimes. There is no practical limit on the number of bots that can be ‘recruited’ into a botnet.

The Tallinn Manual, 2013

2.151.7 (EN) BOTNET

The term 'botnet' indicates a network of computers that have been infected by malicious software (computer virus). Such a network of compromised computers ('zombies') may be activated to perform specific actions, such as attacking information systems (cyber attacks). These 'zombies' can be controlled – often without the knowledge of the users of the compromised computers – by another computer. This 'controlling' computer is also known as the 'command-and-control centre'. The persons who control this centre are among the offenders, as they use the compromised computers to launch attacks against information systems. It is very difficult to trace the perpetrators, as the computers that make up the botnet and carry out the attack may be in a different location from the offender himself.

Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a los ataques contra los sistemas de información, por la que se deroga la Decisión marco 2005/222/JAI del Consejo, Bruselas, 30.9.2010, COM(2010) 517 final, 2010/0273 (COD)

2.151.1 (EN) BOTNET

A network of compromised computers running malicious programmes under a command and control infrastructure. [CSS NZ:2011]

2.151.2 (EN) BOTNET

A network of infected computers remotely controlled by a hacker, used for malicious activity such as sending out spam or performing Distributed Denial-of-Service (DDoS) attacks. Security experts have detected botnets that included hundreds of thousands of infected computers in a wide variety of countries.

2.151.3 (FR) BOTNET

Ce terme désigne un groupe d'ordinateurs qui ont été contaminés par des logiciels malveillants (virus informatiques). Un tel réseau d'ordinateurs compromis («zombies») peut être activé pour exécuter certaines actions, comme attaquer des systèmes d'information (cyberattaques). Les «zombies» peuvent être contrôlés, souvent à l'insu des utilisateurs de ces ordinateurs, par un autre ordinateur, également appelé «centre de commande et de contrôle». Les personnes qui gèrent ce centre font partie des auteurs de l'infraction puisqu'elles utilisent les ordinateurs compromis pour attaquer des systèmes d'information. Il est très difficile de repérer les coupables car les ordinateurs qui composent le réseau zombie et lancent l'attaque peuvent se trouver ailleurs.

Proposition de DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI du Conseil, Bruxelles, le 30.9.2010, COM(2010) 517 final, 2010/0273 (COD)

2.152 BUG

Ver:

- *Defecto (en programas)*
- *Flaw*

2.152.1 BUG

Error generalmente de diseño de un programa o producto que es descubierto después de ser lanzado al mercado.

2.152.2 (EN) BUG (IMPLEMENTATION)

A software security defect that can be detected locally through static analysis.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/risk/248-BSI.html

2.152.3 (EN) BUGS

Bugs are software problems that exist only in code. A bug that exists in code may or may not ever be executed or exploitable. Therefore, a bug may or may not represent a vulnerability in the underlying software. Bugs are used to describe minor implementation errors that are typically easy to fix. Note that simply because bugs are minor implementation errors does not mean that the impact of an attacker exploiting the bug is small. For instance, a buffer overflow is a well-known type of bug that is generally easy to fix. However, exploiting a buffer overflow can give an attacker full control over a system.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/attack/590-BSI.html

2.152.4 (EN) BUG

A fault in a program which causes the program to perform in an unintended or unanticipated manner. See: anomaly, defect, error, exception, fault.

http://www.fda.gov/ora/Inspect_ref/igs/gloss.html

2.153 BULO

2.153.1 BULO

Mensaje de correo electrónico creado para su reenvío masivo que intenta hacer creer al remitente algo que es falso. El bulo más común es para alertar de virus inexistentes. Pueden ser varias las motivaciones para crear dicho mensaje, algunas de ellas son para recopilar gran cantidad de direcciones de correo, difundir información falsa en perjuicio de terceras personas u organismos o incitar al receptor del mensaje a causar daños en su propio ordenador.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.153.2 (EN) HOAX EMAIL

An otherwise harmless email that is designed to cause alarm or get itself forward to other users (or both). For example a fake virus warning or a chain letter.

http://www.getsafeonline.org/

2.153.3 (FR) CANULAR

Les hoaxes sont de fausses nouvelles ou de fausses informations qui se diffusent très rapidement. Les motivations sont différentes selon l'individu à l'origine de ces canulars, mais généralement

leur but est de parasiter la bande passante en multipliant les victimes. Un exemple classique de hoax: Envoyez cet e-mail à dix personnes qui le renverront à dix autres personnes ce qui vous apportera chance. Le site Internet www.hoaxbuster.com s'efforce de rétablir la vérité et de lutter contre ces mensonges électroniques.

http://www.cases.public.lu/functions/glossaire/

2.153.4 (FR) CANULAR

Est un message créé pour être largement diffusé (ex.: par messagerie électronique) et annonçant la présente d'un virus fictif.

L'attaque proprement dite consiste en une utilisation abusive, voir une négation de service, des ressources informatiques (ex.: serveur de messagerie).

http://securit.free.fr/glossaire.htm

2.154 BYPASS

2.154.1 MODO DE SOSLAYO (BY-PASS MODE)

Modalidad de trabajo de un dispositivo criptográfico en la cual el texto en claro pasa a su través sin sufrir ningún cifrado. Es un procedimiento útil en ciertas pruebas de funcionamiento de una línea de transmisión.

Por precaución, este modo de trabajo debe estar bloqueado mediante una llave de seguridad.

[Ribagorda:1997]

2.154.2 BYPASS

Modo de funcionamiento de un equipo de cifra de datos en el que permite el paso de información en claro a través de él sin modificarla.

Este modo de funcionamiento está previsto para poder efectuar pruebas de línea desde el equipo terminal de datos hasta el equipo de comunicación de datos (módem) próximo o lejano, donde se cierra el bucle de prueba.

[CESID:1997]

2.154.3 (EN) NON-BYPASSABILITY (OF THE TSF)

the security architecture property whereby all SFR-related actions are mediated by the TSF.

TSF - TOE Security Functionality

TOE - Target of Evaluation

SFR - Security Functional Requirement

[CC:2006]

2.154.4 (EN) BYPASS CAPABILITY

A cryptographic module implements a bypass capability when services are provided without cryptographic processing (e.g., transferring plaintext through the module without encryption). [FIPS-140-2:2001]

2.155 CABALLO DE TROYA

Ver:

- *Código dañino*
- http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29
- *BackOrifice*

2.155.1 CABALLO DE TROYA

Introducción subrepticia en un medio no propicio, con el fin de lograr un determinado objetivo.

DRAE. Diccionario de la Lengua Española.

2.155.2 TROYANO

También denominado “caballo de Troya”. Una clase de software malicioso que al instalarse permite al usuario ejecutar funciones normalmente, mientras los troyanos ejecutan funciones maliciosas sin que este lo sepa.

http://es.pcisecuritystandards.org

2.155.3 TROYANO

Programa que no se replica ni hace copias de sí mismo. Su apariencia es la de un programa útil o inocente, pero en realidad tiene propósitos dañinos, como permitir intrusiones, borrar datos, etc. [CCN-STIC-430:2006]

2.155.4 CABALLO DE TROYA

Programa que aparentemente, o realmente, ejecuta una función útil, pero oculta un subprograma dañino que abusa de los privilegios concedidos para la ejecución del citado programa.

Por ejemplo, un programa que reordene de una manera conveniente un fichero y, prevaliéndose de los derechos de escritura que debe concedérsele, copie el mismo en otro fichero accesible sólo por el creador de dicho programa.

[Ribagorda:1997]

2.155.5 (EN) TROJAN

A computer program that disguises itself as a useful software application, whereas its true purpose is to carry out and run a hidden, harmful transmission of material across a network. [CSS NZ:2011]

2.155.6 (EN) TROJAN HORSE

A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. [CNSSI_4009:2010]

2.155.7 (EN) TROJAN HORSE

(I) A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. (See: malware, spyware. Compare: logic bomb, virus, worm.) [RFC4949:2007]

2.155.8 (EN) TROJAN HORSE

Malicious program that masquerades as a benign application. [ISO-18043:2006]

2.155.9 (EN) TROJAN HORSE

A non-replicating program that appears to be benign but actually has a hidden malicious purpose. [NIST-SP800-83:2005]

2.155.10 (EN) TROJAN HORSE

A nonself-replicating program that seems to have a useful purpose, but in reality has a different, malicious purpose. [NIST-SP800-61:2004]

2.155.11 (EN) TROJAN HORSE

A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security. For example, making a "blind copy" of a sensitive file for the creator of the Trojan Horse. [TCSEC:1985]

2.155.12 (EN) TROJAN:

Also referred to as “Trojan horse.” A type of malicious software that when installed, allows a user to perform a normal function while the Trojan performs malicious functions to the computer system without the user’s knowledge.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.155.13 (EN) TROJAN HORSE

A malicious program that disguises itself as a beneficial or entertaining program but that actually damages a computer or installs code that can counteract security measures (perhaps by collecting passwords) or perform other tasks (such as launching a distributed denial of service attack). Unlike a computer virus, a Trojan horse does not replicate itself.

http://www.csoonline.com/glossary/

2.155.14 (EN) TROJAN HORSES

A Trojan Horse portrays itself as something other than what it is at the point of execution. While it may advertise its activity after launching, this information is not apparent to the user beforehand. A Trojan Horse neither replicates nor copies itself, but causes damage or compromises the security of the computer. A Trojan Horse must be sent by someone or carried by another program and may arrive in the form of a joke program or software of some sort. The malicious functionality of a Trojan Horse may be anything undesirable for a computer user, including data destruction or compromising a system by providing a means for another computer to gain access, thus bypassing normal access controls.

http://www.symantec.com/avcenter/refa.html

2.155.15 (EN) TROJAN HORSE

In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus.

http://searchsoftwarequality.techtarget.com/glossary/

2.155.16 (EN) TROJAN HORSE

A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

http://www.sans.org/security-resources/glossary-of-terms/

2.155.17 (EN) TROJAN

Malware which masquerades as some other type of program such as a link to a web site, a desirable image, etc. to trick a user into installing it. Named for the Ancient Greek legend of the Trojan Horse.

http://cyber.law.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas

2.155.18 TROJAN

Également appelé «cheval de Troie». Logiciel malveillant qui, une fois installé, permet à un utilisateur d’effectuer les fonctions normales tandis que le Trojan effectue des actes malveillants sur un système informatique à l’insu de l’utilisateur.

http://fr.pcisecuritystandards.org/

2.155.19 (FR) CHEVAL DE TROIE

Programme malicieux, conçu par un pirate informatique, souvent dissimulé au sein d'un autre programme et installé sur un système à l'insu de son propriétaire. Le cheval de Troie constitue le point d'entrée sur le système infecté autorisant un pirate informatique à prendre le contrôle à distance du système et de ses ressources.

http://www.cases.public.lu/functions/glossaire/

2.155.20 (FR) CHEVAL DE TROIE

Un cheval de Troie est un programme d'aspect anodin, masquant un code exécutable malicieux déclenchant ou servant à déclencher une attaque.

Un cheval de Troie est en général utiliser pour ouvrir une porte dérobée (backdoor) sur un système.

http://securit.free.fr/glossaire.htm

2.156 CADENA DE CERTIFICACIÓN

Ver:

- *Certificado X.509*
- *Validación de certificados*

2.156.1 TRAYECTO DE CERTIFICACIÓN

Secuencia ordenada de certificados de clave pública de objetos en el árbol de información de directorio que, junto con la clave pública del objeto inicial en el trayecto, puede ser procesada para obtener la del objeto final en el trayecto. [X.509:2005]

2.156.2 TRAYECTORIA DE CERTIFICACIÓN

Sucesión ordenada de certificados de objetos pertenecientes al Árbol de Información del Directorio que, junto con la clave pública del objeto inicial en la trayectoria, puede ser procesada para obtener la del objeto final de la misma (ISO/IEC 9594-8, ITU-T X.509). [Ribagorda:1997]

2.156.3 (EN) CERTIFICATION PATH

1. (I) A linked sequence of one or more public-key certificates, or one or more public-key certificates and one attribute certificate, that enables a certificate user to verify the signature on the last certificate in the path, and thus enables the user to obtain (from that last certificate) a certified public key, or certified attributes, of the system entity that is the subject of that last certificate. (See: trust anchor, certificate validation, valid certificate.)

2. (O) "An ordered sequence of certificates of objects in the [X.500 Directory Information Tree] which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path." [R3647, X509]

[RFC4949:2007]

2.156.4 (EN) CERTIFICATION PATH

An ordered sequence of certificates of objects in the DIT which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path. [X.509:2005]

2.156.5 (EN) PATH DISCOVERY

(I) For a digital certificate, the process of finding a set of public-key certificates that comprise a certification path from a trusted key to that specific certificate. [RFC4949:2007]

2.156.6 (FR) ITINÉRAIRE DE CERTIFICATION

séquence ordonnée de certificats concernant des objets contenus dans l'arbre DIT et qui peuvent être traités à partir de la clé publique de l'objet initial de l'itinéraire pour obtenir l'objet final de cet itinéraire. [X.509:2005]

2.157 CADENA DE CERTIFICADOS DE SEGURIDAD

Ver:

- *Certificado de seguridad*

2.157.1 CADENA DE CERTIFICADOS DE SEGURIDAD

Secuencia ordenada de certificados de seguridad, en la cual el primer certificado de seguridad contiene información pertinente a la seguridad y cada certificado de seguridad subsiguiente contiene información de seguridad que se puede utilizar para verificar certificados de seguridad previos. [X.810:1995]

2.157.2 (EN) SECURITY CERTIFICATE CHAIN

An ordered sequence of security certificates, in which the first security certificate contains security-relevant information, and each subsequent security certificate contains security information which can be used in the verification of previous security certificates. [X.810:1995]

2.157.3 (FR) CHAINE DE CERTIFICAT DE SECURITE

séquence ordonnée de certificats de sécurité, dans laquelle le premier certificat de sécurité contient des informations relatives à la sécurité et les certificats de sécurité suivants contiennent des informations de sécurité qui peuvent être utilisées pour la vérification des certificats de sécurité précédents. [X.810:1995]

2.158 CADENA DE CUSTODIA

2.158.1 CADENA DE CUSTODIA

Concepto legal que cubre la validez e integridad de las evidencias recogidas para sustentar un proceso judicial. Cubre todos los pasos desde la recogida hasta su utilización final.

2.158.2 (EN) CHAIN OF CUSTODY

possession, movement, handling, and location of material from the time it is obtained to the time it is presented in a matter [ISO-27050:2015]

2.158.3 (EN) CHAIN OF CUSTODY

A legal principle regarding the validity and integrity of evidence. It requires accountability for anything that will be used as evidence in a legal proceeding to ensure that it can be accounted for from the time it was collected until the time it is presented in a court of law.

Scope Note:

Includes documentation as to who had access to the evidence and when, as well as the ability to identify evidence as being the exact item that was recovered or tested. Lack of control over evidence can lead to it being discredited. Chain of custody depends on the ability to verify that evidence could not have been tampered with. This is accomplished by sealing off the evidence, so it cannot be changed, and providing a documentary record of custody to prove that the evidence was at all times under strict control and not subject to tampering.

ISACA, Cybersecurity Glossary, 2014

2.158.4 (EN) CHAIN OF CUSTODY

A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. [CNSSI_4009:2010]

2.158.5 (EN) CHAIN OF EVIDENCE

A process and record that shows who obtained the evidence; where and when the evidence was obtained; who secured the evidence; and who had control or possession of the evidence. The “sequencing” of the chain of evidence follows this order: collection and identification; analysis; storage; preservation; presentation in court; return to owner. [CNSSI_4009:2010]

2.159 CADENA DE DELEGACIÓN

Ver:

- *Delegación*

2.159.1 CADENA DE DELEGACIÓN

Secuencia ordenada de certificados que permite verificar la correcta delegación de un privilegio de una entidad a otra.

2.159.2 TRAYECTO DE DELEGACIÓN

Secuencia ordenada de certificados que, junto con la autenticación de una identidad de asertor de privilegios, puede ser procesada para verificar la autenticidad de un privilegio de asertor de privilegios. [X.509:2005]

2.159.3 (EN) DELEGATION PATH

An ordered sequence of certificates which, together with authentication of a privilege asserter's identity can be processed to verify the authenticity of a privilege asserter's privilege. [X.509:2005]

2.159.4 (FR) ITINÉRAIRE DE DÉLÉGATION

séquence ordonnée de certificats qui peuvent, conjointement à l'authentification de l'identité du déclarant, être traités pour vérifier l'authenticité d'un privilège de ce déclarant. [X.509:2005]

2.160 CAESAR_CIPHER

2.160.1 (EN) CAESAR CIPHER

(I) A cipher that is defined for an alphabet of N characters, A(1), A(2), ..., A(N), and creates cipher text by replacing each plaintext character A(i) by A(i+K, mod N) for some 0 < K < N+1. [Schn] [RFC4949:2007]

2.161 CÁMARA DE SEGURIDAD ELECTRÓNICA

2.161.1 CÁMARA DE SEGURIDAD ELECTRÓNICA

Procedimiento de copia de seguridad consistente en que se copian los datos modificados en un servidor y se transmiten a un lugar fuera de las instalaciones mediante un proceso por lotes.

2.161.2 BÓVEDAS ELECTRÓNICAS

Las bóvedas electrónicas o e-vaulting es el proceso de transferencia de datos por vía electrónica a un sitio de copia de seguridad, a diferencia del envío físico de cintas o discos con copias de seguridad. Los criterios principales en materia de e-vaulting son la capacidad de ancho de banda, de almacenamiento y del coste La copia de seguridad de la cinta es más costosa que convencional y se utiliza en los casos donde la velocidad de recuperación de datos es crucial Los datos se pueden almacenar en un servidor dedicado, en una biblioteca de cintas virtuales o «en la nube». Las modalidades de custodia en la nube y en cintas virtuales se refieren a destinos no dedicados exclusivamente a custodiar documentos, donde el coste del almacenamiento depende de la cantidad de espacio que se ocupe. La ventaja de este método es que no es necesario inventir en infraestructura de hardware (OpEx vs. CapEx), por el hecho de que sólo se paga por el almacenamiento actual requerido.

http://www.recall.es/why-recall/data-protection-terminology

2.161.3 (EN) ELECTRONIC VAULTING

A back-up procedure that copies changed files and transmits them to an off-site location using a batch process.

http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-b-glossary.aspx

2.162 CAMBIO

Ver:

- *Gestión de cambios*

2.162.1 CAMBIO

(Transición del Servicio) Adición, modificación o eliminación de algo que podría afectar a los Servicios de TI. El Alcance debería incluir todos los Servicios de TI, Elementos de Configuración, Procesos, Documentación etc. [ITIL:2007]

2.162.2 (EN) CHANGE

(Service Transition) The addition, modification or removal of anything that could have an effect on IT Services. The Scope should include all IT Services, Configuration Items, Processes, Documentation etc. [ITIL:2007]

2.162.3 (FR) CHANGEMENT

(Transition de Services) L'ajout, la modification ou la suppression de quoique que ce soit pouvant avoir un effet sur les services des TI. L'étendue doit inclure tous les services des TI, éléments de configuration, processus, documentation, etc… [ITIL:2007]

2.163 CAMBIO DE CLAVE

2.163.1 CAMBIO DE CLAVE

Cambio de la clave de un sistema criptográfico.

2.163.2 REDIGITACIÓN DE CLAVE

Proceso que consiste en el cambio de las claves criptográficas. La redigitación periódica de clave limita la cantidad de datos que pueden cifrarse con una misma clave.

http://es.pcisecuritystandards.org

2.163.1 (EN) RE-KEYING

Process of changing cryptographic keys. Periodic re-keying limits the amount of data encrypted by a single key.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.163.2 (EN) RE-KEY

To change the value of a cryptographic key that is being used in a cryptographic system/application. [CNSSI_4009:2010]

2.163.3 (EN) AUTOMATIC REMOTE REKEYING

Procedure to rekey distant cryptographic equipment electronically without specific actions by the receiving terminal operator. See manual remote rekeying. [CNSSI_4009:2010]

2.163.4 (EN) MANUAL REMOTE REKEYING

Procedure by which a distant crypto-equipment is rekeyed electronically, with specific actions required by the receiving terminal operator. Synonymous with cooperative remote rekeying. See also automatic remote keying. [CNSSI_4009:2010]

2.163.5 (EN) OVER-THE-AIR REKEYING (OTAR)

Changing traffic encryption key or transmission security key in remote cryptographic equipment by sending new key directly to the remote cryptographic equipment over the communications path it secures. [CNSSI_4009:2010]

2.163.6 (EN) REMOTE REKEYING

Procedure by which a distant crypto-equipment is rekeyed electrically. See automatic remote re-keying and manual remote rekeying. [CNSSI_4009:2010]

2.163.1 (EN) REKEY

(I) Change the value of a cryptographic key that is being used in an application of a cryptographic system. (See: certificate rekey.) [RFC4949:2007]

2.163.2 (FR) CHANGEMENT DE CLÉ

Processus de changement des clés cryptographiques. Le changement de clé périodique limite la quantité de données cryptées par une seule clé.

http://fr.pcisecuritystandards.org/

2.164 CAMELIA

Ver:

- *Cifrado en bloque*
- *Criptografía de clave secreta*
- https://www.cosic.esat.kuleuven.be/nessie/
- [ISO-18033-3:2005]
- http://en.wikipedia.org/wiki/Camellia_%28cipher%29

2.164.1 CAMELIA

Algoritmo de cifra basado en un secreto compartido (clave). Cifra el texto en bloques de 128 bits. Utiliza claves de 128, 192 o 256 bits.

2.164.2 (EN) CAMELIA

In cryptography, Camellia is a block cipher that has been evaluated favorably by several organisations, including the European Union's NESSIE project (a selected algorithm), and the Japanese CRYPTREC project (a recommended algorithm). The cipher was developed jointly by Mitsubishi and NTT in 2000, and has similar design elements to earlier block ciphers (MISTY1 and E2) from these companies.

Camellia has a block size of 128 bits, and can use 128-bit, 192-bit or 256-bit keys the same interface as the Advanced Encryption Standard.

http://en.wikipedia.org/wiki/Camellia_%28cipher%29

2.165 CAN

Ver:

- *Obligatorio*

2.165.1 (EN) CAN

within normative text, can indicates statements of possibility and capability, whether material, physical or causal (ISO/IEC).[CC:2006]

2.166 CANAL CONFIABLE

Ver:

- *Confianza*

2.166.1 CANAL CONFIABLE

Medio por el que se pueden comunicar, con la confianza necesaria, la TSF y un producto de TI confiable remoto.

TSF - TOE Security Functionality

TOE - Target of Evaluation

[CC:2006]

2.166.2 (EN) TRUSTED CHANNEL

A channel where the endpoints are known and data integrity is protected in transit. Depending on the communications protocol used, data privacy may be protected in transit. Examples include SSL, IPSEC, and secure physical connection. [CNSSI_4009:2010]

2.166.3 (EN) TRUSTED CHANNEL

a means by which a TSF and a remote trusted IT product can communicate with necessary confidence.

TSF - TOE Security Functionality

TOE - Target of Evaluation

[CC:2006]

2.167 CANAL ENCUBIERTO

2.167.1 CANAL OCULTO

1. Mecanismo no proyectado para comunicaciones, que es usado para transferir información violando la seguridad (ITSEC).

2. Canal de transmisión que permite a un proceso transmitir datos violando la política de seguridad del sistema (TCSEC).

Puede presentarse como canal de almacenamiento (storage channel) o como canal de tiempo (timing channel). El primero sucede cuando un proceso puede escribir, directa o indirectamente, en un almacenamiento que puede leer, directa o indirectamente otro proceso distinto utilizando este procedimiento para pasarse ilícitamente información. Típicamente requiere un recurso (por ejemplo, un disco) compartido por dos sujetos con diferentes habilitaciones de seguridad.

En el segundo, un proceso difunde información a otro modulando su propio uso de los recursos del sistema (por ejemplo, tiempo de UCP) lo que afecta al tiempo de respuesta. Ello puede ser observado e interpretado por el segundo proceso.

[Ribagorda:1997]

2.167.2 CANAL SUBLIMINAL

Transmisión de información de manera oculta sobre un canal que transmite información. Se aplica especialmente a algunos esquemas de firma digital. [CESID:1997]

2.167.1 (EN) COVERT CHANNEL

An unauthorized communication path that manipulates a communications medium in an unexpected, unconventional or unforeseen way in order to transmit information without detection by anyone other than the entities operating the covert channel. [CNSSI_4009:2010]

2.167.2 (EN) COVERT CHANNEL ANALYSIS

Determination of the extent to which the security policy model and subsequent lower-level program descriptions may allow unauthorized access to information. [CNSSI_4009:2010]

2.167.3 (EN) COVERT STORAGE CHANNEL

Covert channel involving the direct or indirect writing to a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels. [CNSSI_4009:2010]

2.167.4 (EN) COVERT TIMING CHANNEL

Covert channel in which one process signals information to another process by modulating its own use of system resources (e.g., central processing unit time) in such a way that this manipulation affects the real response time observed by the second process. [CNSSI_4009:2010]

2.167.5 (EN) COVERT CHANNEL

1. (I) An unintended or unauthorized intra-system channel that enables two cooperating entities to transfer information in a way that violates the system's security policy but does not exceed the entities' access authorizations.

(See: covert storage channel, covert timing channel, out-of-band, tunnel.)

2. (O) "A communications channel that allows two cooperating processes to transfer information in a manner that violates the system's security policy." [NCS04]

[RFC4949:2007]

2.167.6 (EN) COVERT STORAGE CHANNEL

(I) A system feature that enables one system entity to signal information to another entity by directly or indirectly writing a storage location that is later directly or indirectly read by the second entity. (See: covert channel.) [RFC4949:2007]

2.167.7 (EN) COVERT TIMING CHANNEL

(I) A system feature that enables one system entity to signal information to another by modulating its own use of a system resource in such a way as to affect system response time observed by the second entity. (See: covert channel.) [RFC4949:2007]

2.167.8 (EN) COVERT CHANNEL

an enforced, illicit signalling channel that allows a user to surreptitiously contravene the multi-level separation policy and unobservability requirements of the TOE (this is a special case of monitoring attacks).

TOE - Target of Evaluation

[CC:2006]

2.167.9 (EN) COVERT CHANNEL

the use of a mechanism not intended for communication to transfer information in a way that violates security. [ITSEC:1991]

2.167.10 (EN) COVERT CHANNEL

A communication channel that allows a process to transfer information in a manner that violates the system's security policy. [TCSEC:1985]

2.167.11 (EN) COVERT STORAGE CHANNEL

A covert channel that involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels. [TCSEC:1985]

2.167.12 (EN) COVERT TIMING CHANNEL

A covert channel in which one process signals information to another by modulating its own use of system resources (e.g., CPU time) in such a way that this manipulation affects the real response time observed by the second process. [TCSEC:1985]

2.168 CANISTER

2.168.1 CANISTER

Contenedor físico empleado para transportar y proteger claves criptográficas en cinta perforada o en papel.

2.168.2 (EN) CANISTER

Type of protective package used to contain and dispense keying material in punched or printed tape form. [CNSSI_4009:2010]

2.169 CAPACIDAD

2.169.1 CAPACIDAD

1. Testigo usado como identificador de un recurso, tal que la posesión del mismo por una entidad le confiere derechos de acceso sobre dicho recurso (ISO-7498-2).

2. Mecanismo de control de acceso que asocia a cada sujeto los objetos y los derechos de acceso que posee sobre estos últimos.

[Ribagorda:1997]

2.169.2 CAPACIDAD

Testigo (token) utilizado como identificador de un recurso de modo que la posesión del testigo confiera derechos de acceso a ese recurso. [ISO-7498-2:1989]

2.169.3 (EN) CAPABILITY

A token used as an identifier for a resource such that possession of the token confers access rights for the resource. [ISO-7498-2:1989]

2.169.4 (FR) CAPACITÉ

Jeton utilisé comme identificateur d'une ressource de telle sorte que la possession du jeton confère des droits d'accès à cette ressource. [ISO-7498-2:1989]

2.170 CAPACIDAD DE SUPERVIVENCIA

2.170.1 CAPACIDAD DE SUPERVIVENCIA

Capacidad de un sistema para continuar prestando un servicio activamente bajo condiciones adversas. Se consideran tanto desastres naturales, como accidentes y ataques deliberados.

2.170.2 (EN) SURVIVABILITY

(I) The ability of a system to remain in operation or existence despite adverse conditions, including natural occurrences, accidental actions, and attacks. (Compare: availability, reliability.) [RFC4949:2007]

2.170.3 (EN) SURVIVABILITY

The capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents. Timeliness is a critical factor that is typically included in (or implied by) the very high-level requirements that defines mission. However, timeliness is such an important factor that we include it explicitly in the definition of survivability. It is important to recognize that is it the mission fulfillment that must survive, not any particular subsystem to fulfill its mission, even if significant portions of the system are damaged or destroyed. We will sometimes use the term survivable system as a less than perfectly precise shorthand for a system with the capability to fulfill a specified mission in the face of attacks, failures, or accidents.

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.171 CAPEC

2.171.1 CAPEC

Iniciativa gubernamental (USA) participativa para establecer una taxonomía y un diccionario de ataques en busca de un mejor entendimiento y una mejor defensa colectiva.

https://capec.mitre.org/index.html

2.171.2 (EN) CAPEC

Understanding how your adversary operates is essential to effective cyber security. CAPEC™ is a comprehensive dictionary and classification taxonomy of known attacks that can be used by analysts, developers, testers, and educators to advance community understanding and enhance defenses.

https://capec.mitre.org/index.html

2.172 CAPI - CRYPTOGRAPHIC APPLICATION PROGRAMMING INTERFACE

Acrónimos: CAPI

Ver:

- http://www.ietf.org/rfc/rfc2628
- *PKCS - Public Key Cryptography Standards*

2.172.1 CAPI - CRYPTOGRAPHIC APPLICATION PROGRAMMING INTERFACE

Interfaz normalizada para que los programas usen servicios criptográficos facilitados por diferentes proveedores bajo una interfaz homogénea.

2.172.2 (EN) CRYPTOGRAPHIC APPLICATION PROGRAMMING INTERFACE (CAPI)

(I) The source code formats and procedures through which an application program accesses cryptographic services, which are defined abstractly compared to their actual implementation. Example, see: PKCS #11, [R2628]. [RFC4949:2007]

2.173 CAPTCHA

Acrónimos: CAPTCHA

Ver:

- *Verificación visual*
- *Pregunta-respuesta*

2.173.1 CAPTCHA

Captcha es el acrónimo de Completely Automated Public Turing test to tell Computers and Humans Apart (Prueba de Turing pública y automática para diferenciar a máquinas y humanos).

Se trata de una prueba desafío-respuesta utilizada en computación para determinar cuándo el usuario es o no humano. El término se empezó a utilizar en el año 2000 por Luis von Ahn, Manuel Blum y Nicholas J. Hopper de la Carnegie Mellon University, y John Langford de IBM.

La típica prueba consiste en que el usuario introduzca un conjunto de caracteres que se muestran en una imagen distorsionada que aparece en pantalla. Se supone que una máquina no es capaz de comprender e introducir la secuencia de forma correcta por lo que solamente el humano podra hacerlo (salvo error).

Como el test es controlado por una máquina en lugar de un humano como en la Prueba de Turing, también se denomina Prueba de Turing Inversa.

http://es.wikipedia.org/wiki/Captcha

2.173.2 (EN) COMPLETELY AUTOMATED PUBLIC TURING TEST TO TELL COMPUTERS AND HUMANS APART (CAPTCHA)

An interactive feature added to web-forms to distinguish use of the form by humans as opposed to automated agents. Typically, it requires entering text corresponding to a distorted image or from a sound stream.

[NIST-SP800-63:2013]

2.173.3 (EN) CAPTCHA

A CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart) is a challenge-response system test designed to differentiate humans from automated programs. A CAPTCHA differentiates between human and bot by setting some task that is easy for most humans to perform but is more difficult and time-consuming for current bots to complete.

CAPTCHAs are often used to stop bots and other automated programs from using blogs (see splog) to affect search engine rankings, signing up for e-mail accounts to send out spam or take part in on-line polls.

Frequently, a CAPTCHA features an image file of slightly distorted alphanumeric characters. A human can usually read the characters in the image without too much difficulty. A bot program is able to recognize that the content contains an image , but it has no idea what the image is. To accomodate the visually-impaired, some CAPTCHAs use audio files. In such a system, the human listens to a series of letters or short words and types what he hears to prove he is not a bot.

http://searchsoftwarequality.techtarget.com/glossary/

2.174 CAPTURA DEL TECLADO

Ver:

- *Monitorización del teclado*
- http://en.wikipedia.org/wiki/Keylogging

2.174.1 KEYLOGGER

Es un tipo de troyano que se caracteriza por capturar y almacenar las pulsaciones efectuadas sobre el teclado. Posteriormente esta información (que puede contener información sensible) se envía a un atacante, que las puede utilizar en su propio provecho.

Las ultimas versiones de este tipo de programas maliciosos también hacen capturas de pantalla del equipo atacado. De esta forma, se hace ineficaz e inseguro el uso del teclado virtual.

http://www.inteco.es/glossary/Formacion/Glosario/

2.174.2 CAPTURADOR DE PULSACIONES DE TECLADO

Programa que intercepta todas las pulsaciones realizadas en el teclado (e incluso a veces también el ratón), y las guarda en un archivo para obtener datos sensibles como contraseñas, etc. Posteriormente puede ser enviado a un tercero sin conocimiento ni consentimiento del usuario.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.174.3 (EN) KEY LOGGER

Key loggers are used to monitor keyboard activity on a PC. These can be software-based (bundled with Trojan horses, adware, and spyware) or hardware-based (between the keyboard cable and the PC, acoustic etc.) Usually this information is retrieved across a local network, the internet, or from the physical device connected to the keyboard.

PC Security Handbook, Rich Robinson

2.174.4 (EN) KEY LOGGER

A virus that logs a user's keystrokes as they type in order to capture private information, passwords or credit card information. Occasionally, key loggers can be physical devices attached to a PC.

http://www.getsafeonline.org/

2.174.5 (EN) KEYSTROKE LOGGER

A device that monitors and records keyboard usage. [NIST-SP800-83:2005]

2.174.6 (EN) KEYSTROKE LOGGING (OFTEN CALLED KEYLOGGING)

is a diagnostic used in software development that captures the user's keystrokes. It can be useful to determine sources of error in computer systems and is sometimes used to measure employee productivity on certain clerical tasks. Such systems are also highly useful for law enforcement and espionagefor instance, providing a means to obtain passwords or encryption keys and thus bypassing other security measures. However, keyloggers are widely available on the Internet and can be used by anyone for the same purposes.

http://en.wikipedia.org/wiki/Keylogging

2.174.7 (EN) KEYLOGGER

Keyloggers are programs that can monitor and record your every keystroke, exposing you to the risk of identity theft by revealing user names, passwords and other confidential information.

http://www.passwordnow.com/en/glossary/keylogger.html

2.174.8 (EN) KEYLOGGER

A keylogger, sometimes called a keystroke logger, key logger, or system monitor, is a hardware device or small program that monitors each keystroke a user types on a specific computer's keyboard. As a hardware device, a keylogger is a small battery-sized plug that serves as a connector between the user's keyboard and computer. Because the device resembles an ordinary keyboard plug, it is relatively easy for someone who wants to monitor a user's behavior to physically hide such a device "in plain sight." (It also helps that most workstation keyboards plug into the back of the computer.) As the user types, the device collects each keystroke and saves it as text in its own miniature hard drive. At a later point in time, the person who installed the keylogger must return and physically remove the device in order to access the information the device has gathered.

http://searchsoftwarequality.techtarget.com/glossary/

2.174.9 (FR) KEYLOGGER

Les keyloggers (de l'anglais Keystroke Logger, enregistreur de frappes de touches) sont des petits programmes espions qui enregistrent toutes les frappes sur les touches d'un clavier. Régulièrement, le keylogger envoie les informations ainsi collectées au pirate. Les keyloggers les plus sophistiqués ne se contentent pas d'enregistrer les frappes sur le clavier mais effectuent également des captures d'écran. Les keyloggers constituent une atteinte à la confidentialité des ressources.

http://www.cases.public.lu/functions/glossaire/

2.175 CARGADOR DE CLAVES

Ver:

- *Clave*
- *Clave criptográfica*

2.175.1 CARGADOR DE CLAVES

Unidad electrónica autocontenida capaz de almacenar, al menos, una clave criptográfica y transmitir esta, bajo petición, al equipo criptográfico. (ISO-8732). [Ribagorda:1997]

2.175.2 (EN) KEY LOADER

A self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or a component of a key that can be transferred, upon request, into a cryptographic module. [CNSSI_4009:2010]

2.175.3 (EN) KEY LOADER

a self-contained device that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module. [ISO-19790:2006]

2.175.4 (EN) KEY LOADER

a self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module. [FIPS-140-2:2001]

2.176 CARGA REMOTA DE CLAVES

2.176.1 CARGA REMOTA DE CLAVES

Transmisión de un equipo criptográfico a otro de una clave criptográfica cifrada , que una vez descifrada operará en este último.

La transmisión cifrada evita el compromiso de la clave criptográfica.

[Ribagorda:1997]

2.176.2 CARGA REMOTA DE CLAVES

Técnica por la que un equipo de cifra puede transmitir a otro compatible una clave cifrada que, una vez descifrada, puede utilizar en operaciones de cifra. [CESID:1997]

2.176.3 (EN) REMOTE KEY LOAD

Loading of a cryptographic key froma remote equipment. The key is transmitted encrypted.

2.177 CARTAS NIGERIANAS

Ver:

- *Scam*

2.177.1 CARTAS NIGERIANAS

Las conocidas como cartas nigerianas son una forma de estafa tradicional que empleando las nuevas tecnologías, en particular el correo electrónico, consisten en el envío de comunicaciones o cartas en las que el remitente pone a disposición del destinatario ofertas “falsas” para participar en negocios supuestamente rentables, o con la intención de involucrar a la víctima en cualquier otra situación engañosa, procurando que transfiera una fuerte cantidad de dinero para llevar a cabo la operación.

Inicialmente los estafadores se hacían pasar por ciudadanos nigerianos lo que dió origen al término en cuestión. Sin embargo, y en todo caso, los estafadores se valen de información falsa y sitios fraudulentos en Internet para cometer el acto ilícito.

http://www.inteco.es/glossary/Formacion/Glosario/

2.177.2 (EN) NIGERIAN LETTER SCAMS

Nigerian Letter scams have been around for ages. Originally, these scams originated in Nigeria, though today they come from just about anywhere.

To create the scam, criminals send out thousands of letters that appear to be from a banking or legal official. The letters claim there is a large sum of money that can only be released to a relative of some deceased member of royalty (often, a person that was persecuted by the government).

Victims are asked to provide a bank account into which the money can be transferred and promised a large percentage of the money for performing the service. In same cases, victims may also be asked to pay a fee or a series of fees for the release of the money.

Once the victim has provided account information, the criminals will often drain their bank accounts, and occasionally use that information to open new, fraudulent accounts.

http://idtheft.about.com/od/glossary/

2.178 CAST

Acrónimos: CAST

Ver:

- *Cifrado en bloque*
- *Criptografía de clave secreta*
- http://www.ietf.org/rfc/rfc2612
- http://www.ietf.org/rfc/rfc2144
- [ISO-18033-3:2005]

2.178.1 CAST

Algoritmo de cifra basado en un secreto compartido (clave).

- CAST-128: Cifra el texto en bloques de 64 bits. Utiliza claves de 40 a 128 bits.
- CAST-256: Cifra el texto en bloques de 128 bits. Utiliza claves de 128, 192 o 256 bits.

2.178.2 CAST-256 (O CAST6)

es un algoritmo de cifrado por bloques publicado en junio de 1998 y propuesto como candidato para el programa Advanced Encryption Standard (AES). Es una extensión de algoritmo de cifrado CAST-128; ambos fueron diseñados siguiendo la metodología de diseño "CAST" inventada por Carlisle Adams y Stafford Tavares. Howard Heys y Michael Wiener contribuyeron también en su diseño.

CAST-256 utiliza los mismos elementos que CAST-128, incluyendo cajas de tipo S-Box, pero éste último está adaptado al tamaño de bloque de 128 bits - el doble que su predecesor. (Una

construcción similar ocurrió en la evolución de RC5 hacia RC6). 'CAST-256 acepta claves de tamaño 128, 160, 192, 224 y 256 bits. CAST-256 ejecuta 48 vueltas, algunas veces descritas como 12 quad-rounds, organizadas en una red de Feistel generalizada.

En el RFC 2612, los autores afirman que, "El algoritmo de cifrado CAST-256 descrito en este documento está disponible en todo el mundo sin cobro de royalties y sin necesidad de licencia para aplicaciones no comerciales."

http://es.wikipedia.org/wiki/CAST-256

2.178.3 CAST-128 (O TAMBIÉN, CAST5)

es un cifrador por bloques usado en un gran número de productos, notablemente como cifrador por defecto en algunas versiones de GPG y PGP. Ha sido aprobado por el gobierno canadiense para ser usado por el Communications Security Establishment. El algoritmo fue creado en 1996 por Carlisle Adams y Stafford Tavares usando el procedimiento de diseño CAST. Otro miembro de la familia de CAST es CAST-256 (un candidato a AES) derivó de CAST-128. De acuerdo con algunas fuentes, el nombre CAST se basa en las iniciales de sus autores, mientras que Bruce Schneier informa que los autores indican que el nombre deberá conjurar imágenes de aleatoriedad (Schneier, 1996).

http://es.wikipedia.org/wiki/CAST-128

2.178.4 (EN) CAST

(N) A design procedure for symmetric encryption algorithms, and a resulting family of algorithms, invented by Carlisle Adams (C.A.) and Stafford Tavares (S.T.). [R2144, R2612] [RFC4949:2007]

2.179 CATEGORÍA DE UN SISTEMA DE INFORMACIÓN

2.179.1 CATEGORÍA DE UN SISTEMA.

Es un nivel, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios. [ENS:2010]

2.179.2 (EN) SECURITY CATEGORY

The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation.[FIPS 199, Adapted] [NIST-SP800-53:2013]

2.179.3 (EN) SECURITY CATEGORIZATION

The process of determining the security category for information or an information system. See Security Category. [NIST-SP800-53:2013]

2.179.4 (EN) SECURITY CATEGORY

The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation. [CNSSI_4009:2010]

2.180 CBC - CIPHER BLOCK CHAINING

Acrónimos: CBC

Ver:

- *Modo de operación (1)*
- [NIST-SP800-38A:2001]
- [FIPS-81:1980]
- *Criptografía de clave secreta*
- http://www.ietf.org/rfc/rfc1829
- http://www.ietf.org/rfc/rfc2405
- *Valor de inicialización*
- http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

2.180.1 CBC - CIPHER BLOCK CHAINING

1. Cifrado de información tal que cada bloque de texto cifrado es criptográficamente dependiente del precedente (ISO 8372).

2. Modalidad de cifrado de bloques en la cual cada bloque cifrado se realimenta a la entrada del cifrador para componerse o-exclusivo con el siguiente texto en claro, cifrándose seguidamente el resultado.

Su aplicación más frecuente se encuentra en el almacenamiento cifrado de ficheros de acceso secuencial.

[Ribagorda:1997]

2.180.2 (EN) CIPHER BLOCK CHAINING (CBC)

(N) A block cipher mode that enhances ECB mode by chaining together blocks of cipher text it produces. [FP081] (See: block cipher, [R1829], [R2405], [R2451], [SP38A].) [RFC4949:2007]

2.180.3 (EN) CBC - CIPHER BLOCK CHAINING

In the cipher-block chaining (CBC) mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block is dependent on all plaintext blocks processed up to that point. Also, to make each message unique, an initialization vector must be used in the first block.

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

2.181 CCM - COUNTER WITH CIPHER BLOCK CHAINING-MESSAGE AUTHENTICATION CODE

Acrónimos: CCM

Ver:

- *Modo de operación (1)*
- [NIST-SP800-38A:2001]
- [NIST-SP800-38C:2004]
- *Criptografía de clave secreta*
- http://csrc.nist.gov/CryptoToolkit/modes/800-38_Series_Publications/NIST-SP800-38C.pdf

2.181.1 CCM - COUNTER WITH CIPHER BLOCK CHAINING-MESSAGE AUTHENTICATION CODE

Modo de operación de un cifrador que garantiza confidencialidad y autenticidad.

2.181.2 (EN) COUNTER WITH CIPHER BLOCK CHAINING-MESSAGE AUTHENTICATION CODE

(CCM) (N) A block cipher mode [SP38C] that provides both data confidentiality and data origin authentication, by combining the techniques of CTR and a CBC-based message authentication code. (See: block cipher.) [RFC4949:2007]

2.181.3 (EN) CCM - COUNTER WITH CIPHER BLOCK CHAINING-MESSAGE AUTHENTICATION CODE

Counter with Cipher Block Chaining-Message Authentication Code can provide assurance of the confidentiality and authenticity of data. CCM is based on an approved symmetric key block cipher algorithm whose block size is 128 bits, such as the Advanced Encryption Standard (AES) algorithm currently specified in Federal Information Processing Standard (FIPS) Pub. 197; thus, CCM cannot be used with the Triple Data Encryption Algorithm, whose block size is 64 bits. CCM can be considered a mode of operation of the block cipher algorithm.

2.182 CEGUERA

2.182.1 CEGUERA

Técnica de ocultación de tráfico importante en una red. La técnica consiste en inyectar tráfico masivo que provoque una saturación en los detectores que pudieran estar al acecho.

2.182.2 (EN) BLINDING

Generating network traffic that is likely to trigger many alerts in a short period of time, to conceal alerts triggered by a real attack performed simultaneously. [NIST-SP800-94:2007]

2.183 CENTRO DE DISTRIBUCIÓN DE CLAVES

Acrónimos: KDC

Ver:

- *Clave*
- *Clave criptográfica*
- *Distribución de claves*

2.183.1 CENTRO DE DISTRIBUCIÓN DE CLAVES

Instalación que genera y entrega claves criptográficas para su distribución (ISO-8732) [Ribagorda:1997]

2.183.2 CENTRO DE DISTRIBUCIÓN DE CLAVES

Ver Centro de gestión de claves. [CESID:1997]

2.183.3 CENTRO DE GESTIÓN O DISTRIBUCIÓN DE CLAVES

Equipo utilizado en una red de cifra para generar y distribuir física o electrónicamente claves a los equipos de la misma, pudiendo crear diversas subredes a base de asignar distintas claves a diversos grupos de cifradores. [CESID:1997]

2.183.1 (EN) KEY DISTRIBUTION CENTER (KDC)

COMSEC facility generating and distributing key in electronic form. [CNSSI_4009:2010]

2.183.2 (EN) KEY DISTRIBUTION CENTER (KDC)

1. (I) A type of key center (used in symmetric cryptography) that implements a key-distribution protocol to provide keys (usually, session keys) to two (or more) entities that wish to communicate securely. (Compare: key translation center.) [RFC4949:2007]

2.183.3 (EN) KEY CENTER

(I) A centralized, key-distribution process (used in symmetric cryptography), usually a separate computer system, that uses master keys (i.e., KEKs) to encrypt and distribute session keys needed by a community of users. [RFC4949:2007]

2.184 CENTRO DE GENERACIÓN DE CLAVES

Acrónimos: KGC

2.184.1 CENTRO DE GENERACIÓN DE CLAVES

Tercero en el que confían las partes para que genere claves privadas de firma.

2.184.2 (EN) TRUSTED KEY GENERATION CENTRE KGC

Trusted third party, which, in an identity-based signature mechanism, generates a private signature key for each signing entity. [ISO-14888-3:2006]

2.185 CENTRO DE OPERACIONES DE SEGURIDAD

2.185.1 CENTRO DE OPERACIONES DE SEGURIDAD

Un Centro de Operaciones de Seguridad (COS) es una central de seguridad informática que previene, monitorea y controla la seguridad en las redes y en Internet.

Los servicios que presta van desde el diagnóstico de vulnerabilidades hasta la recuperación de desastres, pasando por la respuesta a incidentes, neutralización de ataques, programas de prevención, administración de riesgos y alertas de antivirus informáticos.

https://es.wikipedia.org/wiki/Centro_de_operaciones_de_seguridad

2.185.2 SOC – SECURITY OPERATIONS CENTER

An information security operations center (ISOC) is a dedicated site where enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended.

https://en.wikipedia.org/wiki/Information_security_operations_center

2.186 CER - CANONICAL ENCODING RULES

Acrónimos: CER

Ver:

- *ASN.1 - Abstract Syntax Notation One*
- *BER - Basic Encoding Rules*
- *DER - Distinguished Encoding Rules*
- *PER - Packet Encoding Rules*
- *XER - XML Encoding Rules*

2.186.1 CER - CANONICAL ENCODING RULES

Conjunto de reglas para formatear en binario datos descritos en ASN.1.

2.186.2 (EN) CER - CANONICAL ENCODING RULES

a set of ASN.1 encoding rules for formatting data in binary.

http://en.wikipedia.org/wiki/Canonical_Encoding_Rules

2.187 CERT - EQUIPO DE REACCIÓN RÁPIDA ANTE INCIDENTES INFORMÁTICOS

Acrónimos: CERT

Ver:

- *FIRST - Forum of Incident Response and Security Teams*
- http://www.cert.org/
- http://www.ietf.org/rfc/rfc2350
- *Emergencia*

2.187.1 CERT - EQUIPO DE REACCIÓN RÁPIDA ANTE INCIDENTES INFORMÁTICOS

Organización especializada en responder inmediatamente a incidentes relacionados con la seguridad de las redes o los equipos. También publica alertas sobre amenazas y vulnerabilidades de los sistemas. En general tiene como misiones elevar la seguridad de los sistemas de los usuarios y atender a los incidentes que se produzcan.

2.187.2 (EN) COMPUTER EMERGENCY RESPONSE TEAM (CERT)

Typically an operational team or centre that provides advice and mitigations against cyber attacks for businesses, government and individuals. [CSS NZ:2011]

2.187.3 (EN) COMPUTER EMERGENCY RESPONSE TEAM (CERT)

(I) An organization that studies computer and network INFOSEC in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security. (See: CSIRT, security incident.) [RFC4949:2007]

2.187.4 (EN) COMPUTER EMERGENCY RESPONSE TEAM (CERT):

A team that provides initial emergency-response aid and triage services to the victims or potential victims of cyber operations or cyber crimes, usually in a manner that involves coordination between private sector and governmental entities. These teams also maintain situational awareness about hacker activitiesand new developments in the design and use of malware, providing defenders of computer networks with advice on how to address security threats and vulnerabilities associated with those activities and malware.

The Tallinn Manual, 2013

2.187.1 (EN) COMPUTER INCIDENT RESPONSE TEAM (CIRT)

Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Also called a Computer Security Incident Response Team (CSIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability or Cyber Incident Response Team). [CNSSI_4009:2010]

2.187.2 (EN) COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

(I) An organization "that coordinates and supports the response to security incidents that involve sites within a defined constituency." [R2350] (See: CERT, FIRST, security incident.) [RFC4949:2007]

2.187.3 (EN) COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability). [NIST-SP800-61:2004]

2.187.4 (EN) CERT - COMPUTER EMERGENCY RESPONSE TEAM

An organization that studies computer and network INFOSEC in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security.

2.187.5 (EN) CERT (COMPUTER EMERGENCY RESPONSE TEAM)

A CERT is an organisation that studies computer and network security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security.

http://www.enisa.europa.eu/

2.187.6 (EN) CSIRT (COMPUTER SECURITY AND INCIDENT RESPONSE TEAM)

Over time, the CERTs (see above) extended their services from being a mere reaction force to a more complete security service provider, including preventive services like alerting or advisories and security management services. Therefore, the term CERT was not considered to be sufficient. As a result, the new term CSIRT was established in the end of the -90-ies. At the moment, both terms (CERT and CSIRT) are used in a synonymous manner, with CSIRT being the more precise term.

http://www.enisa.eu.int/

2.187.7 (EN) COMPUTER EMERGENCY RESPONSE TEAM (CERT)

An organization that studies computer and network INFOSEC in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security.

http://www.sans.org/security-resources/glossary-of-terms/

2.187.8 (FR) CERT (COMPUTER EMERGENCY AND RESPONSE TEAM)

Organisation spécialisée dans la gestion et la réponse aux incidents informatiques. Elle est en charge du suivi de l'incident (enregistrement) afin d'en déterminer la cause et de trouver des actions correctives. A l'origine, il s'agit d'une organisation américaine (Institut de génie logiciel de l'université de Carnegie Mellon ? Pittsburgh / USA) spécialisée dans la sécurité informatique. Depuis, chaque pays industrialisé à mis en place au moins une structure CERT nationale, qui établit également des alertes sécurité relatives aux failles détectées et aux solutions de protection en fonction des incidents relevés au niveau international.

http://www.cases.public.lu/functions/glossaire/

2.187.9 (FR) CERT - COMPUTER EMERGENCY RESPONSE TEAM

Équipe de l'université de Carnegie-Mellon, créée en 1988 après une célèbre diffusion d'un ver (worm) sur Internet, et dédiée à la veille en sécurité informatique.

CERT publie régulièrement des avis/alertes sur les failles de sécurité découvertes.

Le modèle du CERT est classiquement repris au sein des grandes entreprises ou administrations pour constituer des équipes de veille en sécurité ou de réaction sur incident de sécurité (Security incident response team). En France, le CERT/A assure cette fonction vis-à-vis des grandes administrations françaises.

http://securit.free.fr/glossaire.htm

2.187.10 (FR) CERT/A

CERT français, CERT/A est une structure d'alerte et d'assistance chargée de coordonner les réactions aux attaques sur les systèmes d'informations des administrations de l'État. Le CERT/A est rattaché à la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI).

http://www.certa.ssi.gouv.fr/

2.188 CERTIFICACIÓN

Ver:

- *Organismo de certificación*
- *Acreditación*
- *Evaluación*

2.188.1 CERTIFICACIÓN

Documento en que se asegura la verdad de un hecho.

DRAE. Diccionario de la Lengua Española.

2.188.2 CERTIFICACIÓN

Emisión de un certificado que acredita la Conformidad con un Estándar. La Certificación incluye una Auditoría formal realizada por un organismo independiente y Acreditado. El término Certificación también se usa para denotar la concesión de un certificado que acredita que una persona ha logrado una cualificación determinada. [ITIL:2007]

2.188.3 CERTIFICACIÓN DE LA SEGURIDAD

Determinación positiva de que un producto o sistema tiene capacidad para proteger la información según un nivel de seguridad y de acuerdo a unos criterios establecidos en el procedimiento o metodología de evaluación correspondiente.

2.188.4 CERTIFICACIÓN

Confirmación del resultado de una evaluación, y que los criterios de evaluación utilizados fueron correctamente aplicados. [Magerit:2012]

2.188.5 CERTIFICACIÓN

Emisión de un informe formal confirmando el resultado de una evaluación, así como qu4e el criterio de evaluación usado ha sido correctamente aplicado (ITSEC).

Esta certificación es. O será en el caso de algunos países, emitida por la Institución de Certificación de cada país, y se pretende tenga validez en todos los de la Unión Europea.

[Ribagorda:1997]

2.188.6 CERTIFICACIÓN

1. (notarization) Mecanismo de seguridad por el que una Autoridad de Certificación asegura la integridad, origen, tiempo o destino de una comunicación.

2. Confirmación del resultado de una evaluación, y que los criterios de evaluación utilizados fueron correctamente aplicados.

[CESID:1997]

2.188.7 (EN) CERTIFICATION

Comprehensive evaluation of the technical and non-technical security safeguards of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. See security control assessment. [CNSSI_4009:2010]

2.188.8 (EN) CERTIFICATION

1. (I) /information system/ Comprehensive evaluation (usually made in support of an accreditation action) of an information system's technical security features and other safeguards to establish the extent to which the system's design and implementation meet a set of specified security requirements. [C4009, FP102, SP37] (See: accreditation. Compare: evaluation.)

2. (I) /digital certificate/ The act or process of vouching for the truth and accuracy of the binding between data items in a certificate. (See: certify.)

3. (I) /PKI/ The act or process of vouching for the ownership of a public key by issuing a public-key certificate that binds the key to the name of the entity that possesses the matching private key. Besides binding a key with a name, a public-key certificate may bind those items with other restrictive or explanatory data items. (See: X.509 public-key certificate.)

[RFC4949:2007]

2.188.9 (EN) CERTIFICATION

in the context of this document, the process, producing written results, of performing a comprehensive evaluation of security features and other safeguards of a system to establish the extent to which the design and implementation meet a set of specified security requirements.

NOTE. This definition is generally accepted within the security community; within ISO the more generally used definition is: Procedure by which a third party gives written assurance that a product, process or service conforms to specified requirements [ISO/IEC Guide 2].

[ISO-21827:2007]

2.188.10 (EN) CERTIFICATION

Issuing a certificate to confirm Compliance to a Standard. Certification includes a formal Audit by an independent and Accredited body. The term Certification is also used to mean awarding a certificate to verify that a person has achieved a qualification. [ITIL:2007]

2.188.11 (EN) CERTIFICATION

A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. [NIST-SP800-53:2013] [FIPS-200:2006] [NIST-SP800-37:2004]

2.188.12 (EN) WHAT IS SECURITY CERTIFICATION?

Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The results of a security certification are used to reassess the risks and update the system security plan, thus providing the factual basis for an authorizing official to render a security accreditation decision. [NIST-SP800-100:2006]

2.188.13 (EN) CERTIFICATION

the issue of a formal statement confirming the results of an evaluation, and that the evaluation criteria used were correctly applied. [ITSEC:1991]

2.188.14 (EN) CERTIFICATION

The technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process, that establishes the extent to which a particular computer system's design and implementation meet a set of specified security requirements. [TCSEC:1985]

2.188.15 (FR) CERTIFICATION

Publier un certificat pour valider la conformité à un standard. La certification comporte un audit formel réalisé par une structure indépendante et accréditée. Le terme Certification signifie également décerner un certificat pour valider la qualification d'une personne. [ITIL:2007]

2.189 CERTIFICADO

Ver:

- *Certificado X.509*
- *Certificado de autenticación*

2.189.1 CERTIFICADO DIGITAL

Documento electrónico que permite asociar una clave criptográfica pública a una entidad propietaria de dicha clave, y que está protegido criptográficamente para garantizar su integridad y su autenticidad. [CCN-STIC-430:2006]

2.189.2 CERTIFICADO

1. En un sistema de clave pública, clave pública de un usuario más alguna otra información, todo ello cifrado con la clave privada de la autoridad de certificación, para hacerlo infalsificable.

2. Documento, expedido por la autoridad competente, que concede a un equipo de cifra una determinada habilitación de seguridad. (v. Evaluación).

[CESID:1997]

2.189.3 CERTIFICADO DIGITAL

Un Certificado Digital es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

http://es.wikipedia.org/wiki/Certificado

2.189.4 CERTIFICADO DE CLAVE PÚBLICA

Es la pieza central de la infraestructura PKI, y es la estructura de datos que enlaza la clave pública con los datos que permiten identificar al titular. Su sintaxis, se define empleando el lenguaje ASN.1 (Abstract Syntax Notation One), y los formatos de codificación más comunes son DER (Distinguish Encoding Rules) o PEM (Privacy Enhanced Mail).

http://es.wikipedia.org/wiki/Certificado_de_clave_p%C3%BAblica

2.189.1 (EN) CERTIFICATE

A digitally signed representation of information that 1) identifies the authority issuing it, 2) identifies the subscriber, 3) identifies its valid operational period (date issued / expiration date). In the IA community certificate usually implies public key certificate and can have the following types:

cross certificate – A certificate issued from a CA that signs the public key of another CA not within its trust hierarchy that establishes a trust relationship between the two CAs.

encryption certificate – A certificate containing a public key that can encrypt or decrypt electronic messages, files, documents, or data transmissions, or establish or exchange a session key for these same purposes. Key management sometimes refers to the process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate.

identity certificate – A certificate that provides authentication of the identity claimed. Within the NSS PKI, identity certificates may be used only for authentication or may be used for both authentication and digital signatures.

[CNSSI_4009:2010]

2.189.2 (EN) DIGITAL CERTIFICATE

(I) A certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object. (See: attribute certificate, public-key certificate.) [RFC4949:2007]

2.189.3 (EN) CERTIFICATE

an entity's data rendered unforgettable with the private or secret key of a certification authority. [ISO-19790:2006]

2.189.4 (EN) CERTIFICATE

An entity's data rendered unforgeable with the private or secret key of a certification authority. [ISO-13888-1:2004]

2.189.5 (EN) CERTIFICATE / CERTIFICATION REPORT

the public document issued by a Certification Body as a formal statement confirming the results of the evaluation and that the evaluation criteria, methods and procedures were correctly applied; including appropriate details about the evaluation based obn the ETR. [ITSEM:1993]

2.189.6 (FR) CERTIFICAT ÉLECTRONIQUE

Document électronique émis par un tiers de confiance permettant de lier une clé publique à une personne morale ou physique. On parle également de certificat de clé publique ou de certificat X509.

http://www.cases.public.lu/functions/glossaire/

2.190 CERTIFICADO AUTOEXPEDIDO

Ver:

- *Certificado*

2.190.1 CERTIFICADO DE ATRIBUTO AUTOEXPEDIDO

Certificado de atributo (AC) en el que el expedidor y el sujeto son la misma autoridad de atributo. Una autoridad de atributo podría utilizar un AC autoexpedido, por ejemplo, para publicar información de políticas. [X.509:2005]

2.190.2 CERTIFICADO AUTOEXPEDIDO

Certificado de clave pública en el que el expedidor y el sujeto son la misma autoridad de certificación (CA). Una CA podría utilizar certificados autoexpedidos, por ejemplo, durante una operación de renovación de clave para pasar la confianza de la clave antigua a la clave nueva. [X.509:2005]

2.190.3 CERTIFICADO AUTOFIRMADO

Constituye un caso especial de certificados autoexpedidos en los que la clave privada utilizada por la autoridad de certificación (CA) para firmar el certificado corresponde a la clave pública que está certificada en el certificado. Una CA podría utilizar un certificado autofirmado, por ejemplo, para anunciar su clave pública u otra información sobre sus operaciones.

NOTA. La utilización de certificados autoexpedidos y autofirmados expedidos por entidades distintas a las autoridades de certificación queda fuera del alcance de esta Recomendación | Norma Internacional.

[X.509:2005]

2.190.4 (EN) SELF-ISSUED AC

An attribute certificate where the issuer and the subject are the same Attribute Authority. An Attribute Authority might use a self-issued AC, for example, to publish policy information. [X.509:2005]

2.190.5 (EN) SELF-ISSUED CERTIFICATE

A public-key certificate where the issuer and the subject are the same CA. A CA might use self-issued certificates, for example, during a key rollover operation to provide trust from the old key to the new key. [X.509:2005]

2.190.6 (EN) SELF-SIGNED CERTIFICATE

A special case of self-issued certificates where the private key used by the CA to sign the certificate corresponds to the public key that is certified within the certificate. A CA might use a self-signed certificate, for example, to advertise their public key or other information about their operations.

NOTE. Use of self-issued certificates and self-signed certificates issued by other than CAs are outside the scope of this Recommendation | International Standard.

[X.509:2005]

2.190.7 (FR) CERTIFICAT D'AUTORITE DE CERTIFICATION AUTOEMIS

certificat d'attribut dont l'émetteur et le sujet sont la même autorité d'attribut. Une autorité d'attribut peut utiliser un certificat d'autorité de certification émis à l'ordre d'elle-même, par exemple afin de publier des informations de politique. [X.509:2005]

2.190.8 (FR) CERTIFICAT AUTOÉMIS

certificat dont l'émetteur et le sujet sont la même autorité de certification. Une autorité de certification peut utiliser des certificats émis à l'ordre d'elle-même, par exemple lors d'une opération de renouvellement de clé pour transférer la confiance de l'ancienne clé vers la nouvelle. [X.509:2005]

2.190.9 (FR) CERTIFICAT AUTOSIGNÉ

cas particulier de certificats autoémis pour lequel la clé privée utilisée par l'autorité de certification pour la signature du certificat correspond à la clé publique qui est certifiée au sein du certificat.

Une autorité de certification peut, par exemple, utiliser un certificat signé par elle-même pour publier sa clé publique ou d'autres informations concernant son fonctionnement.

NOTE. L'utilisation des certificats autoémis et des certificats autosignés émis par des entités autres que les autorités de certification ne relève pas du domaine d'application de la présente Recommandation | Norme internationale.

[X.509:2005]

2.191 CERTIFICADO CRUZADO

Ver:

- *Certificado X.509*

2.191.1 CERTIFICADO CRUZADO

Clave pública o certificado de atributo en el que el expedidor y el sujeto/titular son respectivamente dos CA o dos AA diferentes. Las CA y las AA expiden respectivamente certificados cruzados a otras CA o AA como mecanismo para autorizar la existencia de la CA sujeto (por ejemplo, en una jerarquía estricta) o para reconocer la existencia de la CA sujeto o la AA titular (por ejemplo, en un modelo fiduciario distribuido). La estructura del certificado cruzado se utiliza en ambos casos. [X.509:2005]

2.191.2 (EN) CROSS-CERTIFICATE

A certificate used to establish a trust relationship between two Certification Authorities. [CNSSI_4009:2010]

2.191.3 (EN) CROSS-CERTIFICATE

(I) A public-key certificate issued by a CA in one PKI to a CA in another PKI.

(See cross-certification.)

[RFC4949:2007]

2.191.4 (EN) CROSS-CERTIFICATION

(I) The act or process by which a CA in one PKI issues a public- key certificate to a CA in another PKI. [X509]

(See: bridge CA.)

[RFC4949:2007]

2.191.5 (EN) CROSS-CERTIFICATE

A public-key or attribute certificate where the issuer and the subject/holder are different CAs or AAs respectively. CAs and AAs issue cross-certificates to other CAs or AAs respectively as a mechanism to authorize the subject CA's existence (e.g., in a strict hierarchy) or to recognize the existence of the subject CA or holder AA (e.g., in a distributed trust model). The cross-certificate structure is used for both of these. [X.509:2005]

2.191.6 (EN) CROSS-CERTIFICATE

A certificate generated for a certification authority other than an immediate parent. [ISO-8732:1999]

2.191.7 (FR) CERTIFICAT CROISÉ

certificat d'attribut ou de clé publique dont l'émetteur et le sujet sont des autorités de certification ou des autorités d'attribut différentes. Des autorités de certification et des autorités d'attribut émettent des certificats destinés à d'autres autorités de certification et d'attribut, soit comme procédé d'autorisation de l'existence de l'autorité de certification sujette (par exemple, au sein d'une hiérarchie stricte), soit pour reconnaître l'existence de l'autorité de certification sujette ou de l'autorité d'attribut détentrice (par exemple dans un modèle de confiance réparti). La structure de certificat croisé est utilisée dans les deux cas. [X.509:2005]

2.192 CERTIFICADO DE AC

Ver:

- *Autoridad de certificación (AC)*
- *Certificado X.509*
- *Lista de revocación de autoridades de certificación*
- *Certificado de autoridad*

2.192.1 CERTIFICADO DE AUTORIDAD DE CERTIFICACIÓN; CERTIFICADO DE CA

Certificado para una CA expedido por otra CA. [X.509:2005]

2.192.2 (EN) CA CERTIFICATE

(D) "A [digital] certificate for one CA issued by another CA." [X509] [RFC4949:2007]

2.192.3 (EN) CA-CERTIFICATE

A certificate for one CA issued by another CA. [X.509:2005]

2.192.4 (FR) CERTIFICAT D'AUTORITÉ DE CERTIFICATION

certificat émis par une autorité de certification pour une autre autorité de certification. [X.509:2005]

2.193 CERTIFICADO DE ATRIBUTO

Acrónimos: AC

Ver:

- *Atributo*
- *Autoridad de atributo*
- *Certificado X.509*

2.193.1 CERTIFICADO DE ATRIBUTO (AC, ATTRIBUTE CERTIFICATE)

Estructura de datos, firmada digitalmente por una autoridad de atributo, que vincula algunos valores de atributo con información de identificación de su titular. [X.509:2005]

2.193.2 (EN) ATTRIBUTE CERTIFICATE

1. (I) A digital certificate that binds a set of descriptive data items, other than a public key, either directly to a subject name or to the identifier of another certificate that is a public-key certificate. (See: capability token.)

2. (O) "A data structure, digitally signed by an [a]ttribute [a]uthority, that binds some attribute values with identification information about its holder." [X509]

[RFC4949:2007]

2.193.3 (EN) ATTRIBUTE CERTIFICATE

A data structure, digitally signed by an Attribute Authority, that binds some attribute values with identification information about its holder. [X.509:2005]

2.193.4 (FR) CERTIFICAT D'ATTRIBUT (AC, ATTRIBUTE CERTIFICATE)

structure de donnée, portant la signature numérique d'une autorité d'attribut, qui lie certaines valeurs d'attribut à des informations d'identification concernant son détenteur. [X.509:2005]

2.194 CERTIFICADO DE AUTENTICACIÓN

Ver:

- *Autenticación*
- *Certificado*
- *Certificado X.509*

2.194.1 CERTIFICADO DE AUTENTICACIÓN

Información de autenticación en forma de certificado, avalado por una Autoridad de Certificación, que puede ser usado para confirmar la identidad de una entidad (ISO/IEC ISO-10181-2). [Ribagorda:1997]

2.194.2 (EN) AUTHENTICATION CERTIFICATE

An authentication certificate for use in an authentication exchange, obtained directly by the claimant from the authority who guarantees it. [ISO-10181-2:1996]

2.195 CERTIFICADO DE AUTENTICACIÓN DE SITIO WEB

Ver:

- *Certificado*

2.195.1 CERTIFICADO DE AUTENTICACIÓN DE SITIO WEB

«certificado de autenticación de sitio web», una declaración que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se ha expedido el certificado; [PE-CONS 60/14]

2.195.2 CERTIFICADO CUALIFICADO DE AUTENTICACIÓN DE SITIO WEB

«certificado cualificado de autenticación de sitio web», un certificado de autenticación de sitio web expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo IV; [PE-CONS 60/14]

2.195.3 (EN) CERTIFICATE FOR WEBSITE AUTHENTICATION'

‘certificate for website authentication' means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued; [PE-CONS 60/14]

2.195.4 (EN) QUALIFIED CERTIFICATE FOR WEBSITE AUTHENTICATION

'qualified certificate for website authentication' means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV; [PE-CONS 60/14]

2.195.5 (FR) CERTIFICAT D'AUTHENTIFICATION DE SITE INTERNET

"certificat d'authentification de site internet ", une attestation qui permet d'authentifier un site internet et associe celui-ci à la personne physique ou morale à laquelle le certificat est délivré; [PE-CONS 60/14]

2.195.6 (FR) CERTIFICAT QUALIFIE D'AUTHENTIFICATION DE SITE INTERNET

"certificat qualifié d'authentification de site internet ", un certificat d'authentification de site internet, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'annexe IV; [PE-CONS 60/14]

2.196 CERTIFICADO DE AUTORIDAD

Ver:

- *Autoridad*
- *Certificado X.509*
- *Certificado de AC*

2.196.1 CERTIFICADO DE AUTORIDAD

Certificado expedido a una autoridad (por ejemplo, puede ser a una autoridad de certificación o a una autoridad de atributo). [X.509:2005]

2.196.2 (EN) AUTHORITY CERTIFICATE

A certificate issued to an authority (e.g. either to a certification authority or to an attribute authority). [X.509:2005]

2.196.3 (FR) CERTIFICAT D'AUTORITÉ

certificat émis à destination d'une autorité (par exemple, une autorité de certification ou une autorité d'attribut). [X.509:2005]

2.197 CERTIFICADO DE CLAVE PÚBLICA

Ver:

- *Clave pública*
- *Certificado X.509*

2.197.1 CERTIFICADO DE CLAVE PÚBLICA

Clave pública de un usuario, junto con alguna otra información, hecha infalsificable por firma digital con la clave privada de la autoridad de certificación que la emitió. [X.509:2005]

2.197.2 (EN) PUBLIC-KEY CERTIFICATE

1. (I) A digital certificate that binds a system entity's identifier to a public key value, and possibly to additional, secondary data items; i.e., a digitally signed data structure that attests to the ownership of a public key. (See: X.509 public-key certificate.)

2. (O) "The public key of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it." [X509]

[RFC4949:2007]

2.197.3 (EN) PUBLIC KEY CERTIFICATE

A set of data that uniquely identifies an entity, contains the entity's public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity. Additional information in the certificate could specify how the key is used and its cryptoperiod. [NIST-SP800-57:2007]

2.197.4 (EN) PUBLIC KEY CERTIFICATE

The public key of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it. [X.509:2005]

2.197.5 (EN) PUBLIC KEY CERTIFICATE

The public key information of an entity signed by the certification authority and thereby rendered unforgeable. [ISO-13888-1:2004]

2.197.6 (EN) PUBLIC KEY CERTIFICATE

a set of data that uniquely identifies an entity, contains the entity's public key, and is digitally signed by a trusted party, thereby binding the public key to the entity. [FIPS-140-2:2001]

2.197.7 (EN) PUBLIC KEY CERTIFICATE

public key information of an entity signed by the certification authority and thereby rendered unforgeable. [ISO-11770-3:2008]

2.197.8 (FR) CERTIFICAT DE CLÉ PUBLIQUE

clé publique d'un utilisateur, associée à certaines autres informations qui sont rendues non falsifiables par signature numérique en utilisant la clé privée de l'autorité de certification émettrice. [X.509:2005]

2.197.9 (FR) CERTIFICAT DE CLÉS PUBLIQUE

Clé publique, identité et autres informations d'une entité rendues infalsifiables par la signature du certificat calculée avec la clé privée de l'autorité de certification qui l'a généré. [ISO-15782-1:2003]

2.197.10 (FR) CERTIFICAT DE CLÉS PUBLIQUE

Le format standard de certificat est X.509 v.3 (norme PKI-X). Les informations certifiées sont notamment:

- L'identité du porteur.
- La clé publique du porteur.
- La durée de vie du certificat.
- L'identité de l'autorité de certification émettrice.
- La signature de l'autorité de certification émettrice.

http://securit.free.fr/glossaire.htm

2.198 CERTIFICADO DE FIRMA ELECTRÓNICA

Ver:

- *Firma digital*
- *Certificado*

2.198.1 CERTIFICADO DE FIRMA ELECTRÓNICA

«certificado de firma electrónica», una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona; [PE-CONS 60/14]

2.198.2 CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA

«certificado cualificado de firma electrónica», un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I; [PE-CONS 60/14]

2.198.3 CERTIFICADO ELECTRÓNICO

documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad. [Ley-59:2003]

2.198.4 CERTIFICADOS RECONOCIDOS

son los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

Los certificados reconocidos incluirán, al menos, los siguientes datos:

- La indicación de que se expiden como tales.
- El código identificativo único del certificado.
- La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.
- La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
- La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.
- Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.
- El comienzo y el fin del período de validez del certificado.
- Los límites de uso del certificado, si se establecen.
- Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

[Ley-59:2003]

2.198.5 (EN) CERTIFICATE FOR ELECTRONIC SIGNATURE

'certificate for electronic signature' means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person; [PE-CONS 60/14]

2.198.6 (EN) QUALIFIED CERTIFICATE FOR ELECTRONIC SIGNATURE

'qualified certificate for electronic signature' means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I; [PE-CONS 60/14]

2.198.7 (EN) CERTIFICATE

means an electronic attestation which links signature-verification data to a person and confirms the identity of that person. [Directive-1999/93/EC:1999]

2.198.8 (EN) QUALIFIED CERTIFICATE

means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II.

Annex I:

- an indication that the certificate is issued as a qualified certificate;
- the identification of the certification-service-provider and the State in which it is established;
- the name of the signatory or a pseudonym, which shall be identified as such;
- provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
- signature-verification data which correspond to signature-creation data under the control of the signatory;
- an indication of the beginning and end of the period of validity of the certificate;
- the identity code of the certificate;
- the advanced electronic signature of the certification-service-provider issuing it;
- limitations on the scope of use of the certificate, if applicable; and
- limits on the value of transactions for which the certificate can be used, if applicable.

[Directive-1999/93/EC:1999]

2.198.9 (FR) CERTIFICAT DE SIGNATURE ÉLECTRONIQUE

"certificat de signature électronique", une attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne; [PE-CONS 60/14]

2.198.10 (FR) CERTIFICAT QUALIFIE DE SIGNATURE ELECTRONIQUE

"certificat qualifié de signature électronique", un certificat de signature électronique, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'annexe I; [PE-CONS 60/14]

2.199 CERTIFICADO DE REVOCACIÓN

Ver:

- *Certificado X.509*
- *Lista de revocación de certificados*

2.199.1 CERTIFICADO DE REVOCACIÓN

Certificado de seguridad expedido por una autoridad de seguridad para indicar que un determinado certificado de seguridad ha sido revocado. [X.810:1995]

2.199.2 (EN) REVOCATION CERTIFICATE

A security certificate issued by a security authority to indicate that a particular security certificate has been revoked. [X.810:1995]

2.199.3 (FR) CERTIFICAT DE RÉVOCATION

certificat de sécurité émis par une autorité de sécurité pour indiquer qu'un certificat de sécurité particulier a été révoqué. [X.810:1995]

2.200 CERTIFICADO DE SEGURIDAD

Ver:

- *Certificación*

2.200.1 CERTIFICADO DE SEGURIDAD

Conjunto de datos pertinentes a la seguridad expedida por una autoridad de seguridad o tercera parte confiable, junto con información de seguridad que se utiliza para proporcionar servicios de integridad y autenticación de origen de los datos para los datos.

NOTA. Se considera que todos los certificados son certificados de seguridad (véanse las definiciones pertinentes en ISO-7498-2). Se adopta el término certificado de seguridad para evitar conflictos de terminología con la Rec. UIT-T X.509 | ISO/IEC 9594-8 (es decir, la norma de autenticación del directorio).

[X.810:1995]

2.200.2 (EN) SECURITY CERTIFICATE

A set of security-relevant data issued by a security authority or trusted third party, together with security information which is used to provide the integrity and data origin authentication services for the data.

NOTE. All certificates are deemed to be security certificates (see the relevant definitions in ISO-7498-2). The term security certificate is adopted in order to avoid terminology conflicts with ITU-T Rec. X.509 | ISO/IEC 9594-8 (i.e. the directory authentication standard).

[X.810:1995]

2.200.3 (FR) CERTIFICAT DE SÉCURITÉ

ensemble de données relatives à la sécurité émis par une autorité de sécurité ou une tierce partie de confiance ainsi que les informations de sécurité qui sont utilisées pour fournir des services d'intégrité et d'authentification de l'origine des données.

NOTE. Tous les certificats sont réputés être des certificats de sécurité (voir les définitions applicables dans l'ISO-7498-2). Le terme certificat de sécurité est adopté afin d'éviter des conflits de terminologie avec la Rec. UIT-T X.509 | ISO/CEI 9594-8 (c'est-à-dire la norme d'authentification de l'annuaire).

[X.810:1995]

2.201 CERTIFICADO X.509

Ver:

- *Clave pública*
- *Certificado*
- *Certificado de clave pública*
- *Certificado de atributo*
- *Política de certificación*
- *Autoridad de certificación (AC)*
- *PKCS #10*
- *Jerarquía de certificación*
- *Cadena de certificación*
- *Validación de certificados*
- *Renovación del certificado*
- *Certificado de autoridad*
- *Certificado de AC*
- *Certificado cruzado*
- *Certificado de revocación*
- http://www.ietf.org/rfc/rfc3280

2.201.1 CERTIFICADO DE USUARIO

Clave pública de un usuario, junto con alguna otra información adicional, que se hace infalsificable cifrándola con la clave privada de la Autoridad de Certificación que las emite (ISO/IEC 9594-8, ITU-T X.509).

A menudo se denomina simplemente Certificado.

[Ribagorda:1997]

2.201.2 (EN) X.509 PUBLIC KEY CERTIFICATE

The public key for a user (or device) and a name for the user (or device), together with some other information, rendered unforgeable by the digital signature of the certification authority that issued the certificate, encoded in the format defined in the ISO/ITU-T X.509 standard. Also known as X.509 Certificate. [CNSSI_4009:2010]

2.201.3 (EN) X.509 PUBLIC KEY CERTIFICATE

The public key for a user (or device) and a name for the user (or device), together with some other information, rendered un-forgeable by the digital signature of the certification authority that issued the certificate, encoded in the format defined in the ISO/ITU-T X.509 standard. [NIST-SP800-57:2007]

2.201.4 (EN) SELF-SIGNED CERTIFICATE

A public key certificate whose digital signature may be verified by the public key contained within the certificate. The signature on a selfsigned certificate protects the integrity of the data, but does

not guarantee authenticity of the information. The trust of self-signed certificates is based on the secure procedures used to distribute them. [NIST-SP800-57:2007]

2.201.5 (EN) SELF-ISSUED AC

An attribute certificate where the issuer and the subject are the same Attribute Authority. An Attribute Authority might use a self-issued AC, for example, to publish policy information. [X.509:2005]

2.201.6 (EN) SELF-ISSUED CERTIFICATE

A public-key certificate where the issuer and the subject are the same CA. A CA might use self-issued certificates, for example, during a key rollover operation to provide trust from the old key to the new key. [X.509:2005]

2.201.7 (EN) SELF-SIGNED CERTIFICATE

A special case of self-issued certificates where the private key used by the CA to sign the certificate corresponds to the public key that is certified within the certificate. A CA might use a self-signed certificate, for example, to advertise their public key or other information about their operations. [X.509:2005]

2.202 CFB - CIPHER FEEDBACK MODE

Acrónimos: CFB

Ver:

- *Modo de operación (1)*
- [NIST-SP800-38A:2001]
- [FIPS-81:1980]
- *Criptografía de clave secreta*
- *Valor de inicialización*
- http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

2.202.1 CFB - CIPHER FEEDBACK MODE

Modalidad de cifrado de bloques que realimenta el texto cifrado, o parte del mismo para ser nuevamente cifrado operando el resultado o-exclusivo con el texto el claro, para obtener el siguiente bloque del texto cifrado.

Si se realimentan n bits, el cifrado se denomina en modo realimentado de n bits.

Su aplicación más frecuente se encuentra en la transmisión cifrada de información. Si se emplean para ello protocolos orientados al carácter se toman n=8 y si se eligen protocolos orientados al bit se escogen n=1.

[Ribagorda:1997]

2.202.2 (EN) CIPHER FEEDBACK (CFB)

(N) A block cipher mode that enhances ECB mode by chaining together the blocks of cipher text it produces and operating on plaintext segments of variable length less than or equal to the block length. [FP081] (See: block cipher, [SP38A].) [RFC4949:2007]

2.202.3 (EN) CFB - CIPHER FEEDBACK MODE

The cipher feedback (CFB) mode, a close relative of CBC, makes a block cipher into a self-synchronizing stream cipher. Operation is very similar; in particular, CFB decryption is almost identical to CBC decryption performed in reverse.

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

2.203 CHAP - CHALLENGE-HANDSHAKE AUTHENTICATION PROTOCOL

Acrónimos: CHAP

Ver:

- *Pregunta-respuesta*
- *PAP - Password Authentication Protocol*
- http://www.ietf.org/rfc/rfc1994

2.203.1 CHAP - CHALLENGE-HANDSHAKE AUTHENTICATION PROTOCOL

Protocolo de reto-respuesta por el que el receptor del reto es capaz de generar una respuesta válida, sólo si es quien dice ser. El reto debe cambiarse continuamente, sin repeticiones, para evitar ataques de "replay".

2.203.2 (EN) CHALLENGE-RESPONSE PROTOCOL

An authentication protocol where the Verifier sends the Claimant a challenge (usually a random value or a nonce) that the Claimant combines with a secret (such as by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the Verifier. The Verifier can independently verify the response generated by the Claimant (such as by re-computing the hash of the challenge and the shared secret and comparing to the response, or performing a public key operation on the response) and establish that the Claimant possesses and controls the secret. [NIST-SP800-63:2013]

2.203.3 (EN) CHALLENGE HANDSHAKE AUTHENTICATION PROTOCOL (CHAP)

(I) A peer entity authentication method (employed by PPP and other protocols, e.g., RFC 3720) that uses a randomly generated challenge and requires a matching response that depends on a cryptographic hash of some combination of the challenge and a secret key. [R1994] (See: challenge-response, PAP.) [RFC4949:2007]

2.203.4 (EN) CHALLENGE-HANDSHAKE AUTHENTICATION PROTOCOL - CHAP

a three-way authentication protocol defined in RFC 1994. [ISO-18028-4:2005]

2.203.5 (EN) CHAP (CHALLENGE HANDSHAKE AUTHENTICATION PROTOCOL)

A type of authentication where the person logging in uses secret information and some special mathematical operations to come up with a number value. The server he or she is logging into knows the same secret value and performs the same mathematical operations. If the results match, the person is authorized to access the server. One of the numbers in the mathematical operation is changed after every log-in, to protect against an intruder secretly copying a valid authentication session and replaying it later to log in.

http://www.watchguard.com/glossary/

2.203.6 (EN) CHALLENGE-HANDSHAKE AUTHENTICATION PROTOCOL (CHAP)

The Challenge-Handshake Authentication Protocol uses a challenge/response authentication mechanism where the response varies every challenge to prevent replay attacks.

http://www.sans.org/security-resources/glossary-of-terms/

2.203.7 (FR) CHAP - CHALLENGE-HANDSHAKE AUTHENTICATION PROTOCOL.

Protocole d'authentification basée sur le mécanisme de challenge/response, CHAP permet l'authentification par un serveur d' un client disposant d'un secret commun, sans véhiculer ce secret (et améliore en ce sens le protocole PAP). CHAP se déroule en trois étapes:

- Le serveur envoie le défi au client.
- Le client utilise une fonction de hachage à sens unique (one-way hash function) pour forger la réponse qu'il ré-émet au serveur.
- Le serveur effectue la même opération et compare les deux résultats. La concordance assure l'authenticité.

Périodiquement, ces trois étapes sont répétées afin de garantir l'identité des interlocuteurs.

CHAP implémente un service d'anti-rejeu.

CHAP n'assure pas l'authentification mutuelle (le serveur n'est pas authentifié par le client).

http://securit.free.fr/glossaire.htm

2.204 CIBERAMENAZA

2.204.1 CIBERAMENAZA

Amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste.

2.204.2 (EN) CYBER THREAT INFORMATION

(A) In general.--The term `cyber threat information' means information directly pertaining to--

(i) a vulnerability of a system or network of a government or private entity or utility;

(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or utility or any information stored on, processed on, or transiting such a system or network;

(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network of a government or private entity or utility; or

(iv) efforts to gain unauthorized access to a system or network of a government or private entity or utility, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network of a government or private entity or utility.

(B) Exclusion.--Such term does not include information pertaining to efforts to gain unauthorized access to a system or network of a government or private entity or utility that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

Cyber Intelligence Sharing and Protection Act. H.R. 624. 2013.

2.204.3 (EN) CYBER THREAT INTELLIGENCE

(A) In general.--The term `cyber threat intelligence' means intelligence in the possession of an element of the intelligence community directly pertaining to

(i) a vulnerability of a system or network of a government or private entity or utility;

(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or utility or any information stored on, processed on, or transiting such a system or network;

(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network of a government or private entity or utility; or

(iv) efforts to gain unauthorized access to a system or network of a government or private entity or utility, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network of a government or private entity or utility.

(B) Exclusion.--Such term does not include intelligence pertaining to efforts to gain unauthorized access to a system or network of a government or private entity or utility that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

Cyber Intelligence Sharing and Protection Act. H.R. 624. 2013.

2.205 CIBERATAQUE

2.205.1 CIBERATAQUE

Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan.

O.M. 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas

2.205.2 CIBERATAQUE

Uso del ciberespacio para atacar a los sistemas y servicios presentes en el mismo o alcanzables a través suyo. El atacante busca acceder sin autorización a información, o alterar o impedir el funcionamiento de los servicios.

2.205.3 (EN) CYBER ATTACK

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, or for destroying the integrity of the data or stealing controlled information. [US-ESC:2012]

2.205.4 (EN) CYBER ATTACK

An attempt to undermine or compromise the function of a computer-based system, access information, or attempt to track the online movements of individuals without their permission. [CSS NZ:2011]

2.205.5 (EN) CYBER ATTACK

A cyber attack is an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security. The aims of IT security, confidentiality, integrity and availability may all or individually be compromised.[CSS DE:2011]

2.205.6 (EN) CYBERATTACK

An act or action initiated in cyberspace to cause harm by compromising communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems.

2.205.7 NATO AC/322-N(2014)0072

2.205.8 (EN) CYBER ATTACK

is an offensive use of a cyber weapon intended to harm a designated target.

Russia-U.S. Bilateral On Cybersecurity Critical Terminology Foundations, Apr. 2011.

2.205.9 (EN) CYBER ATTACK

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. [CNSSI_4009:2010]

2.206 CIBERCONFLICTO

2.206.1 CIBERGUERRA

Lucha armada (en este caso las armas son las TIC) entre dos o más naciones o entre bandos de una misma nación, en la que se utiliza el Ciberespacio como campo de batalla. [ISDEFE-6:2009]

2.206.2 (EN) CYBER CONFLICT

is tense situation between or among nation-states or organized groups where unwelcome cyber attacks result in retaliation.

Russia-U.S. Bilateral On Cybersecurity Critical Terminology Foundations, Apr. 2011.

2.207 CIBERCRISIS

2.207.1 CIBERCRISIS

Un evento TIC grave, no autorizado o inesperado, donde han fracasado los mecanismos automáticos previstos, y los técnicos no pueden resolverlo.

2.207.2 (EN) CYBER CRISIS

An unauthorized or unexpected CIS event where automated measures have failed, whose impact is considered severe and recovery cannot be achieved through the involvement of cyber experts.

NATO AC/322-N(2014)0072

2.208 CIBERDEFENSA

2.208.1 CIBERDEFENSA

Concepto que engloba todas las actividades ofensivas y defensivas en las que se utilizan como medio aquellos relacionados con las infraestructuras TIC (Ej. Redes de ordenadores, ordenadores, programas informáticos, etc.), y cuyo "campo de batalla" es el Ciberespacio. Las actividades de desarrollo de la ciberdefensa van encaminadas hacia la capacitación de los gobiernos y naciones en la denominada "Ciberguerra". [ISDEFE-6:2009]

2.208.2 (EN) CYBER DEFENCE

The application of effective protective measures to obtain an appropriate level of Cyber Security in order to guarantee Defence's operation and functionalities. This is achieved by applying appropriate protective measures to reduce the security risk to an acceptable level. Cyber Defence consists of following duties: Protect, Detect, Respond, and Recover.

NATO - Cyber Security Strategy for Defence,- ACST–Strategy-CyberSecurity-001, 2014

2.208.3 (EN) ACTIVE CYBER DEFENCE

A proactive measure for detecting or obtaining information as to a cyber intrusion, cyber attack, or impending cyber operation, or for determining the origin of an operation that involves launching a pre-emptive, preventive, or cyber-counter operation against the source.

The Tallinn Manual, 2013

2.208.4 (EN) PASSIVE CYBER DEFENCE:

A measure for detecting and mitigating cyber intrusions and the effects of cyber attacks that does not involve launching a preventive, pre-emptive or countering operation against the source. Examples of passive cyber defence measures are firewalls, patches, anti-virus software, and digital forensics tools.

The Tallinn Manual, 2013

2.208.5 (EN) CYBER DEFENCE

The means to achieve and execute defensive measures to counter cyberattacks and mitigate their effects, and thus preserve and restore the security of communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems.

NATO AC/322-N(2014)0072

2.208.6 (EN) CYBER DEFENSE

is organized capabilities to protect against, mitigate from, and rapidly recover from the effects of cyber attack.

Russia-U.S. Bilateral On Cybersecurity Critical Terminology Foundations, Apr. 2011.

2.208.7 (EN) CYBER DEFENSIVE COUNTERMEASURE

is the deployment of a specific cyber defensive capability to deflect or to redirect a cyber attack.

Russia-U.S. Bilateral On Cybersecurity Critical Terminology Foundations, Apr. 2011.

2.208.8 (EN) CYBER DEFENSIVE CAPABILITY

is a capability to effectively protect and repel against a cyber exploitation or cyber attack, that may be used as a cyber deterrent.

Russia-U.S. Bilateral On Cybersecurity Critical Terminology Foundations, Apr. 2011.

2.209 CIBERDELINCUENCIA

2.209.1 CIBERDELINCUENCIA

Actividades delictivas llevadas a cabo mediante el empleo del ciberespacio, ya sea para dirigirlas hacia los sistemas y servicios presentes en el mismo o alcanzables a través suyo.

2.209.2 CIBERDELINCUENTE

Aquel que delinque en o usando el ciberespacio.

2.210 CIBERDELITO

2.210.1 CIBERDELITO

Actividad delictiva que emplea el ciberespacio como objetivo, herramienta o medio.

Ejemplos: fraude, suplantación de personalidad, robo, crimen organizado, etc.

2.210.2 (EN) CYBERCRIME

Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware). [CSS EU:2013]

2.210.3 (EN) CYBERSECURITY CRIME

The term `cybersecurity crime' means--

(A) a crime under a Federal or State law that involves

(i) efforts to deny access to or degrade, disrupt, or destroy a system or network;

(ii) efforts to gain unauthorized access to a system or network; or

(iii) efforts to exfiltrate information from a system or network without authorization; or

(B) the violation of a provision of Federal law relating to computer crimes, including a violation of any provision of title 18, United States Code, created or amended by the Computer Fraud and Abuse Act of 1986 (Public Law 99-474).

Cyber Intelligence Sharing and Protection Act. H.R. 624. 2013.

2.210.4 CYBERCRIME

criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime [ISO-27032:2012]

2.210.5 (EN) CYBER CRIME (OR COMPUTER CRIME)

Any crime where information and communications technology is:

- used as a tool in the commission of an offence
- the target of an offence
- a storage device in the commission of an offence.

In New Zealand some of the most common examples of cyber crime include fraud, identity theft and organised crime.

[CSS NZ:2011]

2.210.6 (EN) CYBER CRIME

is the use of cyberspace for criminal purposes as defined by national or international law.

Russia-U.S. Bilateral On Cybersecurity Critical Terminology Foundations, Apr. 2011.

2.210.7 (EN) CYBERCRIME

Also known as computer crime, cybercrime refers to any crime that involves a networked (e.g. connected to the internet) computer.

PC Security Handbook, Rich Robinson

2.211 CIBERESPACIO

2.211.1 CIBERESPACIO

Dominio global y dinámico compuesto por infraestructuras de tecnología de la información —incluyendo internet—, redes de telecomunicaciones y sistemas de información.

O.M. 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas

2.211.2 CIBERESPACIO

nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información – incluida Internet–, las redes y los sistemas de información y de telecomunicaciones

Estrategia de ciberseguridad nacional, 2013

2.211.3 CIBERESPACIO

Espacio virtual que engloba todos los sistemas TIC, tanto sistemas de información como sistemas de control industrial. El ciberespacio se apoya en la disponibilidad de Internet como red de redes, enriquecida con otras redes de transporte de datos.

Los sistemas interconectados en espacios aislados no forman parte del ciberespacio.

2.211.4 CIBERESPACIO

Conjunto de redes de comunicaciones y ordenadores existentes a nivel mundial que se encuentran interconectados directa o indirectamente entre sí. En ocasiones, este término se suele acotar y centrar en Internet, pero durante el estudio el término se ha utilizado en el sentido más amplio. [IS-DEFE-6:2009]

2.211.5 (EN) CYBERSPACE

The global environment that is created through the interconnection of communication and information systems. The cyberspace includes the physical and virtual computer networks, computer systems, digital media and data.

NATO - Cyber Security Strategy for Defence,- ACST–Strategy-CyberSecurity-001, 2014

2.211.6 (EN) CYBERSPACE:

The environment formed by physical and non-physical components, characterized by the use of computers and the electro-magnetic spectrum, to store, modify, and exchange data using computer networks.

The Tallinn Manual, 2013

2.211.7 (EN) CYBERSPACE

A global domain within the information environment consisting of the interdependent network of IT and ICS infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. [CSS US:2012]

2.211.8 (EN) THE CYBERSPACE

complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form [ISO-27032:2012]

2.211.9 (EN) CYBER SPACE

The global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems in which online communication takes place. [CSS NZ:2011]

2.211.10 (EN) CYBERSPACE

Cyberspace is the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace.[CSS DE:2011]

2.211.11 (EN) CYBERSPACE

The global domain created by communication, information and other electronic systems, their interaction and the information that is stored, processed or transmitted in these systems.

NATO AC/322-N(2014)0072

2.211.12 (EN) CYBERSPACE

is an electronic medium through which information is created, transmitted, received, stored, processed, and deleted.

Russia-U.S. Bilateral On Cybersecurity Critical Terminology Foundations, Apr. 2011.

2.211.13 (EN) CRITICAL CYBERSPACE

is cyber infrastructure and cyber services that are vital to preservation of public safety, economic stability, national security and international stability.

Russia-U.S. Bilateral On Cybersecurity Critical Terminology Foundations, Apr. 2011.

2.211.14 (EN) CYBERSPACE

Cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship. [CSS CA:2010]

2.211.15 (EN) CYBERSPACE

A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. [CNSSI_4009:2010]

2.211.16 (EN) CYBERSPACE

A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.[US MSCO:2006]

2.212 CIBERESPIONAJE

Actividades de espionaje llevadas a cabo en el ciberespacio o utilizando el ciberespacio como medio.

2.212.1 (EN) CYBER ESPIONAGE

Some of the most advanced and persistent cyber attacks on governments and critical infrastructure worldwide are thought to originate from foreign military and intelligence services or organised criminal groups. Media organisations around the world are reporting attacks on government systems, national infrastructure and businesses that have resulted in access to commercially sensitive information, intellectual property and state or trade secrets.[CSS NZ:2011]

2.212.2 (EN) CYBER ESPIONAGE

Cyber attacks directed against the confidentiality of an IT system, which are launched or managed by foreign intelligence services, are called cyber espionage. [CSS DE:2011]

2.212.3 (EN) CYBERESPIONAGE

Activities conducted in the name of security, business, politics or technology to find information that ought to remain secret. It is not inherently military.

ISACA, Cybersecurity Glossary, 2014

2.213 CIBERINCIDENTE

Ver

- *Incidente*

2.213.1 CIBERINCIDENTE

Incidente relacionado con la seguridad de las TIC que se produce en el Ciberespacio. Este término engloba aspectos como los ataques a sistemas TIC, el fraude electrónico, el robo de identidad, el abuso del Ciberespacio, etc. [ISDEFE-6:2009]

2.213.2 (EN) CYBER EVENT

An unauthorized or unexpected CIS event whose impact is minimal and recovery is easy or automatic.

NATO AC/322-N(2014)0072

2.213.3 (EN) CYBER INCIDENT

An unauthorized or unexpected CIS event where automated measures have failed, whose impact is not severe and recovery can be achieved through the involvement of cyber experts

NATO AC/322-N(2014)0072

2.213.4 (EN) CYBERSECURITY EVENT

A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).

Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, February 12, 2014

2.213.5 (EN) CYBER SECURITY INCIDENT

A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or,
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.

[NERC:2014]

2.213.6 (EN) CYBER INCIDENT

Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See incident. [CNSSI_4009:2010]

2.214 CIBERINFRAESTRUCTURA

2.214.1 CIBERINFRAESTRUCTURA

Agregado de sistemas, procesos y personas que constituyen el ciberespacio.

2.214.2 (EN) CYBER INFRASTRUCTURE:

The communications, storage, and computing resources upon which information systems operate. The internet is an example of a global information infrastructure.

The Tallinn Manual, 2013

2.214.3 (EN) CYBER INFRASTRUCTURE

is the aggregation of people, processes and systems that constitute cyberspace.

Russia-U.S. Bilateral On Cybersecurity Critical Terminology Foundations, Apr. 2011.

2.214.4 (EN) CRITICAL CYBER INFRASTRUCTURE

is the cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and to the sustainability and restoration of critical cyber-space.

Russia-U.S. Bilateral On Cybersecurity Critical Terminology Foundations, Apr. 2011.

2.215 CIBERINTELIGENCIA

2.215.1 CIBERINTELIGENCIA

Actividades de inteligencia en soporte de la ciberseguridad. Se trazan ciberamenazas, se analizan las intenciones y oportunidades de los ciberadversarios con el fin de identificar, localizar y atribuir fuentes de ciberataques.

2.215.2 (EN) CYBER INTELLIGENCE

Activities using all “intelligence” sources in support of Cyber Security to map out the general cyber threat, to collect cyber intentions and possibilities of potential adversaries, to analyse and communicate, and to identify, locate, and allocate the source of cyber-attacks.

NATO - Cyber Security Strategy for Defence,- ACST–Strategy-CyberSecurity-001, 2014

2.216 CIBEROFENSIVA

2.216.1 CIBEROFENSIVA

Capacidad ofensiva en redes y sistemas con el objetivo de limitar o destruir la capacidad operativa de un ciberadversario. Esta capacidad busca garantizar la libertad de acción propia en el ciberes-pacio. Los ciberataques se pueden lanzar bien para repeler un ataque (ciberdefensa), bien como soporte de otras operaciones.

2.216.2 (EN) CYBER OFFENSIVE

The offensive capacity includes the manipulation or disruption of networks and systems with the purpose of limiting or eliminating the adversary’s operational capability. This capability can be required to guarantee one’s freedom of action in the cyber domain. Cyber-attacks can be launched to repel an attack (active defence) or to support the operational action.

NATO - Cyber Security Strategy for Defence,- ACST–Strategy-CyberSecurity-001, 2014

2.216.1 (EN) CYBER OFFENSIVE CAPABILITY

is a capability to initiate a cyber attack that may be used as a cyber deterrent.

Russia-U.S. Bilateral On Cybersecurity Critical Terminology Foundations, Apr. 2011.

2.217 CIBEROPERACIONES

2.217.1 CIBEROPERACIONES

Empleo de las oportunidades que ofrece el ciberespacio a fin de alcanzar objetivos en o usando el ciberespacio.

2.217.2 (EN) CYBER OPERATIONS:

The employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace.

The Tallinn Manual, 2013

2.218 CIBERRECONOCIMIENTO

2.218.1 CIBERRECONOCIMIENTO

2.218.2 (EN) CYBER RECONNAISSANCE:

The use of cyber capabilities to obtain information about activities, information resources, or system capabilities

The Tallinn Manual, 2013

2.219 CIBERSEGURIDAD

2.219.1 CIBERSEGURIDAD

Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan

O.M. 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas

2.219.2 CIBERSEGURIDAD

Conjunto de actuaciones orientadas a asegurar, en la medida de lo posible, las redes y sistemas de que constituyen el ciberespacio:

- detectando y enfrentándose a intrusiones,
- detectando, reaccionando y recuperándose de incidentes, y
- preservando la confidencialidad, disponibilidad e integridad de la información.

2.219.3 CIBERSEGURIDAD

Sinónimo del termino Ciberdefensa. Normalmente el término Ciberdefensa se suele utilizar en el ámbito militar, y el termino Ciberseguridad en el ámbito civil, aunque en el presente estudio se han utilizado indistintamente ambos términos. [ISDEFE-6:2009]

2.219.4 CYBER SECURITY

The desired situation in which the protection of cyberspace is proportionate to the cyber threat and the possible consequences of cyber-attacks. At Defence Cyber Security comprises three pillars: Cyber Defence, Cyber Intelligence and cyber counter-offensive.

NATO - Cyber Security Strategy for Defence,- ACST–Strategy-CyberSecurity-001, 2014

2.219.5 (EN) CYBERSECURITY

The process of protecting information by preventing, detecting, and responding to attacks.

Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, February 12, 2014

2.219.1 (EN) CYBERSECURITY

The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems

ISACA, Cybersecurity Glossary, 2014

2.219.2 (EN) CYBER-SECURITY

Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein. [CSS EU:2013]

2.219.3 (EN) CYBERSECURITY PURPOSE

(A) In general.--The term `cybersecurity purpose' means the purpose of ensuring the integrity, confidentiality, or availability of, or safeguarding, a system or network, including protecting a system or network from--

(i) a vulnerability of a system or network;

(ii) a threat to the integrity, confidentiality, or availability of a system or network or any information stored on, processed on, or transiting such a system or network;

(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network; or

(iv) efforts to gain unauthorized access to a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network.

(B) Exclusion.--Such term does not include the purpose of protecting a system or network from efforts to gain unauthorized access to such system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

Cyber Intelligence Sharing and Protection Act. H.R. 624. 2013.

2.219.4 (EN) CYBERSECURITY SYSTEM

(A) In general.--The term `cybersecurity system' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or safeguard, a system or network, including protecting a system or network from

(i) a vulnerability of a system or network;

(ii) a threat to the integrity, confidentiality, or availability of a system or network or any information stored on, processed on, or transiting such a system or network;

(iii) efforts to deny access to or degrade, disrupt, or destroy a system or network; or

(iv) efforts to gain unauthorized access to a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network.

(B) Exclusion.--Such term does not include a system designed or employed to protect a system or network from efforts to gain unauthorized access to such system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

Cyber Intelligence Sharing and Protection Act. H.R. 624. 2013.

2.219.5 (EN) CYBERSECURITY

The ability to protect or defend the use of cyberspace from cyber attacks. [CSS US:2012]

2.219.6 (EN) CYBERSAFETY

condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable

NOTE 1 This can take the form of being protected from the event or from exposure to something that causes health or economic losses. It can include protection of people or of assets.

NOTE 2 Safety in general is also defined as the state of being certain that adverse effects will not be caused by some agent under defined conditions.

[ISO-27032:2012]

2.219.7 (EN) CYBERSECURITY

Cyberspace security

preservation of confidentiality, integrity and availability of information in the Cyberspace

NOTE 1 In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

NOTE 2 Adapted from the definition for information security in ISO/IEC 27000:2009.

[ISO-27032:2012]

2.219.8 (EN) CYBER SECURITY

The practice of making the networks that constitute cyber space as secure as possible against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them. [CSS NZ:2011]

2.219.9 (EN) CYBER SECURITY AND CIVILIAN AND MILITARY CYBER SECURITY

(Global) cyber security is the desired objective of the IT security situation in which the risks of global cyberspace have been reduced to an acceptable minimum.

Hence, cyber security in Germany is the desired objective of the IT security situation, in which the risks of the German cyberspace have been reduced to an acceptable minimum. Cyber security (in Germany) is the sum of suitable and appropriate measures.

Civilian cyber security focuses on all IT systems for civilian use in German cyberspace. Military cyber security focuses on all IT systems for military use in German cyberspace.

[CSS DE:2011]

2.219.10 (EN) CYBERSECURITY

is a property of cyber space that is an ability to resist intentional and unintentional threats and respond and recover.

Russia-U.S. Bilateral On Cybersecurity Critical Terminology Foundations, Apr. 2011.

2.219.11 (EN) CYBERSECURITY

The ability to protect or defend the use of cyberspace from cyber attacks. [CNSSI_4009:2010]

2.219.12 (EN) CYBER SECURITY

The Australian Government defines cyber security as:

'Measures relating to the confidentially, availability and integrity of information that is processed, stored and communicated by electronic or similar means.'

http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Pages/default.aspx#h2strategy

2.220 CIBERTERRORISMO

2.220.1 CIBERTERRORISMO

El ciberterrorismo o terrorismo electrónico es el uso de medios de tecnologías de información, comunicación, informática, electrónica o similar con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violación a la libre voluntad de las personas. Los fines pueden ser económicos, políticos o religiosos principalmente.

El término ha sido muy criticado, siendo considerado como un método de satanización para aquellas personas descontentas del orden establecido y que actúan en contra de éste es Internet, gracias a la libertad de ésta.

http://es.wikipedia.org/wiki/Ciberterrorismo

2.220.2 (EN) CYBER TERRORISM

is the use of cyberspace for terrorist purposes as defined by national or international law.

Russia-U.S. Bilateral On Cybersecurity Critical Terminology Foundations, Apr. 2011.

2.220.3 (EN) CYBER TERRORISM

A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.

http://cyber.law.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas

2.221 CICLO DE DEMING

Acrónimos: PDCA

Ver:

- *Sistema de gestión de la seguridad de la información (SGSI)*

2.221.1 CICLO DE DEMING

Sinónimo de Planificar Ejecutar Comprobar y Actuar. [ITIL:2007]

2.221.2 PLANIFICAR, REALIZAR, COMPROBAR, ACTUAR

(Mejora Continua del Servicio) Ciclo de gestión de Procesos en cuatro etapas, atribuido a Edward Deming. Plan-Do-Check-Act es también conocido como el Ciclo de Deming.

- PLAN: Diseñar o revisar Procesos que soportan Servicios de TI.
- DO: Implementación del Plan y gestión de los Procesos.
- CHECK: Medición de los Procesos y de los Servicios de TI, comparación con los Objetivos marcados y generación de informes.
- ACT: Planificación e implementación de Cambios para la mejora de los Procesos.

[ITIL:2007]

2.221.3 (EN) DEMING CYCLE

Synonym for Plan Do Check Act. [ITIL:2007]

2.221.4 (EN) PLAN-DO-CHECK-ACT

(Continual Service Improvement) A four stage cycle for Process management, attributed to Edward Deming. Plan-Do-Check-Act is also called the Deming Cycle.

- PLAN: Design or revise Processes that support the IT Services.
- DO: Implement the Plan and manage the Processes.
- CHECK: Measure the Processes and IT Services, compare with Objectives and produce reports
- ACT: Plan and implement Changes to improve the Processes.

[ITIL:2007]

2.221.5 (FR) CYCLE DE DEMING

Synonyme de Planifier-Faire-Vérifier-Agir (Plan-Do-Check-Act). [ITIL:2007]

2.221.6 (FR) MODELE PLANIFIER-FAIRE-VERIFIER-AGIR (PDCA)

(Amélioration continue du service) Un cycle en quatre phases pour la gestion des processus attribué à Edward Deming. Planifier-Réaliser-Vérifier-Agir est aussi appelé roue de Deming.

- PLANIFIER: Concevoir ou réviser les processus qui soutiennent les services des TI.
- REALISER: Mettre en œuvre le plan et gérer les processus.
- VÉRIFIE: Mesurer les processus et les services des TI, les comparer avec les objectifs et produite un reporting.
- AGIR: Planifier et mettre en œuvre les changements afin d'améliorer les processus.

[ITIL:2007]

2.222 CIFRADO

Ver:

- *Encripción*
- *Cifrar*

2.222.1 CIFRADO

Escrito en cifra.

Cifra. Escritura en que se usan signos, guarismos o letras convencionales, y que solo puede comprenderse conociendo la clave.

DRAE. Diccionario de la Lengua Española.

2.222.2 CIFRADO

Proceso para convertirinformación en un formato ilegible, a excepción de los titulares de una clave criptográfica específica. El cifrado se utiliza para proteger la información entre el proceso de cifrado y el proceso de descifrado (lo contrario del cifrado) de la divulgación no autorizada.

Consulte Criptografía sólida.

http://es.pcisecuritystandards.org

2.222.3 CIFRA O CIFRADO

1. Algoritmo que produce un texto cifrado mediante técnicas criptográficas (ISO-7498-2).

Es término sinónimo de "algoritmo de cifra".

2. Resultado de aplicar un algoritmo de cifra a un texto en claro. Es término sinónimo de: Texto cifrado.

Algoritmo que produce un texto cifrado mediante técnicas criptográficas (ISO-7498-2).

[Ribagorda:1997]

2.222.4 CIFRA

Transformación de una información (texto claro) en otra ininteligible (texto cifrado) según un procedimiento y usando una clave determinados, que pretende que sólo quién conozca dichos procedimiento y clave puede acceder a la información original. Es un mecanismo de seguridad. [CESID:1997]

2.222.5 CIFRA DE ALTO NIVEL

Ver Cifra estratégica. [CESID:1997]

2.222.6 CIFRA DE BAJO NIVEL

Ver Cifra táctica. [CESID:1997]

2.222.7 CIFRA ENCUBIERTA O MENSAJE DISIMULADO O ESTEGANOGRAFÍA

Procedimientos encaminados a ocultar la existencia de un mensaje (tintas invisibles, micropunto, disimulación de archivos...). [CESID:1997]

2.222.8 CIFRA ESTRATÉGICA O DE ALTO NIVEL

Cifra orientada a proporcionar confidencialidad durante un largo periodo de tiempo, aún ante criptoanálisis con medios especializados. [CESID:1997]

2.222.9 CIFRA TÁCTICA O DE BAJO NIVEL

Cifra orientada a proporcionar confidencialidad durante un tiempo limitado. [CESID:1997]

2.222.10 CIFRADO

Transformación criptográfica de datos (véase criptografía) para producir un criptograma o texto cifrado.

NOTA. El cifrado puede ser irreversible, en cuyo caso no puede realizarse el proceso de descifrado correspondiente.

[ISO-7498-2:1989]

2.222.11 (EN) ENCIPHERMENT

alternative term for encryption. [ISO-18033-1:2005]

2.222.12 (EN) ENCIPHERMENT

Encipherment (encryption) is the process of making data unreadable to unauthorized entities by applying a cryptographic algorithm (an encryption algorithm). [H.235:2005]

2.222.13 (EN) ENCIPHERMENT

The (reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data. [ISO-11770-1:1996]

2.222.14 (EN) ENCIPHERMENT

the (reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e. to hide the information content of the data. [ISO-9798-1:1997]

2.222.15 (EN) ENCIPHERMENT OR ENCRYPTION

The cryptographic transformation of data (see cryptography) to produce ciphertext.

NOTE. Encipherment may be irreversible, in which case the corresponding decipherment process cannot feasibly be performed.

[ISO-7498-2:1989]

2.222.16 (EN) ENCRYPTION:

Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure. See Strong Cryptography.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.222.17 (FR) CRYPTAGE

Processus de conversion d'informations sous une forme inintelligible, sauf pour les détenteurs de la clé cryptographique spécifique. L'utilisation du cryptage protège les informations entre les processus de cryptage et de décryptage (l'inverse du cryptage)contre toute divulgation non autorisée. Voir Cryptographie robuste.

http://fr.pcisecuritystandards.org/

2.222.18 (FR) CHIFFREMENT

Transformation réversible de données par un algorithme cryptographique pour produire du texte chiffré c'est à dire de manière à dissimuler l'information contenue dans les données. [ISO-18033-1:2005]

2.222.19 (FR) CHIFFREMENT

Transformation cryptographique de données produisant un cryptogramme.

Remarque. Le chiffrement peut être irréversible. Dans ce cas, le déchiffrement correspondant ne peut pas être effectué.

[ISO-7498-2:1989]

2.223 CIFRADO ANALÓGICO DE VOZ

Ver:

- *Secráfono*
- *Cifrado digital de voz*

2.223.1 CIFRADO ANALÓGICO DE VOZ

Procedimiento impropiamente llamado cifrado consistente en alterar alguna de las características de la señal eléctrica resultante de la audible. Por ejemplo, se pueden invertir las frecuencias de dicha señal, o dividir la banda de frecuencias y permutar las subbandas entre sí, o realizar una multiplexación en el tiempo de la misma.

Es término sinónimo de "secrafonía".

[Ribagorda:1997]

2.223.2 CIFRADO ANALÓGICO DE LA VOZ (SCRAMBLING)

Cifrado aplicado a la naturaleza analógica de la voz. [CESID:1997]

2.223.3 (EN) ANALOG VOICE ENCRYPTION (SCRAMBLING)

Encryption of analog information. However, rather than proper digital encryption, it uses to mean that the signal is messed up in an unintelligible way, but it still can be recovered.

2.224 CIFRADO ASIMÉTRICO

Ver:

- *Sistema de cifra asimétrica*
- *Técnica criptográfica asimétrica*
- *Criptografía de clave pública*
- *Sistema de cifra*

2.224.1 CRIPTOSISTEMA ASIMÉTRICO

Aquel basado en técnicas criptográficas asimétricas, cuya clave pública se usa para cifrar y cuya clave privada se emplea para descifrar.

Es término sinónimo de "criptosistema de clave pública".

[Ribagorda:1997]

2.224.2 CIFRA ASIMÉTRICA (ONE-WAY SYSTEM)

Ver Cifra de clave pública. [CESID:1997]

2.224.3 (EN) ASYMMETRIC CRYPTOGRAPHY

(I) A modern branch of cryptography (popularly known as "public- key cryptography") in which the algorithms use a pair of keys (a public key and a private key) and use a different component of the pair for each of two counterpart cryptographic operations (e.g., encryption and decryption, or signature creation and signature verification). (See: key pair, symmetric cryptography.) [RFC4949:2007]

2.224.4 (EN) ASYMMETRIC ENCRYPTION SYSTEM

System based on asymmetric cryptographic techniques whose public transformation is used for encryption and whose private transformation is used for decryption. [ISO-18033-1:2005]

2.225 CIFRADO AUTENTICADO

2.225.1 CIFRADO AUTENTICADO

Transformación de los datos con el objetivo de proteger la confidencialidad y la integridad, así como de garantizar el origen de los datos.

2.225.2 (EN) AUTHENTICATED ENCRYPTION

Transformation of a data string with the objectives of protecting data confidentiality, data integrity, and data origin authentication.

2.225.3 (EN) AUTHENTICATED ENCRYPTION

Cryptographic technique used to protect the confidentiality and guarantee the origin and integrity of data, and which consists of three component processes: an encryption algorithm, a decryption algorithm, and a method for generating keys.

2.226 CIFRADO AUTOSÍNCRONO

Ver:

- *Cifrado de flujo*
- *Cifrado de flujo síncrono*
- *Clave auto-clave*

2.226.1 CIFRADO AUTOSÍNCRONO

Cifrado de flujo que utiliza una serie cifrante tal que cada uno de sus símbolos se obtiene a partir de un cierto número de símbolos previos del texto en claro. [Ribagorda:1997]

2.226.2 (EN) SELF-SYNCHRONOUS STREAM CIPHER

stream cipher with the property that the keystream symbols are generated as a function of a secret key and a fixed number of previous ciphertext bits. [ISO-18033-1:2005]

2.227 CIFRADO DE ARCHIVOS

2.227.1 CIFRADO A NIVEL DE ARCHIVO

Técnica o tecnología (ya sea software o hardware) para cifrar todo el contenido de archivos específicos. Consulte también Cifrado de disco o Cifrado de bases de datos a nivel de columna.

http://es.pcisecuritystandards.org/

2.227.2 (EN) FILE-LEVEL ENCRYPTION:

Technique or technology (either software or hardware) for encrypting the full contents of specific files. Alternatively, see Disk Encryption or Column-Level Database Encryption.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.227.3 (FR) CRYPTAGE AU NIVEAU FICHIER

Technique ou technologie (logicielle ou matérielle) de cryptage de la totalité du contenu de fichiers spécifiques. Voir également Cryptage par disqueou Cryptage de la base de données au niveau colonne.

http://fr.pcisecuritystandards.org/

2.228 CIFRADO DE COLUMNAS EN BASES DE DATOS

2.228.1 CIFRADO DE BASES DE DATOS A NIVEL DE COLUMNA

Técnica o tecnología (ya sea software o hardware) para cifrar el contenido de una columna específica de una base de datos y no todo el contenido de toda la base de datos. Consulte también Cifrado de disco o Cifrado a nivel de archivo.

http://es.pcisecuritystandards.org/

2.228.2 (EN) COLUMN-LEVEL DATABASE ENCRYPTION

Technique or technology (either software or hardware) for encrypting contents of a specific column in a database versus the full contents of the entire database. Alternatively, see Disk Encryption or File-Level Encryption.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.228.3 (FR) CRYPTAGE DE BASE DE DONNEES AU NIVEAU DE COLONNE

Technique ou technologie (matérielle ou logicielle) de cryptage du contenu d'une colonne spécifique de la base de données au lieu de la totalité du contenu de la base de données. Voir également Cryptage de disque ou Cryptage au niveau fichier.

http://fr.pcisecuritystandards.org/

2.229 CIFRADO DE DISCO

2.229.1 CIFRADO DE DISCO

Técnica o tecnología (ya sea de software o hardware) que se utiliza para cifrar todos los datos almacenados en un dispositivo (por ejemplo, un disco duro o una unidad flash). También se utiliza el cifrado a nivel de archivo y el cifrado de bases de datos a nivel de columna para cifrar el contenido de archivos o columnas específicas.

http://es.pcisecuritystandards.org/

2.229.2 (EN) DISK ENCRYPTION:

Technique or technology (either software or hardware) for encrypting all stored data on a device (for example, a hard disk or flash drive). Alternatively, File-Level Encryption or Column-Level Database Encryption is used to encrypt contents of specific files or columns.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.229.3 (FR) CRYPTAGE PAR DISQUE

Technique ou technologie (logicielle ou matérielle) de cryptage de toutes les données stockées sur un dispositif (par exemple, disque dur ou clé USB). Le cryptage au niveau fichier ou le cryptage de base de données au niveau colonne sont également utilisés pour crypter le contenu de fichiers ou de colonnes spécifiques.

http://fr.pcisecuritystandards.org/

2.230 CIFRADO DE FLUJO

Ver:

- *Sistema de cifra*
- *Cifrado de flujo síncrono*
- *Cifrado autosíncrono*
- *Cifrado simétrico*

2.230.1 CIFRADO DE FLUJO

Algoritmo de cifra que opera sobre el texto en claro símbolo a símbolo (sea éste un bit o un carácter), por contraste con el modo de operar del cifrado de bloque.

Habitualmente esta operación es un simple o-exclusivo entre un símbolo en claro y uno de la clave (serie cifrante), en cuyo caso este cifrado se denomina cifrado Vernam.

El cifrado de flujo se denomina periódico si los símbolos de la serie cifrante se repiten tras un cierto número de ellos.

[Ribagorda:1997]

2.230.2 CIFRA EN FLUJO

Ver Cifra en serie. [CESID:1997]

2.230.3 CIFRA EN SERIE Ó EN FLUJO

Procedimiento de cifrado por sustitución en el que a cada carácter del texto en claro se le suma un carácter de la serie cifrante para obtener el texto cifrado.

Si la serie cifrante es independiente del texto claro, se denomina síncrona, mientras que si un número determinado de caracteres de la serie cifrante son función de igual número de caracteres del cripto precedente se denomina cifrado de texto con autoclave.

[CESID:1997]

2.230.4 (EN) STREAM CIPHER

(I) An encryption algorithm that breaks plain text into a stream of successive elements (usually, bits) and encrypts the n-th plaintext element with the n-th element of a parallel key stream, thus converting the plaintext stream into a ciphertext stream. [Schn] (See: block cipher.) [RFC4949:2007]

2.230.5 (EN) STREAM CIPHER

symmetric encryption system with the property that the encryption algorithm involves combining a sequence of plaintext symbols with a sequence of keystream symbols one symbol at a time, using an invertible function. Two types of stream cipher can be identified: synchronous stream ciphers and self-synchronous stream ciphers, distinguished by the method used to obtain the keystream. [ISO-18033-1:2005]

2.230.6 (EN) SYNCHRONOUS STREAM CIPHER

stream cipher with the property that the keystream symbols are generated as a function of a secret key, and are independent of the plaintext and ciphertext. [ISO-18033-1:2005]

2.231 CIFRADO DE FLUJO SÍNCRONO

Ver:

- *Cifrado de flujo*
- *Cifrado autosíncrono*

2.231.1 CIFRADO DE FLUJO SÍNCRONO

cifrador de flujo en el que la serie de símbolos de cifra depende exclusivamente de la clave, siendo independiente del texto en claro o del texto cifrado.

2.231.2 (EN) SYNCHRONIZATION

(I) Any technique by which a receiving (decrypting) cryptographic process attains an internal state that matches the transmitting (encrypting) process, i.e., has the appropriate keying material to process the cipher text and is correctly initialized to do so. [RFC4949:2007]

2.231.3 (EN) SYNCHRONOUS STREAM CIPHER

stream cipher with the property that the keystream symbols are generated as a function of a secret key, and are independent of the plaintext and ciphertext. [ISO-18033-1:2005]

2.232 CIFRADO DEL ENLACE

Ver:

- *Cifrado*
- *Cifrado extremo a extremo*

2.232.1 CIFRADO A NIVEL DE ENLACE

1. Aplicación individual de cifrado de datos en cada enlace de un sistema de comunicación (ISO-7498-2).

2. Cifrado de información realizado en el segundo nivel (enlace) del modelo OSI (Open System Interconnection).

En este cifrado tanto el propio mensaje, obtenido en el nivel de aplicación, como los datos añadidos en los niveles comprendidos entre el sexto (presentación) y el tercero (red) se transmiten cifrados. Por tanto, y a diferencia de lo que sucede en el cifrado extremo a extremo, se debe descifrar el paquete en cada nodo de la red para que éste averigüe el siguiente nodo al que mandar el mismo.

[Ribagorda:1997]

2.232.2 CIFRADO DE ENLACE

Cifrado de la información que circula por un enlace. [CESID:1997]

2.232.3 CIFRADO DE ENLACE A ENLACE (LINK-BY-LINK)

Cifrado existente en una red en la que la información circula cifrada por los enlaces de la red y en claro por sus nodos. [CESID:1997]

2.232.4 CIFRADO ENLACE POR ENLACE

Aplicación individual del cifrado a datos en cada enlace de un sistema de comunicación. (Véase también «cifrado de extremo a extremo».) [ISO-7498-2:1989]

2.232.5 (EN) LINK ENCRYPTION

(I) Stepwise (link-by-link) protection of data that flows between two points in a network, provided by encrypting data separately on each network link, i.e., by encrypting data when it leaves a host or subnetwork relay and decrypting when it arrives at the next host or relay. Each link may use a different key or even a different algorithm. [R1455]

(Compare: end-to-end encryption.)

[RFC4949:2007]

2.232.6 (EN) LINK ENCRYPTION

Encryption of information between nodes of a communications system. [CNSSI_4009:2010]

2.232.7 (EN) LINK-BY-LINK ENCIPHERMENT

The individual application of encipherment to data on each link of a communications system. (See also end-to-end encipherment.)

NOTE. The implication of link-by-link encipherment is that data will be in cleartext form in relay entities.

[ISO-7498-2:1989]

2.232.8 (FR) CHIFFREMENT DE LIAISON (LIAISON PAR LIAISON)

Application particulière du chiffrement à chaque liaison d'un système de communication (voir aussi «chiffrement de bout en bout», § 3.3.29).

Remarque. Le chiffrement liaison par liaison implique que les données soient du texte en clair dans les entités relais.

[ISO-7498-2:1989]

2.233 CIFRADO DE TEXTO CON AUTO-CLAVE

Acrónimos: CTAK

2.233.1 CIFRADO DE TEXTO CON AUTO-CLAVE O AUTOSÍNCRONO O CON REALIMENTACIÓN

Método de cifra en serie en el que se utiliza como clave de cifrado el texto cifrado obtenido anteriormente. [CESID:1997]

2.233.2 (EN) CIPHER TEXT AUTO-KEY (CTAK)

Cryptographic logic that uses previous cipher text to generate a key stream. [CNSSI_4009:2010]

2.234 CIFRADO DE VOZ

Ver:

- *Cifrado analógico de voz*
- *Cifrado digital de voz*

2.235 CIFRADO DIGITAL DE VOZ

Ver:

- *A5 - Cifrado de voz GSM*

- *Cifrado analógico de voz*

2.235.1 CIFRADO DIGITAL DE LA VOZ

Es el contenido digitalizando la voz y aplicando al resultado un algoritmo de cifra cualquiera. [Ribagorda:1997]

2.235.2 CIFRADO DIGITAL DE LA VOZ

Cifrado aplicado a la voz digitalizada o a una representación por parámetros de la misma (mediante vocoder). [CESID:1997]

2.235.3 (EN) DIGITAL VOICE ENCRYPTION

Encryption of voice when digitally encoded.

2.236 CIFRADO EN BLOQUE

Ver:

- *Sistema de cifra*
- *Cifrado simétrico*
- *Modo de operación (1)*
- *CMAC authentication mode*
- *Criptografía de clave secreta*

2.236.1 CIFRADO EN BLOQUE

Algoritmo de cifra que divide el texto en claro en bloques de igual longitud, operando sobre cada uno de éstos considerado como una unidad.

La longitud del bloque está prefijada en algunos algoritmos de cifra, como el DES o el IDEA, y en otros es variable por el usuario, como el RC-5

[Ribagorda:1997]

2.236.2 CIFRA EN BLOQUE

Procedimiento de cifrado en el que la serie de caracteres del texto claro se divide en bloques de una determinada longitud, cada uno de los cuales se transforma con un bloque de caracteres de la serie cifrante para obtener el texto cifrado.

Si existe solape entre los bloques se denomina cifra en bloques encadenados, que puede ser en modalidad criptograma (el bloque lo forman el texto claro y parte del bloque cifrado anterior), modalidad mensaje claro (el bloque lo forman el texto claro y parte del bloque de texto claro anterior) o mixto (mezcla de los dos sistemas anteriores).

Si no existe solape de bloques se denomina cifra en bloque puro.

[CESID:1997]

2.236.3 (EN) BLOCK CIPHER

An encryption algorithm that breaks plain text into fixed-size segments and uses the same key to transform each plaintext segment into a fixed-size segment of cipher text. Examples: AES, Blowfish, DEA, IDEA, RC2, and SKIPJACK. (See: block, mode. Compare: stream cipher.) [RFC4949:2007]

2.236.4 (EN) BLOCK ENCRYPTION

A block cipher encrypts one block of data at a time.

2.236.5 (EN) BLOCK CIPHER

symmetric encipherment system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext. [ISO-18033-1:2005]

2.237 CIFRADO EXTREMO A EXTREMO

Ver:

- *Cifrado*
- *Cifrado del enlace*

2.237.1 CIFRADO EXTREMO A EXTREMO

Cifrado de información entre los extremos emisor y receptor del canal de transmisión (ISO-7498-2)

Más concretamente, se denomina así al cifrado realizado en los niveles superiores (aplicación o presentación) del modelo OSI.

Presenta la ventaja de no precisar el descifrado al atravesar los sucesivos nodos de la red.

[Ribagorda:1997]

2.237.2 CIFRADO EXTREMO A EXTREMO

Cifrado de datos en el extremo origen de una información correspondiéndose con el descifrado de los mismos en el extremo destinatario, unidos a través de un circuito. [CESID:1997]

2.237.3 CIFRADO PUNTO A PUNTO

Cifrado de datos en el extremo origen de una información correspondiéndose con el descifrado de los mismos en el extremo destinatario, unidos a través de un circuito permanente. [CESID:1997]

2.237.4 CIFRADO DE EXTREMO A EXTREMO

Cifrado de datos en el interior o en el sistema extremo fuente, cuyo descifrado correspondiente se produce sólo en el interior o en el sistema extremo de destino (véase también «cifrado enlace por enlace»). [ISO-7498-2:1989]

2.237.5 (EN) END-TO-END ENCRYPTION

Encryption of information at its origin and decryption at its intended destination without intermediate decryption. [CNSSI_4009:2010]

2.237.6 (EN) END-TO-END ENCRYPTION

(I) Continuous protection of data that flows between two points in a network, effected by encrypting data when it leaves its source, keeping it encrypted while it passes through any intermediate computers (such as routers), and decrypting it only when it arrives at the intended final destination. (See: wiretapping. Compare: link encryption.) [RFC4949:2007]

2.237.7 (EN) END-TO-END ENCRYPTION

Encryption of information at its origin and decryption at its intended destination without intermediate decryption. [CNSSI_4009:2010]

2.237.8 (EN) END-TO-END ENCIPHERMENT

Encipherment of data within or at the source end system, with the corresponding decipherment occurring only within or at the destination end system. [ISO-7498-2:1989]

2.237.9 (FR) CHIFFREMENT DE BOUT EN BOUT

Chiffrement de données à l'intérieur ou au niveau du système d'extrémité source, le déchiffrement correspondant ne se produisant qu'à l'intérieur, ou au niveau du système d'extrémité de destination [ISO-7498-2:1989]

2.238 CIFRADO IRREVERSIBLE

2.238.1 CIFRADO IRREVERSIBLE

Aquél basado en un algoritmo irreversible. Se emplea, principalmente, para almacenar de manera segura contraseñas de usuarios de un sistema. Últimamente se usa también para la generación de contraseñas desechables. [Ribagorda:1997]

2.238.2 (EN) ONE-WAY ENCRYPTION

(I) Irreversible transformation of plain text to cipher text, such that the plain text cannot be recovered from the cipher text by other than exhaustive procedures even if the cryptographic key is known. (See: brute force, encryption.) [RFC4949:2007]

2.238.3 (EN) ONE-WAY ENCRYPTION

Irreversible transformation of plaintext to cipher text, such that the plaintext cannot be recovered from the cipher text by other than exhaustive procedures even if the cryptographic key is known.

2.239 CIFRADO MASIVO

2.239.1 CIFRADO MASIVO

Proceso de cifrado en el cual un único dispositivo criptográfico cifra dos o más canales de un sistema de telecomunicación. [Ribagorda:1997]

2.239.2 CIFRADO DE GRUPO O MASIVO

Cifrado simultáneo de todos los canales del multicanal de un enlace. [CESID:1997]

2.239.3 (EN) BULK ENCRYPTION

Simultaneous encryption of all channels of a multi-channel telecommunications link- [CNSSI_4009:2010]

2.239.4 (EN) BULK ENCRYPTION

1. (I) Encryption of multiple channels by aggregating them into a single transfer path and then encrypting that path. (See: channel.)

2. (O) "Simultaneous encryption of all channels of a multichannel telecommunications link." [C4009] (Compare: bulk keying material.)

[RFC4949:2007]

2.239.5 (EN) BULK ENCRYPTION

Simultaneous encryption of all channels of a multichannel telecommunications link. [CNSSI_4009:2010]

2.239.6 (EN) BULK ENCRYPTION

Simultaneous encryption of all channels of a multichannel telecommunications link.

http://www.atis.org/tg2k/_bulk_encryption.html

2.240 CIFRADOR

2.240.1 CIFRADOR

Sistema de cifrado.

2.240.1 (EN) CIPHER

Any cryptographic system in which arbitrary symbols or groups of symbols, represent units of plain text, or in which units of plain text are rearranged, or both. [CNSSI_4009:2010]

2.240.2 (EN) CIPHER

(I) A cryptographic algorithm for encryption and decryption. [RFC4949:2007]

2.240.3 (EN) CIPHER

alternative term for encipherment system. [ISO-18033-1:2005]

2.241 CIFRADO REVERSIBLE

Ver:

- *Algoritmo reversible*

2.242 CIFRADO SIMÉTRICO

Ver:

- *Criptografía de clave secreta*
- *Cifrado de flujo*
- *Cifrado de flujo*

2.242.1 CIFRADO SIMÉTRICO

Algoritmo de cifra basado en una función invertible, tal que tanto el algoritmo como su inverso dependen de un parámetro igual para ambos llamado clave secreta.

También recibe este nombre aquel algoritmo de cifra que depende de un parámetro diferente del de su inverso, pero tal que el conocimiento de uno permite, en un tiempo razonable y con unos recursos limitados, el conocimiento del otro.

[Ribagorda:1997]

2.242.2 CRIPTOSISTEMA SIMÉTRICO

Aquel basado en técnicas criptográficas simétricas. Requiere de un proceso de especificación de la clave, previo a la transformación de la in formación en claro a cifrada.

Es término sinónimo de "criptosistema de clave secreta", "criptosistema de clave única" y "criptosistema convencional".

[Ribagorda:1997]

2.242.3 TÉCNICAS CRIPTOGRÁFICAS SIMÉTRICAS

Aquella que usa la misma clave, secreta, para el algoritmo de cifrado y descifrado. Sin el conocimiento de la clave secreta es computacionalmente inviable calcular ni el algoritmo de cifrado ni el de descifrado. (ISO/IEC ISO-11770-3) [Ribagorda:1997]

2.242.4 CIFRA DE CLAVE SECRETA O CIFRA SIMÉTRICA

Sistema en el que las claves para cifrar son iguales a las de descifrar, y en el que la totalidad o la mayor parte de las claves permanecen en secreto (clave secreta). [CESID:1997]

2.242.5 (EN) SYMMETRIC CRYPTOGRAPHY

(I) A branch of cryptography in which the algorithms use the same key for both of two counterpart cryptographic operations (e.g., encryption and decryption).

(See: asymmetric cryptography. Compare: secret-key cryptography.)

[RFC4949:2007]

2.242.6 (FR) CHIFFREMENT SYMÉTRIQUE

Technique de chiffrement qui repose sur l'utilisation d'une seule clé secrète qui doit être partagée par toutes les entités qui souhaitent communiquer entre-elles de manière confidentielle. A la différence du chiffrement asymétrique c'est la même clé qui sert à la fois au chiffrement et au déchiffrement des données.

http://www.cases.public.lu/functions/glossaire/

2.243 CIFRADO VERNAM

Ver:

- *Máscara de un solo uso*
- *Cifrado de flujo*

2.243.1 CIFRADO VERNAM

Cifrado de flujo que usa una clave constituida por una sucesión de símbolos (bits o caracteres) llamada serie cifrante, operando o-exclusivo cada símbolo de ésta con el correspondiente del texto en claro. Debido a la definición de la función o exclusivo, el descifrado se realiza, igualmente, operando con dicha función cada bit de la misma serie cifrante con el correspondiente del texto cifrado. Si la serie cifrante no se repite, es aleatoria, y de longitud igual, al menos, al texto a cifrar éste cifrado alcanza el secreto perfecto. Además, es el único que verifica tal condición. Este cifrado fue ideado en 1971 por Gilbert S. Vernam -ingeniero de la compañía ATT- para ser usado en transmisión telegráfica con el código Baudot. [Ribagorda:1997]

2.243.2 (EN) VERNAM CIPHER

Cipher developed for encrypting teletype traffic by computing the exclusive or of the data bits and the key bits. This is a common approach for constructing stream ciphers.

http://www.smat.us/crypto/inet-crypto/glossary.html

2.244 CIFRAR

Ver:

- *Cifrado*

2.244.1 CIFRAR

Transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje cuyo contenido se quiere ocultar.

DRAE. Diccionario de la Lengua Española.

2.244.1 (EN) ENCIPHER

Convert plain text to cipher text by means of a cryptographic system. [CNSSI_4009:2010]

2.244.2 (EN) ENCIPHER

(D) Synonym for "encrypt". [RFC4949:2007]

2.244.3 (EN) ENCIPHER

To use a secret system to change a message into a secret that only you and your friends know how to read.

Pssst! The words encode or encypt mean the same thing as encipher!

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.244.4 (FR) CHIFFER

Appliquer un code secret â un ensemble de donnes pour en assurer la confidentialité et l'authenticité.

2.245 COMUNICACIÓN DEL RIESGO

Ver:

- *Riesgo*

2.245.1 COMUNICACIÓN Y CONSULTA

Procesos iterativos y continuos que realiza una organización para proporcionar, compartir u obtener información y para establecer el diálogo con las partes interesadas, en relación con la gestión del riesgo. [UNE-ISO GUÍA 73:2010]

NOTA 1 La información puede corresponder a la existencia, la naturaleza, la forma, la probabilidad la importancia, la evaluación, la aceptabilidad y el tratamiento de la gestión del riesgo.

NOTA 2 La consulta constituye un proceso de comunicación informada de doble sentido entre una organización y sus partes interesadas, sobre una cuestión antes de tomar una decisión o determinar una orientación sobre dicha cuestión. La consulta es:

- un proceso que impacta sobre una decisión a través de la influencia más que por la autoridad; y
- una contribución para una toma de decisión, y no una toma de decisión conjunta.

[UNE-ISO/IEC 27000:2014]

2.245.2 (EN) RISK COMMUNICATION AND CONSULTATION

continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk

NOTE 1: The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of risk.

NOTE 2: Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is:

- a process which impacts on a decision through influence rather than power; and
- an input to decision making, not joint decision making.

[ISO/IEC 27000:2014]

2.245.3 (EN) RISK COMMUNICATION

exchange of information with the goal of improving risk understanding, affecting risk perception and/or equipping people or groups to act appropriately in response to an identified risk

Annotation: Risk communication is practiced for both non-hazardous conditions and during incidents. During an incident, risk communication is intended to provide information that fosters trust and credibility in government and empowers partners, stakeholders, and the public to make the best possible decisions under extremely difficult time constraints and circumstances.

DHS Risk Lexicon, September 2008

2.246 CLASIFICACIÓN

Ver:

- *Información clasificada*
- *Agregación*
- *Clasificar*

2.246.1 CLASIFICACIÓN

Procedimiento(s) a seguir para establecer el nivel de clasificación bajo el que se tratará una cierta información.

2.246.2 (EN) CLASSIFICATION

1. (I) A grouping of classified information to which a hierarchical, restrictive security label is applied to increase protection of the data from unauthorized disclosure. (See: aggregation, classified, data confidentiality service. Compare: category, compartment.)

2. (I) An authorized process by which information is determined to be classified and assigned to a security level. (Compare: declassification.)

[RFC4949:2007]

2.247 CLASIFICAR

Ver:

- *Información clasificada*

2.247.1 CLASIFICAR

Ejecución de los procedimientos de clasificación de la información, por los que se le asigna un cierto nivel de protección.

2.247.2 (EN) CLASSIFY

(I) To officially designate an information item or type of information as being classified and assigned to a specific security level. (See: classified, declassify, security level.) [RFC4949:2007]

2.248 CLAVE

Ver:

- *Clave criptográfica*

2.248.1 CLAVE CRIPTOGRÁFICA

Valor que determina el resultado de un algoritmo de cifrado al transformar texto simple en texto cifrado. En general, la extensión de una clave determina la dificultad para descifrar el texto de un determinado mensaje.

Consulte Criptografía sólida.

http://es.pcisecuritystandards.org

2.248.2 CLAVE

Secuencia de caracteres, usualmente dígitos binarios aleatorios o pseudoaleatorios, usados inicialmente para configurar las operaciones realizadas por un equipo de cifra, determinar la señal de salida en dispositivos TRANSEC, o producir otras claves. [CESID:1997]

2.248.3 CLAVE

Secuencia de símbolos que controla las operaciones de cifrado y descifrado. [ISO-7498-2:1989]

2.248.1 (EN) KEY

A numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. [CNSSI_4009:2010]

2.248.2 (EN) KEY

1a. (I) /cryptography/ An input parameter used to vary a transformation function performed by a cryptographic algorithm. (See: private key, public key, storage key, symmetric key, traffic key. Compare: initialization value.) [RFC4949:2007]

2.248.3 (EN) KEY

sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment). [ISO/IEC ISO-11770-1:1996] [ISO-18033-1:2005]

2.248.4 (EN) KEY

A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature calculation, or signature verification). [ISO-9798-1:1997] [ISO-11770-1:1996]

2.248.5 (EN) KEY

A sequence of symbols that controls the operations of encipherment and decipherment. [ISO-7498-2:1989]

2.248.6 (EN) KEY

In cryptography, a key is a value that determines the output of an encryption algorithm when transforming plain text to ciphertext. The length of the key generally determines how difficult it will be to decrypt the ciphertext in a given message. See Strong Cryptography.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.248.7 (EN) KEY

A symbol or group of symbols used for controlling the making (cryptography) and breaking (cryptanalysis) of codes.

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.248.8 (FR) CLÉS CRYPTOGRAPHIQUES

Une valeur déterminant le résultat d'un algorithme de cryptage lorsqu'il transforme un texte clair en cryptogramme. La longueur de la clé détermine généralement le degré de difficulté du décryptage du cryptogramme d'un message donné. Voir Cryptographie robuste.

http://fr.pcisecuritystandards.org/

2.248.9 (FR) CLÉ

Série de symboles commandant les opérations de chiffrement et de déchiffrement. [ISO-7498-2:1989]

2.248.10 (FR) CLÉ / CLEF (ÉLECTRONIQUE)

Code informatique découlant le plus souvent de propriétés mathématiques autorisant les opérations de chiffrement et de déchiffrement pour un algorithme cryptographique donné. En ne considérant que les algorithmes cryptographiques sûrs et pour lesquels aucun faille de conception n'a été découverte, on peut considérer que la robustesse du chiffrement augmente avec la longueur de la clé choisie pour assurer ce chiffrement.

http://www.cases.public.lu/functions/glossaire/

2.249 CLAVE AUTO-CLAVE

Acrónimos: KAK

Ver:

- *Cifrado autosíncrono*

2.249.1 CIFRADO AUTOCLAVE

Cifrado de flujo que utiliza como serie cifrante una sucesión de símbolos predeterminada seguidos, o bien de los símbolos del propio texto en claro, o bien de los que se van obteniendo del texto cifrado.

En aquel caso, el algoritmo se denomina primer cifrado de Vigenère (Blaise de Vigenère, 1523-1596) y en éste, segundo cifrado de Vigenère.

[Ribagorda:1997]

2.249.2 CLAVE AUTO-CLAVE

Procedimiento que utiliza una clave anterior para producir otra clave. [CESID:1997]

2.249.1 (EN) KEY-AUTO-KEY (KAK)

Cryptographic logic using previous key to produce key. [CNSSI_4009:2010]

2.249.2 (EN) KEY-AUTO-KEY (KAK)

(D) "Cryptographic logic [i.e., a mode of operation] using previous key to produce key." [C4009, A1523] (See: CTAK, /cryptographic operation/ under "mode".) [RFC4949:2007]

2.250 CLAVE CRIPTOGRÁFICA

Ver:

- *Clave*

2.250.1 CLAVE CRIPTOGRÁFICA

1. Parámetro usado por un algoritmo para validar, autenticar, cifrar o descifrar un mensaje (ISO-8732)

2. Sucesión de símbolos que controlan las operaciones de cifrado y descifrado (ISO-7498-2). 3. Parámetro usado por un algoritmo criptográfico para cifrar y descifrar datos, obtener la firma digital de unos datos, verificar ésta o calcular un código de autenticación de mensajes o una función resumen (FIPS 140-1).

A menudo se expresa simplemente mediante la palabra clave.

[Ribagorda:1997]

2.250.2 (EN) CRYPTOGRAPHIC KEY (KEY)

A parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot.

Examples include:

- The transformation of plaintext data into ciphertext data,
- The transformation of ciphertext data into plaintext data,
- The computation of a digital signature from data,
- The verification of a digital signature,
- The computation of an authentication code from data,
- The verification of an authentication code from data and a received authentication code,
- The computation of a shared secret that is used to derive keying material.

[NIST-SP800-57:2007]

2.250.3 (EN) CRYPTOGRAPHIC KEY

A sequence of symbols that controls the operation of a cryptographic transformation.

EXAMPLE: A cryptographic transformation may include but not limited to encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification.

[ISO-19790:2006]

2.250.4 (EN) CRYPTOGRAPHIC KEY

a parameter used in conjunction with a cryptographic algorithm that determines

- the transformation of plaintext data into ciphertext data,
- the transformation of ciphertext data into plaintext data,
- a digital signature computed from data,
- the verification of a digital signature computed from data,
- an authentication code computed from data, or
- an exchange agreement of a shared secret.

[FIPS-140-2:2001]

2.251 CLAVE CUSTODIADA

2.251.1 CLAVE CUSTODIADA

Sistema de gestión de claves que supone la existencia de una institución (pública o privada) confiable que almacenan una clave criptográfica, custodiándola en nombre de su legítimo propietario.

Usualmente, el sistema conlleva el uso de claves criptográficas constituidas por dos, o más, componentes, que aisladamente no permiten la reconstrucción de la clave. Cada una de estas componentes se almacena y custodia en una institución confiable diferente. Estas instituciones sólo entregan la componente en ellas depositada bajo requerimiento judicial, permitiendo así la recomposición de la clave criptográfica del dispositivo.

Este tipo de claves se ha popularizado a partir de la iniciativa presidencial estadounidense denominada Clipper-chip.

[Ribagorda:1997]

2.251.2 (EN) ESCROW PASSWORDS

Escrow Passwords are passwords that are written down and stored in a secure location (like a safe) that are used by emergency personnel when privileged personnel are unavailable.

2.252 CLAVE DE ARRANQUE

Acrónimos: CIK

2.252.1 CLAVE DE ARRANQUE

Clave que modifica o desbloquea las claves contenidas en un equipo por lo que, cuando no se prevé la utilización del equipo y dicha clave no está cargada, no se precisa borrar el resto de claves por motivos de seguridad pues el equipo no está activado. Suele estar contenida en un módulo de claves. [CESID:1997]

2.252.1 (EN) CRYPTOGRAPHIC IGNITION KEY (CIK)

Device or electronic key used to unlock the secure mode of crypto-equipment. [CNSSI_4009:2010]

2.252.2 (EN) MASTER CRYPTOGRAPHIC IGNITION KEY

Key device with electronic logic and circuits providing the capability for adding more operational CIKs to a keyset. [CNSSI_4009:2010]

2.252.3 (EN) CRYPTOGRAPHIC IGNITION KEY (CIK)

1. (N) A physical (usually electronic) token used to store, transport, and protect cryptographic keys and activation data. (Compare: dongle, fill device.)

2. (O) "Device or electronic key used to unlock the secure mode of cryptographic equipment." [C4009] Usage: Abbreviated as "crypto- ignition key".

[RFC4949:2007]

2.253 CLAVE DÉBIL

Ver:

- *Clave*

2.253.1 CLAVE DÉBIL

Valor particular de una clave criptográfica de la que resulta un criptosistema más vulnerable que el obtenido con claves no débiles. Existen también claves débiles para las funciones resumen y los algoritmos de firma digital. [Ribagorda:1997]

2.253.2 (EN) WEAK KEY

(I) In the context of a particular cryptographic algorithm, a key value that provides poor security. (See: strong.) [RFC4949:2007]

2.253.3 (EN) WEAK KEY

In a key-based cryptosystems, those key values that ease attacks because the cryptographic function becomes too simple to hide data effectively.

2.254 CLAVE DE CIFRADO DE CLAVES

Acrónimos: KEK

Ver:

- *Clave maestra*
- *Clave para envolver claves*
- *Clave*

2.254.1 CLAVE DE CIFRADO DE CLAVES

Clave criptográfica que se emplea para cifrar otras claves (ISO-8732) Es de utilidad en la protección de estas últimas sea durante su almacenamiento o transmisión.

Es término sinónimo de "clave maestra".

[Ribagorda:1997]

2.254.2 CLAVE DE CIFRADO DE CLAVES

Clave utilizada para cifrar otras claves a fin de protegerlas en su transmisión o almacenamiento. [CESID:1997]

2.254.1 (EN) KEY-ENCRYPTION-KEY (KEK)

Key that encrypts or decrypts other key for transmission or storage. [CNSSI_4009:2010]

2.254.2 (EN) KEY-ENCRYPTING KEY (KEK)

(I) A cryptographic key that (a) is used to encrypt other keys (either DEKs or other TEKs) for transmission or storage but (b) (usually) is not used to encrypt application data. Usage: Sometimes called "key-encryption key". [RFC4949:2007]

2.254.3 (EN) KEY ENCRYPTING KEY

A cryptographic key that is used for the encryption or decryption of other keys. [NIST-SP800-57:2007]

2.254.4 (EN) KEY ENCRYPTION KEY

a cryptographic key that is used for the encryption or decryption of other keys.[ISO-19790:2006]

2.254.5 (EN) KEY ENCRYPTING KEY

a cryptographic key that is used for the encryption or decryption of other keys. [FIPS-140-2:2001]

2.255 CLAVE DE SESIÓN

Ver:

- *Clave*
- *Clave maestra*

2.255.1 CLAVE DE SESIÓN

Clave criptográfica que se usa sólo durante un tiempo limitado. Generalmente, es transportada a través de una red de transmisión cifrada bajo otra clave. [Ribagorda:1997]

2.255.2 CLAVE DE SESIÓN

Clave, habitualmente generada de forma aleatoria y transmitida en claro o cifrada a través de la línea al principio del mensaje, que modifica las claves cargadas en el equipo o determina el punto de la serie cifrante en que empieza el cifrado, y que se utiliza únicamente en el cifrado de un mensaje. También puede aprovecharse para sincronizar los equipos de cifra. [CESID:1997]

2.255.3 (EN) SESSION KEY

(I) In the context of symmetric encryption, a key that is temporary or is used for a relatively short period of time. (See: ephemeral, KDC, session. Compare: master key.) [RFC4949:2007]

2.255.4 (EN) SESSION KEY

In the context of symmetric encryption, a key that is temporary or is used for a relatively short period of time. Usually, a session key is used for a defined period of communication between two computers, such as for the duration of a single connection or transaction set, or the key is used in an application that protects relatively large amounts of data and, therefore, needs to be re-keyed frequently.

http://www.sans.org/security-resources/glossary-of-terms/

2.256 CLAVE DE UN SOLO USO

Ver:

- *Clave*
- *Máscara de un solo uso*
- *Criptosistema de un solo uso*
- *Clave efímera*

2.256.1 CLAVE DE USO ÚNICO

Clave cuyo uso no se repite en un criptosistema. [CESID:1997]

2.256.2 (EN) ONE-TIME KEY

A key that is used only once.

2.257 CLAVE EFÍMERA

Ver:

- *Clave*
- *Clave de un solo uso*

2.257.1 CLAVE EFÍMERA

Dícese de las claves criptográficas de corta duración o que simplemente sólo se usan una vez.

2.257.2 (EN) EPHEMERAL

(I) /adjective/ Refers to a cryptographic key or other cryptographic parameter or data object that is short-lived, temporary, or used one time. (See: session key. Compare: static.) [RFC4949:2007]

2.257.3 (EN) EPHEMERAL KEY

A cryptographic key that is generated for each execution of a key establishment process and that meets other requirements of the key type (e.g., unique to each message or session).

In some cases ephemeral keys are used more than once, within a single session (e.g., broadcast applications) where the sender generates only one ephemeral key pair per message and the private key is combined separately with each recipients public key.

[NIST-SP800-57:2007]

2.258 CLAVE FRAGMENTADA

Ver:

- *Conocimiento parcial*

2.258.1 ESQUEMA UMBRAL

Protocolo de compartición de secretos mediante el cual una Tercera Parte Confiable divide en partes una información secreta inicial y las distribuye de modo seguro a varias entidades, de modo que se cumple que conociendo a partir de un número determinado de dichas partes, umbral, es posible recuperar fácilmente la información secreta mientras que el conocimiento de un número de partes menor al umbral no proporciona ningún conocimiento sobre el secreto o el resto de las partes distribuidas. [CESID:1997]

2.258.2 (EN) SPLIT KEY

(I) A cryptographic key that is generated and distributed as two or more separate data items that individually convey no knowledge of the whole key that results from combining the items. (See: dual control, split knowledge.) [RFC4949:2007]

2.258.3 (EN) KEY SPLITTING

The process of dividing a private key into multiple pieces and sharing those pieces among several users. A designated number of users must bring their shares of the key together to use the key.

http://www.watchguard.com/glossary/

2.258.4 (EN) SPLIT KEY

A cryptographic key that is divided into two or more separate data items that individually convey no knowledge of the whole key that results from combining the items.

http://www.sans.org/security-resources/glossary-of-terms/

2.259 CLAVE MAESTRA

Ver:

- *Clave de cifrado de claves*
- *Clave de sesión*
- *Clave*

2.259.1 CLAVE MAESTRA

Clave criptográfica cuyo cometido es cifrar otras claves durante la transmisión de las mismas, o bien durante su almacenamiento. [Ribagorda:1997]

2.259.2 CLAVE MAESTRA O PRIMARIA

Clave de menor jerarquía que la clave estructural, pero de máxima jerarquía entre las que se cambian. [CESID:1997]

2.260 CLAVE PARA ENVOLVER CLAVES

Ver:

- *Clave de cifrado de claves*
- *Clave*
- *Clave criptográfica*

2.260.1 CLAVE PARA ENVOLVER CLAVES

Cómo proteger una clave con otra para proteger su seguridad.

2.260.2 (EN) KEY WRAPPING

A method of encrypting keys (along with associated integrity information) that provides both confidentiality and integrity protection using a symmetric key. [NIST-SP800-57:2007]

2.260.3 (EN) KEY WRAPPING KEY

A symmetric key encrypting key. [NIST-SP800-57:2007]

2.261 CLAVE PRIVADA

Ver:

- *Par asimétrico de claves*

2.261.1 CLAVE PRIVADA

En un criptosistema asimétrico, clave criptográfica de un usuario conocida por el mismo (ISO/IEC 9594-2, ITU-T X.509).

La denominación de secreta para esta clave está en desuso, pues da lugar a confusión con la clave de los criptosistemas simétricos denominada, con más propiedad, secreta.

[Ribagorda:1997]

2.261.2 CLAVE PRIVADA

Clave que se utiliza con un algoritmo criptográfico asimétrico y cuya posesión está restringida (usualmente a una sola entidad). [X.810:1995]

(en) private key

In an asymmetric cryptography scheme, the private or secret key of a key pair which must be kept confidential and is used to decrypt messages encrypted with the public key or to digitally sign messages, which can then be validated with the public key. [CNSSI_4009:2010]

2.261.3 (EN) PRIVATE KEY

1. (I) The secret component of a pair of cryptographic keys used for asymmetric cryptography. (See: key pair, public key, secret key.)

2. (O) In a public key cryptosystem, "that key of a user's key pair which is known only by that user." [X509]

[RFC4949:2007]

2.261.4 (EN) PRIVATE KEY

A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public. In an asymmetric (public) cryptosystem, the private key is associated with a public key. Depending on the algorithm, the private key may be used to:

- Compute the corresponding public key,
- Compute a digital signature that may be verified by the corresponding public key,
- Decrypt data that was encrypted by the corresponding public key, or
- Compute a piece of common shared data, together with other information.

[NIST-SP800-57:2007]

2.261.5 (EN) PRIVATE KEY

that key of an entitys asymmetric key pair which should only be used by that entity

[ISO/IEC ISO-11770-1:1996].

NOTE. A private key should not normally be disclosed.

[ISO-18033-1:2005]

2.261.6 (EN) PRIVATE KEY; SECRET KEY (DEPRECATED)

(In a public key cryptosystem) that key of a user's key pair which is known only by that user. [X.509:2005]

2.261.7 (EN) PRIVATE KEY OR PRIVATE NUMBER

that data item, key or number, of an asymmetric pair, that shall be kept secret and should only be used by a claimant in accordance with an appropriate response formula, thereby establishing its identity. [ISO-9798-5:2004]

2.261.8 (EN) PRIVATE KEY

That key of an entity's asymmetric key pair which can only be used by that entity.

NOTE. In the case of an asymmetric signature system the private key defines the signature transformation. In the case of an asymmetric encipherment system the private key defines the decipherment transformation.

[ISO-11770-3:2008]

2.261.9 (EN) PRIVATE KEY

That key of an entity's asymmetric key pair which shall normally only be known by that entity. [ISO-11770-3:2008]

2.261.10 (EN) PRIVATE KEY

that key of an entity's asymmetric key pair which should only be used by that entity [ISO-9798-1:1997]

2.261.11 (EN) PRIVATE KEY

A key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity). [X.810:1995]

2.261.12 (FR) CLÉ PRIVÉE

clé qui est utilisée avec un algorithme asymétrique de cryptographie et dont la possession est limitée (habituellement à une seule entité). [X.810:1995]

2.261.13 (FR) CLÉ PRIVÉE

Une des deux clés du couple clé publique/clé privée tenue secrète et uniquement connue par son possesseur. Elle intervient dans le mécanisme de déchiffrement et permet de signer électroniquement des messages.

http://www.cases.public.lu/functions/glossaire/

2.262 CLAVE PÚBLICA

Ver:

- *Par asimétrico de claves*
- *Clave*
- *Clave criptográfica*

2.262.1 CLAVE PÚBLICA

(En un critposistema de claves públicas) clave de un par de claves de usuario que es conocida públicamente. [X.509:2005]

2.262.2 CLAVE PÚBLICA

En un criptosistema asimétrico, clave criptográfica de un usuario que se hace de público conocimiento (ISO/IEC 9594-2, ITU-T X.509). [Ribagorda:1997]

2.262.3 CLAVE PÚBLICA

Clave que se utiliza con un algoritmo criptográfico asimétrico y que puede estar disponible públicamente. [X.810:1995]

2.262.4 (EN) PUBLIC KEY

A cryptographic key that may be widely published and is used to enable the operation of an asymmetric cryptography scheme. This key is mathematically linked with a corresponding private key. Typically, a public key can be used to encrypt, but not decrypt, or to validate a signature, but not to sign. [CNSSI_4009:2010]

2.262.5 (EN) PUBLIC KEY

1. (I) The publicly disclosable component of a pair of cryptographic keys used for asymmetric cryptography. (See: key pair. Compare: private key.)

2. (O) In a public key cryptosystem, "that key of a user's key pair which is publicly known." [X509]

[RFC4949:2007]

2.262.6 (EN) PUBLIC KEY

A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public. In an asymmetric (public) cryptosystem, the public key is associated with a private key. The public key may be known by anyone and, depending on the algorithm, may be used to:

- Verify a digital signature that is signed by the corresponding private key,
- Encrypt data that can be decrypted by the corresponding private key, or
- Compute a piece of shared data.

[NIST-SP800-57:2007]

2.262.7 (EN) PUBLIC KEY

that key of an entitys asymmetric key pair which can be made public [ISO/IEC ISO-11770-1:1996]. [ISO-18033-1:2005]

2.262.8 (EN) PUBLIC KEY

(In a public key cryptosystem) that key of a user's key pair which is publicly known. [X.509:2005]

2.262.9 (EN) PUBLIC KEY OR PUBLIC NUMBER

That data item, key or number, of an asymmetric pair, that can be made public and shall be used by every verifier for establishing the claimant's identity. [ISO-9798-5:2004]

2.262.10 (EN) PUBLIC KEY

that key of an entity's asymmetric key pair which can be made public.

NOTE. In the case of an asymmetric signature system the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group.

[ISO-11770-3:2008]

2.262.11 (EN) PUBLIC KEY

That key of an entity's asymmetric key pair which can be made public.

NOTE. In the case of an asymmetric signature system, the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group.

[ISO-9798-1:1997]

2.262.12 (EN) PUBLIC KEY

A key that is used with an asymmetric cryptographic algorithm and that can be made publicly available. [X.810:1995]

2.262.13 (FR) CLÉ PUBLIQUE

(dans un système de chiffrement avec clé publique) celle des clés d'une paire de clés d'un utilisateur qui est connue de manière publique. [X.509:2005]

2.262.14 (FR) CLÉ PUBLIQUE

Une des deux clés du couple clé publique/clé privée rendue publique et connue par tous. Elle intervient dans le mécanisme de chiffrement et permet de chiffrer électroniquement des messages à l'intention du détenteur de cette clef, message qui sera ensuite déchiffré par la clé privée. [ISO-9798-1:1997]

2.262.15 (FR) CLÉ PUBLIQUE

clé qui est utilisée avec un algorithme asymétrique de cryptographie et qui peut être rendue publique. [X.810:1995]

2.263 CLAVE SECRETA

Ver:

- *Clave*
- *Clave criptográfica*
- *Criptografía de clave secreta*

2.263.1 CLAVE SECRETA

En un criptosistema simétrico, clave criptográfica compartida por dos entidades (ISO/IEC ISO-10181-2) [Ribagorda:1997]

2.263.2 CLAVE SECRETA

Clave que se utiliza con un algoritmo criptográfico simétrico. La posesión de una clave secreta está restringida (usualmente a dos entidades). [X.810:1995]

2.263.3 (EN) SECRET KEY

A cryptographic key that is used with a symmetric cryptographic algorithm that is uniquely associated with one or more entities and is not made public. The use of the term “secret” in this context does not imply a classification level, but rather implies the need to protect the key from disclosure. [CNSSI_4009:2010]

2.263.4 (EN) SECRET KEY

(D) A key that is kept secret or needs to be kept secret. [RFC4949:2007]

2.263.5 (EN) SECRET KEY

A cryptographic key that is used with a secret key (symmetric) cryptographic algorithm that is uniquely associated with one or more entities and is not made public. The use of the term secret in this context does not imply a classification level, but rather implies the need to protect the key from disclosure. [NIST-SP800-57:2007]

2.263.6 (EN) SECRET KEY

a cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public. [ISO-19790:2006]

2.263.7 (EN) SECRET KEY

key used with symmetric cryptographic techniques by a specified set of entities [ISO/IEC ISO-11770-3:1999]. [ISO-18033-1:2005]

2.263.8 (EN) PRIVATE KEY; SECRET KEY (DEPRECATED)

(In a public key cryptosystem) that key of a user's key pair which is known only by that user. [X.509:2005]

2.263.9 (EN) SECRET KEY

A key used with symmetric cryptographic techniques and usable only by a set of specified entities. [ISO-13888-1:2004]

2.263.10 (EN) SECRET KEY

a key used with symmetric cryptographic techniques by a set of specified entities. [ISO-15946-3:2002]

2.263.11 (EN) SECRET KEY

A key used with symmetric cryptographic techniques by a specified set of entities. [ISO-11770-3:2008]

2.263.12 (EN) SECRET KEY

A key that is used with a symmetric cryptographic algorithm. Possession of a secret key is restricted (usually to two entities). [X.810:1995]

2.263.13 (FR) CLÉ SECRÈTE

clé qui est utilisée avec un algorithme symétrique de cryptographie. La possession de cette clé est limitée (habituellement à deux entités). [X.810:1995]

2.264 CLAVES ENCAPSULADAS

Ver:

- *Recuperación de claves*
- *Clave*
- *Clave criptográfica*

2.264.1 CLAVES ENCAPSULADAS

Técnica utilizada para recuperar claves de cifra. Consiste en proteger una clave criptográficamente de forma que una tercera persona pueda recuperarla.

2.264.2 (EN) KEY ENCAPSULATION

(N) A key recovery technique for storing knowledge of a cryptographic key by encrypting it with another key and ensuring that only certain third parties called "recovery agents" can perform the decryption operation to retrieve the stored key. Key encapsulation typically permits direct retrieval of a secret key used to provide data confidentiality. (Compare: key escrow.) [RFC4949:2007]

2.265 CLAVE SIMÉTRICA

Ver:

- *Clave*
- *Clave criptográfica*
- *Algoritmo criptográfico simétrico*

2.265.1 CLAVE SIMÉTRICA

Clave secreta que se usa en criptografía de secreto compartido (criptografía simétrica).

2.265.2 (EN) SYMMETRIC KEY

A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code. [CNSSI_4009:2010]

2.265.3 (EN) SYMMETRIC KEY

(I) A cryptographic key that is used in a symmetric cryptographic algorithm. (See: symmetric cryptography.) [RFC4949:2007]

2.265.4 (EN) SYMMETRIC KEY

A single cryptographic key that is used with a secret (symmetric) key algorithm. [NIST-SP800-57:2007]

2.266 CMAC AUTHENTICATION MODE

Acrónimos: CMAC

Ver:

- [NIST-SP800-38B:2005]
- *HMAC - Hash-based Message Authentication Code*

2.266.1 CMAC AUTHENTICATION MODE

Mecanismo de autenticación de mensajes basado en el empleo de un elemento cifrador.

2.266.2 (EN) CMAC AUTHENTICATION MODE

CMAC stands for cipher-based message authentication code (MAC), analogous to HMAC, the hash-based MAC algorithm.

2.266.3 (EN) CMAC

(N) A message authentication code [SP38B] that is based on a symmetric block cipher. (See: block cipher.) [RFC4949:2007]

2.267 CMS - CRYPTOGRAPHIC MESSAGE SYNTAX

Acrónimos: CMS

Ver:

- http://www.ietf.org/rfc/rfc3852
- *PKCS #7*

2.267.1 CMS - CRYPTOGRAPHIC MESSAGE SYNTAX

Formato estándar que se emplea para firmar electrónicamente, transportar resúmenes, autenticar a las partes o cifrar datos.

2.267.2 (EN) CRYPTOGRAPHIC MESSAGE SYNTAX (CMS)

(I) An encapsulation syntax (RFC 3852) for digital signatures, hashes, and encryption of arbitrary messages. [RFC4949:2007]

2.267.3 (EN) CMS - CRYPTOGRAPHIC MESSAGE SYNTAX

Standard syntax that is used to digitally sign, digest, authenticate, or encrypt arbitrary message content.

2.268 CODIFICACIÓN SEGURA

2.268.1 CODIFICACIÓN SEGURA

El proceso de creación e implementación de aplicaciones resistentes a alteración y/o exposición a riesgos.

http://es.pcisecuritystandards.org/

2.268.2 (EN) SECURE CODING:

The process of creating and implementing applications that are resistant to tampering and/or compromise.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.268.3 (FR) CODAGE SÉCURISÉ

Processus de création et de mise en œuvre d'applications résistant aux altérations et/ou aux compromissions.

http://fr.pcisecuritystandards.org/

2.269 CODIFICAR

Ver:

- *Código*
- *Descodificar*

2.269.1 CODIFICAR

Transformar mediante las reglas de un código la formulación de un mensaje.

DRAE. Diccionario de la Lengua Española.

2.269.2 (EN) ENCODE

Convert plain text to cipher text by means of a code. [CNSSI_4009:2010]

2.270 CÓDIGO

Ver:

- *Codificar*
- *Descodificar*
- *Libro de códigos*
- *Sustitución*

2.270.1 CÓDIGO

Conjunto de reglas que transforman los elementos de un conjunto de símbolos en los elementos de otro. Los símbolos pueden ser bits, caracteres o ristras de ambos.

A diferencia de la cifra, que es función al menos de una clave criptográfica, esta transformación no depende más que de los símbolos. A pesar de ello, algunos emplean ambos términos como si fuesen sinónimos.

En su uso para ocultar información, se usan códigos constituidos por miles de frases, palabras, sílabas o letras con sus correspondientes símbolos que reemplazan a aquellos. En cierto sentido se puede considerar como un alfabeto de cifrado gigante en el que la unidad de texto en claro es la palabra o frase, utilizándose las letras o sílabas para deletrear las palabras no presentes en el código.

[Ribagorda:1997]

2.270.1 (EN) CODE

System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length. [CNSSI_4009:2010]

2.270.2 (EN) CODE

2. (I) /cryptography/ An encryption algorithm based on substitution; i.e., a system for providing data confidentiality by using arbitrary groups (called "code groups") of letters, numbers, or symbols to represent units of plain text of varying length. (See: codebook, cryptography.)

3. (I) An algorithm based on substitution, but used to shorten messages rather than to conceal their content.

[RFC4949:2007]

2.270.3 (EN) CODE

A system of changing entire words or phrases into something else.

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.270.4 (EN) CODEMAKER

A person who makes new secret codes and ciphers.

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.270.5 (EN) CODEBREAKER

A person who uses cryptanalysis to solve secret codes and ciphers without having the key.

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.271 CÓDIGO DAÑINO

Acrónimos: Malware

Ver:

- *Bomba lógica*
- *Caballo de Troya*
- *Virus*
- *Gusano informático*
- http://en.wikipedia.org/wiki/Malware

2.271.1 SOFTWARE MALICIOSO O MALWARE

Software o firmware desarrollado para infiltrarse en una computadora o dañarla sin conocimiento ni consentimiento del propietario, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, las aplicaciones o el sistema operativo del propietario. Por lo general, esta clase de software se infiltra en una red durante diversas actividades aprobadas por el negocio, lo que permite explotar las vulnerabilidades del sistema. Algunos ejemplos son los virus, gusanos, troyanos (o caballos de Troya), spyware, adware y rootkits.

http://es.pcisecuritystandards.org

2.271.2 MALWARE MALICIOUS SOFTWARE

también (del inglés llamado badware o software malicioso) es un software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento de su dueño y con finalidades muy diversas ya que en esta categoría encontramos desde un troyano hasta un spyware.

Esta expresión es un término general muy utilizado por profesionales de la computación para definir una variedad de softwares o programas de códigos hostiles e intrusivos. Muchos usuarios de computadores no están aún familiarizados con este término y otros incluso nunca lo han utilizado. Sin embargo la expresión "virus informático" es más utilizada en el lenguaje cotidiano y a menudo en los medios de comunicación para describir todos los tipos de malware.

http://es.wikipedia.org/wiki/Malware

2.271.3 CÓDIGO MALICIOSO

Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.271.4 (EN) MALICIOUS SOFTWARE / MALWARE:

Software designed to infiltrate or damage a computer system without the owner‹s knowledge or consent. Such software typically enters a network during many business-approved activities,

which results in the exploitation of system vulnerabilities. Examples include viruses, worms, Trojans (or Trojan horses), spyware, adware, and rootkits.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.271.5 (EN) MALICIOUS CODE

Software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.

http://www.sans.org/security-resources/glossary-of-terms/

2.271.6 (EN) MALWARE

A generic term for a number of different types of malicious code.

http://www.sans.org/security-resources/glossary-of-terms/

2.271.7 (EN) MALICIOUS LOGIC:

Instructions and data that may be stored in software, firmware, or hardware that is designed or intended adversely to affect the performance of a computer system. The term 'logic' refers to any set of instructions, be they in hardware, firmware, or software, executed by a computing device. Examples of malicious logic include Trojan horses, rootkits, computer viruses, and computer worms. Firmware comprises a layer between software (i.e., applications and operating systems) and hardware and consists of low-level drivers that act as an interface between hardware and software.

The Tallinn Manual, 2013

2.271.8 (EN) MALICIOUS CODE

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. [NIST-SP800-53:2013]

2.271.9 (EN) MALWARE

Malicious software or potentially unwanted software installed without informed user consent, generally covering a range of software programmes designed to attack, or prevent the intended use of information and communications networks. [CSS NZ:2011]

2.271.10 (EN) MALICIOUS CODE

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. [CNSSI_4009:2010]

2.271.11 (EN) MALICIOUS APPLETS

Small application programs that are automatically downloaded and executed and that perform an unauthorized function on an information system. [CNSSI_4009:2010]

2.271.12 (EN) MALICIOUS LOGIC

Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. [CNSSI_4009:2010]

2.271.13 (EN) MALWARE

malicious software, such as a virus or a trojan horse, designed specifically to damage or disrupt a system. [ISO-18028-4:2005]

2.271.14 (EN) MALWARE

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victims data, applications, or operating system or of otherwise annoying or disrupting the victim. [NIST-SP800-94:2007] [NIST-SP800-83:2005]

2.271.15 (EN) MALICIOUS CODE

A virus, worm, Trojan horse, or other code-based entity that infects a host. [NIST-SP800-61:2004]

2.271.16 (EN) MALWARE

is software designed to infiltrate or damage a computer system, without the owner's informed consent. The term is a portmanteau word of "malicious" and "software", and refers to the intent of the creator, rather than any specific behaviors. It includes computer viruses, worms, Trojan horses, spyware, adware, and other malicious and unwanted software. In law, malware is sometimes known as a computer contaminant, for instance in the legal codes of California, West Virginia, and several other U.S. states.

2.271.17 (EN) MALWARE

All types of software that prevent users from using their computers as they were intended. This includes hostile java applets, ActiveX vandals, Trojan horses, script vandals and viruses that are designed to corrupt or steal digital information.

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.271.18 (EN) MALICIOUS SOFTWARE

Malicious Software encompassing viruses, worms and Trojan horses amongst other bits of code.

http://www.enisa.europa.eu/

2.271.19 (EN) MALWARE

A generic term (short for malicious software) that describes a variety of malicious programs that may be installed on machines with or without the users knowledge. Also called scumware; sub-categories include viruses, worms, spyware and others.

http://www.csoonline.com/glossary/

2.271.20 (EN) MALWARE

Malware (for "malicious software") is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses, and also spyware, programming that gathers information about a computer user without permission.

http://searchsoftwarequality.techtarget.com/glossary/

2.271.21 (FR) LOGICIEL MALVEILLANT / MALICIEL

Logiciel ou firmware conçu pour infiltrer ou endommager un système informatique sans l'approbation ou la connaissance de son propriétaire, avec l'intention de compromettre la confidentialité, l'intégrité ou la disponibilité des données, des applications ou du système d'exploitation du propriétaire. Ce type de logiciel s'introduit généralement dans un réseau au cours d'activités approuvées par l'entreprise, et exploite les vulnérabilités du système. Les virus, les chevaux de Troie, les logiciels spyware et adware et les outils de dissimulation d'activité en sont des exemples.

http://fr.pcisecuritystandards.org/

2.271.22 (FR) MALWARE

Contraction de "malicious software"Les malwares correspondent aux programmes de type virus, vers ou chevaux de Troie développés dans le but de nuire au fonctionnement normal d'un système et de porter atteinte à ses utilisateurs.

http://www.cases.public.lu/functions/glossaire/

2.271.23 (FR) MALWARE

Contraction de "malicious software", le terme malware désigne les programmes spécifiquement conçus pour endommager ou entraver le fonctionnement normal d'un système, tels que les virus, les vers, les chevaux de Troie, ainsi que certains javascripts ou applets java hostiles. Cette famille ne doit pas être confondue avec les spywares (espiogiciels), autre famille de logiciels dont le fonctionnement est également contestable mais dont le but premier n'est pas de nuire à l'intégrité d'un système. Les antivirus détectent et éliminent une grande partie des malwares sans toutefois pouvoir jamais atteindre 100% d'efficacité 100% du temps: il reste donc indispensable de n'exécuter un programme ou un fichier joint que si sa sûreté est établie avec certitude, le doute profitant toujours aux malwares.

http://www.secuser.com/glossaire/

2.272 CÓDIGO DE AUTENTICACIÓN DE MENSAJES

Acrónimos: MAC

Ver:

- *Algoritmo de cálculo de códigos de autenticación de mensajes*
- *Función de verificación criptográfica*
- *Detector de manipulación*

2.272.1 CÓDIGO DE AUTENTICACIÓN DE MENSAJES

1. Campo de datos (código) usado para validar la fuente y parte, o todo, del texto de un mensaje. El código es el resultado de una operación preconvenida (ISO-8732).

2. Valor de verificación criptográfico usado como mecanismo de integridad de datos (ISO/IEC ISO-11770-1).

3. Sucesión de bits obtenidos de un conjunto de datos (en claro o cifrados) con el concurso de una clave, que son anexados a dicho conjunto con el fin de permitir la autenticación del mismo.

Es de recalcar la improcedencia de la palabra código en el término definido, pues el resultado se obtiene por aplicación de un algoritmo y nunca de un código.

[Ribagorda:1997]

2.272.2 CÓDIGO DE AUTENTICACIÓN DE MENSAJE

Código, resultado de un cálculo preestablecido, añadido a un mensaje entre dos corresponsales usado para autenticar el origen y parte o la totalidad del texto del mensaje. [CESID:1997]

2.272.1 (EN) MESSAGE AUTHENTICATION CODE

(1) See checksum.

(2) A specific ANSI standard for a checksum.

[CNSSI_4009:2010]

2.272.2 (EN) MESSAGE AUTHENTICATION CODE (MAC), MESSAGE AUTHENTICATION CODE

1. (N) /capitalized/ A specific ANSI standard for a checksum that is computed with a keyed hash that is based on DES. [A9009] Usage: a.k.a. Data Authentication Code, which is a U.S. Government standard. [FP113] (See: MAC.) [RFC4949:2007]

2.272.3 (EN) MESSAGE AUTHENTICATION CODE (MAC)

A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of data. [NIST-SP800-57:2007]

2.272.4 (EN) AUTHENTICATION CODE

a cryptographic checksum based on an approved security function

NOTE. Also known as a Message Authentication Code (MAC).

[ISO-19790:2006]

2.272.5 (EN) AUTHENTICATION CODE

a cryptographic checksum based on an approved security function. [FIPS-140-2:2001]

2.272.6 (EN) MESSAGE AUTHENTICATION CODE (MAC)

string of bits which is the output of a MAC algorithm.

NOTE. A MAC is sometimes called a cryptographic check value (see for example ISO-7498-2).

[ISO-9797-1:1999]

2.273 CÓDIGO DE DETECCIÓN DE ERRORES

2.273.1 CÓDIGO DE DETECCIÓN DE ERRORES

Valor derivado de unos datos que consiste en una información adicional que permite detectar alteraciones accidentales de la información, sin llegar a poder corregirla.

2.273.2 (EN) ERROR DETECTION CODE

A code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data. [CNSSI_4009:2010]

2.273.3 (EN) ERROR DETECTION CODE

a value computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data. [ISO-19790:2006]

2.274 COLD STANDBY

Ver:

- *Opción de recuperación*
- *Sala vacía*

2.274.1 RECUPERACIÓN GRADUAL

(Diseño del Servicio) Una Opción de Recuperación que también es conocida como Reserva fría. Recuperación del Servicio de TI en un período de tiempo superior a 72 horas. La recuperación Gradual normalmente emplea Facilidades Portátiles o Fijas que tienen soporte medioambiental y cableado de Red, pero no Sistemas Informáticos. El hardware y software se instalan dentro del Plan de Continuidad del Servicio de TI. [ITIL:2007]

2.274.2 (EN) COLD STANDBY

Synonym for Gradual Recovery. [ITIL:2007]

2.274.3 (EN) GRADUAL RECOVERY

(Service Design) A Recovery Option which is also known as Cold Standby. Provision is made to Recover the IT Service in a period of time greater than 72 hours. Gradual Recovery typically uses

a Portable or Fixed Facility that has environmental support and network cabling, but no computer Systems. The hardware and software are installed as part of the IT Service Continuity Plan. [ITIL:2007]

2.274.4 (FR) REPRISE GRADUELLE

(Conception de services) Une option de reprise également connue sous le nom de Cold Standby. Une provision est effectuée afin de reprendre le service des TI dans un laps de temps de plus de 72 heures. La reprise graduelle utilise habituellement un lieu fixe ou mobile disposant d'un soutien environnemental et d'un câblage réseau, mais sans systèmes informatiques. Le matériel et le logiciel sont installés en tant qu'éléments du Plan de continuité de services des TI. [ITIL:2007]

2.275 CÓDIGO MÓVIL

Ver:

- *Contenido activo*

2.275.1 CÓDIGO MÓVIL

Los programas o partes de programas descargados de sistemas remotos a través de una red, y que se ejecuta en un sistema de información local sin necesidad de instalación explícita parte del usuario.

Ejemplos de tecnologías relacionadas: Java, JavaScript, ActiveX, VBScript.

2.275.2 (EN) MOBILE CODE

Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. [NIST-SP800-18:2006]

2.275.3 (EN) MOBILE CODE TECHNOLOGIES

Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript). [NIST-SP800-18:2006]

2.276 COF – CIPHERING OFFSET

2.276.1 COF – CIPHERING OFFSET

96 bits que utiliza el protocolo Bluetooth en el establecimiento de la clave de cifra de los datos que se trasmiten. Si se trata de una clave maestra, el COF se deriva de la dirección del maestro. Si no, se utiliza el valor ACO determinado durante el procedimiento de autenticación.

2.276.2 (EN) COF – CIPHERING OFFSET

96-bit data used in Bluetooth protocol to derive the encryption key for data transmission. If the current key is a master key, then COF is derived from the master BD-ADDR. Otherwise the value of COF is set to the value of ACO as computed during the authentication procedure.

2.277 COLISIÓN

Ver:

- *Hash*
- *Resistente a colisiones*

2.277.1 COLISIÓN

Situación que se produce cuando una función hash, operando sobre entradas distintas, genera una misma salida. Puede ser de dos tipos:

- Débil: Cuando dado un mensaje se encuentra otro que produce el mismo hash.
- Fuerte: Cuando se encuentra una pareja de mensajes que producen el mismo hash.

[CESID:1997]

2.277.2 (EN) COLLISION

Two or more distinct inputs produce the same output. Also see hash function. [NIST-SP800-57:2007]

2.277.3 (EN) COLLISION

If, given a message x, it is computationally infeasible to find a message y not equal to x such that H(x) = H(y), then H is said to be a weakly collision-free hash function. A strongly collision-free hash function H is one for which it is computationally infeasible to find any two messages x and y such that H(x) = H(y).

http://www.rsasecurity.com/rsalabs/faq/

2.278 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Ver:

- *Seguridad de la información*

2.278.1 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Órgano colegiado que coordina las actividades de la organización en materia de seguridad de la información. En particular asume los roles de responsable de la información y responsable de los servicios. [CCN-STIC-801:2010]

2.278.2 (EN) COMMITTEE ON INFORMATION SECURITY.

Collegial body that coordinates the activities of the organization's information security. In particular assume the roles of leader and head of information services.

2.279 COMP 128-1

Ver:

- *Módulo de identificación de usuario*

2.279.1 COMP128-1

algoritmo propietario utilizado en los primeros módulos SIM de telefonía GSM. Es un conjunto de algoritmos "hash" para generar una respuesta a un reto de identificación y para generar una clave de sesión.

2.279.2 (EN) COMP128-1

the proprietary algorithm that was initially used by default in SIM cards. [ISO-18028-1:2006]

2.280 COMPARTIMENTACIÓN

Ver:

- *Compartimento*

2.280.1 COMPARTIMENTACIÓN

Aislamiento del sistema operativo, programas y ficheros de datos en los dispositivos de almacenamiento (memoria principal y secundarias), para protegerles de accesos concurrentes o no autorizados. [Ribagorda:1997]

2.280.2 COMPARTIMENTACIÓN

División de la información sensible y de los elementos y recursos de un sistema de información en unidades menores, basándose en la necesidad de conocer y el nivel de habilitación, a fin de reducir el riesgo de accesos no autorizados. [CESID:1997]

2.280.3 (EN) COMPARTMENTALIZATION

A process for protecting very high value assets or in environments where trust is an issue. Access to an asset requires two or more processes, controls or individuals.

ISACA, Cybersecurity Glossary, 2014

2.280.4 (EN) COMPARTMENTALIZATION

A nonhierarchical grouping of sensitive information used to control access to data more finely than with hierarchical security classification alone. [CNSSI_4009:2010]

2.281 COMPARTIMENTO

Ver:

- *Modo compartimentado*
- *Compartimentación*

2.281.1 COMPARTIMENTO

Agrupación de información sensible que comparte unos ciertos requisitos de protección frente al acceso no autorizado.

2.281.2 (EN) COMPARTMENT

1. (I) A grouping of sensitive information items that require special access controls beyond those normally provided for the basic classification level of the information. (See: compartmented security mode. Compare: category, classification.) [RFC4949:2007]

2.282 COMPATIBILIDAD ELECTROMAGNÉTICA

2.282.1 COMPATIBILIDAD ELECTROMAGNÉTICA

la aptitud de un dispositivo, de un aparato o de un sistema para funcionar de forma satisfactoria en su entorno electromagnético, sin producir por sí mismo perturbaciones electromagnéticas intolerables en otros aparatos que se encuentren en dicho entorno.

REAL DECRETO 444/1994, de 11 de marzo, por el que se establece los procedimientos de evaluación de la conformidad y los requisitos de protección relativos a compatibilidad electromagnética de los equipos, sistemas e instalaciones.

2.282.2 (EN) ELECTROMAGNETIC COMPATIBILITY

the ability of electronic devices to function satisfactorily in an electromagnetic environment without introducing intolerable electromagnetic disturbances to other devices in that environment. [FIPS-140-2:2001]

2.283 COMPROMETER

2.283.1 ESTAR O PONER EN COMPROMISO

Estar, o poner, en duda algo que antes era claro y seguro.

DRAE. Diccionario de la Lengua Española.

2.283.2 COMPROMETER

Soslayar o violar los mecanismos o procedimientos de seguridad de un sistema, recurso o activo con el resultado de desproteger a los mismos. [Ribagorda:1997]

2.283.3 COMPROMISO DE SEGURIDAD O COMPROMETIMIENTO DE SEGURIDAD

1. Resultado de un incumplimiento o violación de las medidas de seguridad, por el que determinada información ha quedado desprotegida.

2. Documento en el que una persona reconoce haber sido instruida en las medidas de seguridad vigentes y se compromete a aplicarlas.

[CESID:1997]

2.283.4 (EN) COMPROMISE

To bring somebody/something/yourself into danger or under suspicion, especially by acting in a way that is not very sensible.

Oxford Advanced Learner's Dictionary.

2.283.5 DATA BREACH

compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed [ISO-27050:2015]

2.283.1 (EN) COMPROMISE

Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [CNSSI_4009:2010]

2.283.2 (EN) SECURITY COMPROMISE

(I) A security violation in which a system resource is exposed, or is potentially exposed, to unauthorized access. (Compare: data compromise, exposure, violation.) [RFC4949:2007]

2.283.3 (EN) DATA COMPROMISE

1. (I) A security incident in which information is exposed to potential unauthorized access, such that unauthorized disclosure, alteration, or use of the information might have occurred. (Compare: security compromise, security incident.)

2. (O) /U.S. DoD/ A "compromise" is a "communication or physical transfer of information to an unauthorized recipient." [DoD5]

3. (O) /U.S. Government/ "Type of [security] incident where information is disclosed to unauthorized individuals or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred." [C4009]

[RFC4949:2007]

2.283.4 (EN) COMPROMISE

The unauthorized disclosure, modification, substitution or use of sensitive data (e.g., keying material and other security related information). [NIST-SP800-57:2007]

2.283.5 (EN) COMPROMISE

the unauthorised disclosure, modification, substitution, or use of CSPs or the unauthorised modification or substitution of PSPs.

CSP - critical security parameter - security related information whose disclosure or modification can compromise the security of a cryptographic module.

EXAMPLE: Secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other trust anchors.

NOTE. A CSP may be plaintext or encrypted.

PSP - public security parameter

security related public information whose modification can compromise the security of a cryptographic module.

EXAMPLE: Public cryptographic keys, public key certificates, self-signed certificates, trust anchors, and one time passwords associated with a counter.

[ISO-19790:2006]

2.283.6 (EN) COMPROMISE

Compromise denotes a situation when -due to a breach of security or adverse activity (such as espionage, acts of terrorism, sabotage or theft)- classified information has lost its confidentiality, integrity or availability, or supporting services and resources have lost their integrity or availability. This includes loss, disclosure to unauthorised individuals (e.g. through espionage or to the media) unauthorised modification, destruction in an unauthorised manner, or denial of service.

2.283.7 (EN) COMPROMISE

the unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other CSPs). [FIPS-140-2:2001]

2.283.8 (EN) COMPROMISE

Also referred to as “data compromise,” or “data breach.” Intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.283.9 (EN) COMPROMISE

The unauthorized access to, disclosure, destruction, removal, modification, use or interruption of assets or information.

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

2.283.10 (FR) INCIDENT DE SÉCURITÉ

Également dénommé «compromission des données» ou «atteinte à la protection des données». Intrusion dans un système informatique lorsque l’on soupçonne une divulgation/un vol, une modification ou la destruction non autorisés des données du titulaire de carte.

http://fr.pcisecuritystandards.org/

2.284 COMPUSEC

Acrónimos: COMPUSEC

Ver:

- *Seguridad*

2.284.1 SEGURIDAD DE LOS ORDENADORES (COMPUSEC)

Resultado de un conjunto de medidas aplicadas a un sistema informático y orientadas a evitar accesos, manipulaciones, pérdidas, modificaciones o conocimiento de la información que contiene por personal no autorizado. [CESID:1997]

2.284.1 (EN) COMPUTER SECURITY (COMPUSEC)

Measures and controls that ensure confidentiality, integrity, and availability of IS assets including hardware, software, firmware, and information being processed, stored, and communicated. [CNSSI_4009:2010]

2.284.2 (EN) COMPUTER SECURITY (COMPUSEC)

1. (I) Measures to implement and assure security services in a computer system, particularly those that assure access control service.

2. (O) "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)." [SP12]

[RFC4949:2007]

2.285 CONCENTRADOR

2.285.1 CONCENTRADOR

Elemento de red en el que se concentra el tráfico antes de ser distribuido a los sistemas conectados a la red.

2.285.2 (EN) HUB

A hub is a network device that functions at layer 1 of the OSI reference model (ISO/IEC IS ISO-7498-1). There is no real intelligence in network hubs; they only provide physical attachment points for networked systems or resources. [ISO-18028-4:2005]

2.285.3 (EN) HUB

A device where network traffic comes together before being distributed out to connected systems.

2.286 CONCEPTO DE OPERACIÓN

Acrónimos: CONOP

2.286.1 CONCEPTO DE OPERACIÓN

Declaración expresa que realiza el AOSTIC sobre el objeto o función del Sistema, el tipo de información que va a ser manejada, las condiciones de explotación (perfil de seguridad de los usuarios, clasificación de la información, modo de operación, etc.), y las amenazas a las que estará sometido. [CCN-STIC-301:2006]

2.286.2 (EN) CONCEPT OF OPERATIONS (CONOP)

See security concept of operations. [CNSSI_4009:2010]

2.286.3 SECURITY CONCEPT OF OPERATIONS (SECURITY CONOP)

A security-focused description of an information system, its operational policies, classes of users, interactions between the system and its users, and the system's contribution to the operational mission. [CNSSI_4009:2010]

2.287 CONCESIONES DE SEGURIDAD

2.287.1 CONCESIONES DE SEGURIDAD

2.287.2 (EN) SECURITY TRADE-OFFS

There is no single correct level of security; how much security you have depends on what you're willing to give up in order to get it. This trade-off is, by its very nature, subjective—security decisions are based on personal judgments. Different people have different senses of what constitutes a threat, or what level of risk is acceptable. What's more, between different commu- nities, or organizations, or even entire societies, there is no agreed-upon way in which to define threats or evaluate risks, and the modern technological and media-filled world makes these evaluations even harder.

http://cyber.law.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas

2.288 CONCIENCIACIÓN (EN SEGURIDAD)

Ver:

- *Entrenamiento (en seguridad)*

2.288.1 CONCIENCIACIÓN (EN SEGURIDAD)

concienciación.

1. f. Acción y efecto de concienciar o concienciarse.

concienciar.

1. tr. Hacer que alguien sea consciente de algo. U. t. c. prnl.

2. prnl. Adquirir conciencia de algo.

consciente.

adj. Que siente, piensa, quiere y obra con conocimiento de lo que hace.

DRAE. Diccionario de la Lengua Española.

2.288.2 CONCIENCIACIÓN (EN SEGURIDAD)

Actividad continuada y recurrente en la que todas las personas relacionadas con el sistema de información se familiarizan con los aspectos de seguridad del mismo a fin de que no provoquen

fallos gratuitos por ignorancia, descuido o negligencia. La concienciación incluye conocer cual es el funcionamiento correcto, identificar comportamientos anómalos y saber cómo reportar lo que se salga de lo normal.

2.288.3 (EN) WHAT IS SECURITY AWARENESS?

"Awareness" constitutes the point-of-entry for all employees in pursuing IT security knowledge. Awareness seeks to focus an individuals attention on an issue or a set of issues. Awareness is not training.

Security awareness programs provide a blended solution of activities that promote security, establish accountability, and inform the workforce of security news. Awareness programs continually push the security message to users in a variety of formats and provide security information to users.

[NIST-SP800-100:2006]

2.289 CONFIANZA

Ver:

- *Entidad de confianza*
- *Origen de confianza*
- *Canal confiable*
- *Acceso fiable*
- *Tercera parte de confianza*
- *Red de confianza*

2.289.1 CONFIANZA

Esperanza firme que se tiene de alguien o algo.

DRAE. Diccionario de la Lengua Española.

2.289.2 CONFIANZA

Se dice que A confía en B cuando A presume que B se comportará de una determinada forma. La confianza suele estar limitada a una determinada función de B y no necesariamente se extiende a otras funciones.

2.289.3 FIDUCIARIO

En general, se puede decir que una entidad acepta como "fiduciaria" a una segunda entidad cuando aquella (la primera entidad) supone que la segunda entidad se comportará exactamente como ella lo espera. Esta relación de confianza se puede aplicar solamente para alguna función específica. El cometido principal de la confianza en el marco de la autenticación es describir la relación entre una entidad autenticadora y una entidad de certificación; una entidad autenticadora tendrá que estar segura de que puede confiar en que la autoridad de certificación crea solamente certificados válidos y fiables. [X.509:2005]

2.289.4 CONFIANZA

Se dice que la entidad X confía en la entidad Y para un conjunto de actividades solamente si la entidad X puede confiar en que la entidad Y se comporta de una manera particular con respecto a las actividades. [X.810:1995]

2.289.5 (EN) TRUSTWORTHINESS

The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities. [CNSSI_4009:2010]

2.289.6 (EN) TRUST

1. (I) /information system/ A feeling of certainty (sometimes based on inconclusive evidence) either (a) that the system will not fail or (b) that the system meets its specifications (i.e., the system does what it claims to do and does not perform unwanted functions). (See: trust level, trusted system, trustworthy system. Compare: assurance.)

2. (I) /PKI/ A relationship between a certificate user and a CA in which the user acts according to the assumption that the CA creates only valid digital certificates.

[RFC4949:2007]

2.289.7 (EN) TRUST

Generally, an entity can be said to "trust" a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects. This trust may apply only for some specific function. The key role of trust in this framework is to describe the relationship between an authenticating entity and a authority; an entity shall be certain that it can trust the authority to create only valid and reliable certificates. [X.509:2005]

2.289.8 (EN) TRUST

A relationship between two elements, a set of activities and a security policy in which element x trusts element y if and only if x has confidence that y will behave in a well defined way (with respect to the activities) that does not violate the given security policy. [ISO-13888-1:2004]

2.289.9 (EN) TRUST

Entity X is said to trust entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities. [X.810:1995]

2.289.10 (EN) HIERARCHICAL TRUST

A method of organizing "trust" within an organization by allowing one Certificate Authority to delegate a portion of its responsibility to a subordinate Certificate Authority. For example, a business might have a master Certificate Authority, which vouches for a Certificate Authority at the company's Los Angeles office, which vouches for a Certificate Authority at the company's Phoenix office. Commonly used in ANSI X.509 certificates.

http://www.watchguard.com/glossary/

2.289.11 (EN) TRUSTED IT PRODUCT

an IT product other than the TOE which has its security functional requirements administratively coordinated with the TOE and which is assumed to enforce its security functional requirements correctly (e. g. by being separately evaluated).

TOE - Target of Evaluation

[CC:2006]

2.289.12 (FR) CONFIANCE

on peut dire d'une manière générale qu'une entité "fait confiance" à une autre entité si la première fait l'hypothèse que la deuxième se comportera exactement comme attendu (par la première). Il se peut que cette confiance s'applique uniquement pour une fonction donnée. Le rôle clé de la confiance dans ce cadre décrit la relation entre une entité effectuant l'authentification et une autorité; une entité sera certaine qu'elle peut faire confiance à l'autorité pour ne créer que des certificats valides et fiables. [X.509:2005]

2.289.13 (FR) CONFIANCE

on dit que l'entité X fait confiance à l'entité Y pour un ensemble d'activités si et seulement si l'entité X suppose que l'entité Y se comportera d'une certaine façon par rapport aux activités. [X.810:1995]

2.290 CONFIDENCIALIDAD

2.290.1 CONFIDENCIALIDAD

Propiedad de la información que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27000:2014]

2.290.2 CONFIDENCIALIDAD

Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. [UNE-71504:2008]

2.290.3 CONFIDENCIALIDAD

(Diseño del Servicio) Principio de seguridad que requiere que los datos deberían únicamente ser accedidos por el personal autorizado a tal efecto. [ITIL:2007]

2.290.4 CONFIDENCIALIDAD DE LOS DATOS

Este servicio se puede utilizar para obtener la protección de los datos frente a buscadores no autorizados. El servicio de confidencialidad de datos está soportado por un marco de autenticación. Se puede utilizar para la protección contra la interceptación de datos. [X.509:2005]

2.290.5 CONFIDENCIALIDAD

Propiedad de los elementos esenciales de ser accesibles sólo para los usuarios autorizados cuando éstos lo requieran. [EBIOS:2005]

2.290.6 CONFIDENCIALIDAD

1. Propiedad de la información que impide que ésta esté disponible o sea revelada a individuos, entidades o procesos no autorizados (ISO-7498-2). Según esta norma la confidencialidad es un servicio de seguridad.

2. Prevención de la revelación no autorizada de información (ITSEC).

3. Característica de los datos e informaciones que son revelados sólo a los usuarios, entidades o procesos en el tiempo y forma autorizados (OCDE).

El mantenimiento de la confidencialidad, junto con el de la integridad y disponibilidad, constituye el objetivo de la seguridad de la información.

[Ribagorda:1997]

2.290.7 CONFIDENCIALIDAD DEL TRÁFICO DE DATOS (TRAFFIC FLOW CONFIDENTIALITY)

Servicio de seguridad destinado a prevenir el análisis del tráfico de datos (ISO-7498-2). El mecanismo responsable de suministrar este servicio se denomina rellenado de tráfico. [Ribagorda:1997]

2.290.8 CONFIDENCIALIDAD

Servicio de seguridad que asegura que una información no puede estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. Puede proteger toda la información que circula por un enlace, determinados campos de ella o contra análisis del flujo de tráfico. [CESID:1997]

2.290.9 CONFIDENCIALIDAD

Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados. [ISO-7498-2:1989]

2.290.1 (EN) CONFIDENTIALITY

property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO/IEC 27000:2014]

2.290.2 (EN) CONFIDENTIALITY

The term `confidentiality' means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

Cyber Intelligence Sharing and Protection Act. H.R. 624. 2013.

2.290.1 (EN) CONFIDENTIALITY

The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.

NIST SP 800.53: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

[CNSSI_4009:2010]

2.290.2 (EN) DATA CONFIDENTIALITY

1. (I) The property that data is not disclosed to system entities unless they have been authorized to know the data. (See: Bell- LaPadula model, classification, data confidentiality service, secret. Compare: privacy.)

2. (D) "The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity]." [ISO-7498-2].

[RFC4949:2007]

2.290.3 (EN) CONFIDENTIALITY

(Service Design) A security principle that requires that data should only be accessed by authorised people. [ITIL:2007]

2.290.4 (EN) CONFIDENTIALITY

The property that sensitive information is not disclosed to unauthorized entities. [NIST-SP800-57:2007]

2.290.5 (EN) CONFIDENTIALITY

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

U.S. Code 44, Sec. 3542. Definitions, 2007

2.290.6 (EN) CONFIDENTIALITY

the property that sensitive information is not disclosed to unauthorized individuals, entities, or processes. [ISO-18028-2:2006]

2.290.7 (EN) CONFIDENTIALITY

The property that prevents disclosure of information to unauthorized individuals, entities, or processes. [H.235:2005]

2.290.8 (EN) DATA CONFIDENTIALITY

This service can be used to provide for protection of data from unauthorized disclosure. The authentication framework supports the data confidentiality service. It can be used to protect against data interception. [X.509:2005]

2.290.9 (EN) CONFIDENTIALITY

Property of essential elements making them only accessible to authorised users. [EBIOS:2005]

2.290.10 (EN) CONFIDENTIALITY

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [FIPS-199:2004] [NIST-SP800-60V2:2004]

2.290.11 (EN) CONFIDENTIALITY

The security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and while in transit. [NIST-SP800-27:2004]

2.290.12 (EN) DATA CONFIDENTIALITY

The Data Confidentiality Security Dimension protects data from unauthorized disclosure. Data Confidentiality ensures that the data content cannot be understood by unauthorized entities. Encryption, access control lists, and file permissions are methods often used to provide data confidentiality. [X.805:2003]

2.290.13 (EN) CONFIDENTIALITY

The requirement of keeping proprietary, sensitive, or personal information private and inaccessible to anyone that is not authorized to see it. [Octave:2003]

2.290.14 (EN) CONFIDENTIALITY

The security objective that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and while in transit. [NIST-SP800-33:2001]

2.290.15 (EN) CONFIDENTIALITY

the property that sensitive information is not disclosed to unauthorized individuals, entities, or processes. [FIPS-140-2:2001]

2.290.16 (EN) CONFIDENTIALITY

The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations. [IRM-5239-8:1995]

2.290.17 (EN) CONFIDENTIALITY

the prevention of the unauthorised disclosure of information. [ITSEC:1991]

2.290.18 (EN) CONFIDENTIALITY

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [ISO-7498-2:1989]

2.290.19 (EN) CONFIDENTIALITY

Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it.

http://www.sans.org/security-resources/glossary-of-terms/

2.290.20 (EN) CONFIDENTIALITY

A characteristic applied to information to signify that it can only be disclosed to authorized individuals to prevent injury to national or other interests.

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

2.290.21 (FR) CONFIDENTIALITÉ

(Conception de services) Principe de sécurité nécessitant que les données ne soient accessibles qu'à des personnes autorisées. [ITIL:2007]

2.290.22 (FR) CONFIDENTIALITÉ DES DONNÉES

ce service peut être utilisé pour protéger des données contre une divulgation non autorisée. Le service de confidentialité des données est pris en charge par le cadre d'authentification. Il peut être utilisé pour protéger des données contre les interceptions. [X.509:2005]

2.290.23 (FR) CONFIDENTIALITÉ

Propriété des éléments essentiels de n'être accessibles qu'aux utilisateurs autorisés. [EBIOS:2005]

2.290.24 (FR) CONFIDENTIALITÉ

La propriété qu'une information n'est pas rendue disponible ni révélée à des personnes, des entités ou des processus non autorisés. [ISO-7498-2:1989]

2.290.25 (FR) CONFIDENTIALITÉ

Qualité conférée à des renseignements pour signifier qu'ils ne peuvent être divulgués qu'à des personnes autorisées, afin de prévenir tout préjudice à l'intérêt national ou à d'autres intérêts.

http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578

2.291 CONFIDENCIALIDAD DEL TRÁFICO DE DATOS

Ver:

- *Análisis de tráfico*

2.291.1 CONFIDENCIALIDAD DEL TRÁFICO DE DATOS

Servicio de confidencialidad que protege frente al análisis del tráfico (ISO-7498-2). [Ribagorda:1997]

2.291.2 CONFIDENCIALIDAD DEL FLUJO DE TRÁFICO

Servicio de confidencialidad que ofrece protección contra el análisis de tráfico. [ISO-7498-2:1989]

2.291.3 (EN) TRAFFIC-FLOW CONFIDENTIALITY (TFC)

1. (I) A data confidentiality service to protect against traffic analysis. (See: communications cover.)

2. (O) "A confidentiality service to protect against traffic analysis." [ISO-7498-2]

[RFC4949:2007]

2.291.4 (EN) TRAFFIC FLOW CONFIDENTIALITY

A confidentiality service to protect against traffic analysis. [NIST-SP800-33:2001]

2.291.5 (EN) TRAFFIC FLOW CONFIDENTIALITY

A confidentiality service to protect against traffic analysis. [ISO-7498-2:1989]

2.291.6 (FR) CONFIDENTIALITE DU FLUX DE DONNEES

Service de confidentialité fournissant une protection contre l'analyse du trafic. [ISO-7498-2:1989]

2.292 CONFIGURACIÓN

Ver:

- *Base de datos de configuración (CMDB)*
- *Control de configuración*
- *Clave*
- *Gestión de la configuración*

2.292.1 CONFIGURACIÓN

(Transición del Servicio) Término genérico usado para describir un grupo de Elementos de Configuración que actúan o funcionan juntos para proveer un Servicio de TI, o un subconjunto representativo de un Servicio de TI. El término Configuración también se usa para describir los parámetros y ajustes realizados en uno o más CIs. [ITIL:2007]

2.292.2 ELEMENTO DE CONFIGURACIÓN [CONFIGURATION ITEM] (CI)

(Transición del Servicio) Cualquier Componente que necesite ser gestionado con el objeto de proveer un Servicio de TI. La información sobre cada CI se almacena en un Registro de Configuración dentro del Sistema de Gestión de la Configuración y es mantenido durante todo su Ciclo de Vida por Gestión de la Configuración. Los CIs están bajo el control de Gestión del Cambio. Típicamente, los CIs pueden ser Servicios de TI, hardware, software, edificios, personal, y documentación formal como por ejemplo documentación sobre Procesos y SLAs. [ITIL:2007]

2.292.3 CONFIGURACIÓN

Selección concreta de algunos de los posibles conjuntos de posibilidades de operación de un sistema.

2.292.4 (EN) CONFIGURATION

(Service Transition) A generic term, used to describe a group of Configuration Items that work together to deliver an IT Service, or a recognizable part of an IT Service. Configuration is also used to describe the parameter settings for one or more CIs. [ITIL:2007]

2.292.5 (EN) CONFIGURATION ITEM (CI)

(Service Transition) Any Component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the Configuration Management System and is maintained throughout its Lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT Services, hardware, software, buildings, people, and formal documentation such as Process documentation and SLAs. [ITIL:2007]

2.292.6 (EN) CONFIGURATION

The selection of one of the sets of possible combinations of features of a Target of Evaluation. [ITSEC:1991]

2.292.7 (FR) CONFIGURATION

(Transition de Services) Terme générique servant à décrire un groupe d'éléments de configuration fonctionnant ensemble pour fournir un service informatique ou une partie significative d'un service informatique. Le terme Configuration sert également à décrire les réglages des paramètres d'un ou de plusieurs CI. [ITIL:2007]

2.292.8 (FR) ELEMENT DE CONFIGURATION (CI)

(Transition de Services) Tout composant devant être géré afin de fournir un service des TI. Les informations concernant chaque CI sont enregistrées dans un enregistrement de configuration au sein du Système de gestion des configurations (CMS) où elles sont tenues à jour pendant tout son cycle de vie par la Gestion des configurations. Les CI sont sous le contrôle de la Gestion des changements. Les CI comprennent habituellement les services des TI, le matériel, les logiciels, les immeubles, les personnes et la documentation formelle tels que la documentation des processus et les SLA. [ITIL:2007]

2.293 CONFORMIDAD

2.293.1 CONFORMIDAD

cumplimiento de un requisito [UNE-ISO/IEC 27000:2014]

2.293.2 CONFORMIDAD

Aseguramiento de que se sigue un Estándar o conjunto de Directrices, o de que se emplean unas prácticas de seguimiento adecuadas y consistentes. [ITIL:2007]

2.293.3 (EN) CONFORMITY

fulfillment of a requirement [ISO/IEC 27000:2014]

2.293.4 (EN) COMPLIANCE

Adherence to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies

ISACA, Cybersecurity Glossary, 2014

2.293.5 (EN) COMPLIANCE

Ensuring that a Standard or set of Guidelines is followed, or that proper, consistent accounting or other practices are being employed. [ITIL:2007]

2.293.6 (EN) REGULAROTY COMPLIANCE

Regulatory compliance is an organization's adherence to laws, regulations, guidelines and specifications relevant to its business. Violations of regulatory compliance regulations often result in legal punishment, including federal fines.

http://whatis.techtarget.com/

2.293.7 (FR) CONFORMITÉ

Assurer qu'un standard ou un ensemble de principes est suivi, qu'une comptabilité correcte et cohérente est appliquée ou que diverses pratiques ont été employées. [ITIL:2007]

2.294 CONFUSIÓN

Ver:

- *Difusión*

2.294.1 CONFUSIÓN

Propiedad de un algoritmo criptográfico tal que la frecuencia de aparición de los símbolos cifrados no revela ninguna información sobre los símbolos en claro de los que proceden. De esta manera, las propiedades estadísticas de los símbolos del lenguaje en claro no proporcionan ninguna información al criptoanalista. [Ribagorda:1997]

2.294.2 CONFUSIÓN

Técnica destinada a ocultar la relación entre el texto claro y su correspondiente cifrado desde el punto de vista estadístico del idioma. Principalmente se consigue mediante sustituciones. [CE-SID:1997]

2.294.3 (EN) CONFUSION

Those parts of a cipher mechanism which change the correspondence between input values and output values. In contrast to diffusion.

http://www.ciphersbyritter.com/GLOSSARY.HTM

2.295 CONOCIMIENTO NULO (TÉCNICA DE)

Ver:

- *Prueba de posesión*
- *Método asimétrico de autenticación*

2.295.1 TÉCNICA DE CONOCIMIENTO NULO

Técnica de autenticación basada en un cifrado asimétrico. Se caracteriza porque un único intercambio de información de autenticación no es suficiente para avalar la autenticidad de una entidad, pero dicha información puede bastar para delatar una suplantación (ISO/IEC ISO-10181-2). [Ribagorda:1997]

2.295.2 CONOCIMIENTO CERO

Protocolo que permite demostrar el conocimiento de un secreto sin revelar información alguna relativa al mismo. [CESID:1997]

2.295.3 (EN) ZERO-KNOWLEDGE PASSWORD PROTOCOL

A password based authentication protocol that allows a claimant to authenticate to a Verifier without revealing the password to the Verifier. Examples of such protocols are EKE, SPEKE and SRP. [NIST-SP800-63:2013]

2.295.4 (EN) ZERO-KNOWLEDGE PROOF

(I) /cryptography/ A proof-of-possession protocol whereby a system entity can prove possession of some information to another entity, without revealing any of that information. (See: proof-of-possession protocol.) [RFC4949:2007]

2.295.5 (EN) ZERO-KNOWLEDGE

In an interactive proof, when the verifier learns nothing about the fact being proved (except that it is correct) from the prover that he could not already learn without the prover, even if the verifier does not follow the protocol (as long as the prover does). In a zero-knowledge proof, the verifier cannot even later prove the fact to anyone else.

http://www.rsasecurity.com/rsalabs/faq

2.295.6 (EN) ZERO-KNOWLEDGE PROOF

A zero-knowledge proof or zero-knowledge protocol is an interactive method for one party to prove to another that a (usually mathematical) statement is true, without revealing anything other than the veracity of the statement.

http://en.wikipedia.org/wiki/Zero_Knowledge

2.296 CONOCIMIENTO PARCIAL

Ver:

- *Clave fragmentada*

2.296.1 CONOCIMIENTO PARCIAL

Método mediante el cual dos o más entidades separadas poseen componentes de una clave, pero que, de forma individual, no pueden descifrar la clave criptográfica resultante.

http://es.pcisecuritystandards.org

2.296.2 CONOCIMIENTO PARCIAL

1. Condición bajo la cual dos o más partes, separada y confidencialmente, custodian los componentes de una clave criptográfica. Dichos componentes, aisladamente, no permiten conocer esta última (ISO-8732)

2. Propiedad de un sistema o procedimiento de seguridad que impide el acceso a los recursos si no median dos o más entidades diferentes autorizadas.

Según esta última definición es término sinónimo de: Control dual y Separación de funciones.

[Ribagorda:1997]

2.296.3 CONOCIMIENTO PARCIAL

Sistema de protección de funciones o información sensible, por el cual dos o más entidades diferentes cuando actúan separadamente no pueden acceder o utilizar los recursos de un sistema pero sí cuando lo hacen concertadamente. [CESID:1997]

2.296.4 (EN) SPLIT KNOWLEDGE

1. Separation of data or information into two or more parts, each part constantly kept under control of separate authorized individuals or teams so that no one individual or team will know the whole data.

2. A process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, which can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key.

[CNSSI_4009:2010]

2.296.5 (EN) SPLIT KNOWLEDGE

1. (I) A security technique in which two or more entities separately hold data items that individually do not convey knowledge of the information that results from combining the items. (See: dual control, split key.)

2. (O) "A condition under which two or more entities separately have key components [that] individually convey no knowledge of the plaintext key [that] will be produced when the key components are combined in the cryptographic module." [FP140]

[RFC4949:2007]

2.296.6 (EN) SPLIT KNOWLEDGE

A process by which a cryptographic key is split into n multiple key components, individually providing no knowledge of the original key, which can be subsequently combined to recreate the original cryptographic key. If knowledge of k (where k is less than or equal to n) components is required to construct the original key, then knowledge of any k-1 key components provides no information about the original key other than, possibility, its length. [NIST-SP800-57:2007]

2.296.7 (EN) SPLIT KNOWLEDGE

a process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, that can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key. [ISO-19790:2006]

2.296.8 (EN) SPLIT KNOWLEDGE

a process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, that can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key. [FIPS-140-2:2001]

2.296.9 (EN) SPLIT KNOWLEDGE

Condition in which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic key.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.296.10 (FR) FRACTIONNEMENT DES CONNAISSANCES

Une méthode par laquelle deux ou plusieurs entités détiennent séparément des composants de la clé qui, à eux seuls, ne leur permettent pas d’avoir connaissance de la clé cryptographique qui en résulte.

http://fr.pcisecuritystandards.org/

2.297 CONSECUENCIA

Ver:

- *Impacto*
- *Riesgo*

2.297.1 CONSECUENCIA

Resultado de un suceso que afecta a los objetivos. [UNE-ISO GUÍA 73:2010]

NOTA 1 Un suceso puede conducir a una serie de consecuencias.

NOTA 2 Una consecuencia puede ser cierta o incierta y normalmente es negativa en el contexto de la seguridad de la información.

NOTA 3 Las consecuencias se pueden expresar de forma cualitativa o cuantitativa.

NOTA 4 Las consecuencias iniciales pueden convertirse en reacciones en cadena.

[UNE-ISO/IEC 27000:2014]

2.297.2 CONSECUENCIA

Resultado de un suceso que afecta a los objetivos.

NOTA 3. Las consecuencias se pueden expresar de forma cualitativa o cuantitativa.

[UNE Guía 73:2010]

2.297.3 (EN) CONSEQUENCE

outcome of an event affecting objectives [ISO Guide 73:2009]

NOTE 1: An event can lead to a range of consequences.

NOTE 2: A consequence can be certain or uncertain and in the context of information security is usually negative.

NOTE 3: Consequences can be expressed qualitatively or quantitatively.

NOTE 4: Initial consequences can escalate through knock-on effects.

[ISO/IEC 27000:2014]

2.297.4 (EN) CONSEQUENCE

outcome of an event affecting objectives

NOTE 3 Consequences can be expressed qualitatively or quantitatively.

[ISO Guide 73:2009]

2.297.5 (EN) CONSEQUENCE

effect of an event, incident, or occurrence

Annotation: Consequence is commonly measured in four ways: human, economic, mission, and psychological, but may also include other factors such as impact on the environment.

DHS Risk Lexicon, September 2008

2.297.6 (EN) CONSEQUENCE ASSESSMENT

process of identifying or evaluating the potential or actual effects of an event, incident, or occurrence

DHS Risk Lexicon, September 2008

2.297.7 (EN) ECONOMIC CONSEQUENCE:

effect of an incident, event, or occurrence on the value of property or on the production, trade, distribution, or use of income, wealth, or commodities

Annotation: When measuring economic consequence in the context of homeland security risk, consequences are usually assessed as negative and measured in monetary units.

DHS Risk Lexicon, September 2008

2.297.8 (EN) HUMAN CONSEQUENCE

effect of an incident, event, or occurrence that results in injury, illness, or loss of life

Annotation: When measuring human consequence in the context of homeland security risk, consequence is assessed as negative and can include loss of life or limb, or other short-term or long-term bodily harm or illness.

DHS Risk Lexicon, September 2008

2.297.9 (EN) MISSION CONSEQUENCE:

effect of an incident, event, operation, or occurrence on the ability of an organization or group to meet a strategic objective or perform a function

Annotation: Valuation of mission consequence should exclude other types of consequences (e.g., human consequence, economic consequence, etc.) if they are evaluated separately in the assessment.

DHS Risk Lexicon, September 2008

2.297.10 (EN) PSYCHOLOGICAL CONSEQUENCE:

effect of an incident, event, or occurrence on the mental or emotional state of individuals or groups resulting in a change in perception and/or behavior

Annotation: In the context of homeland security, psychological consequences are negative and refer to the impact of an incident, event, or occurrence on the behavior or emotional and mental state of an affected population.

DHS Risk Lexicon, September 2008

2.297.11 (EN) THREAT CONSEQUENCE

(I) A security violation that results from a threat action.

Tutorial: The four basic types of threat consequence are "unauthorized disclosure", "deception", "disruption", and "usurpation". (See main Glossary entries of each of these four terms for lists of the types of threat actions that can result in these consequences.)

[RFC4949:2007]

2.297.12 (FR) CONSÉQUENCE

effet d'un événement affectant les objectifs

NOTE 3 Les conséquences peuvent être exprimées de façon qualitative ou quantitative.

[ISO Guide 73:2009]

2.298 CONSTRUCTOR DE VIRUS

2.298.1 CONSTRUCTOR DE VIRUS

Es un programa malicioso que permite crear nuevos virus sin necesidad de tener conocimientos de programación, mediante una interfaz a través de la cual se eligen las características del malware creado: tipo, efectos, archivos que infectar, encriptación, polimorfismo, etc.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.298.2 (EN) VIRUS BUILDER

Program that generates virus. The user spcifies the wished properties, and the virus is generated accordingly.

2.299 CONTENCIÓN

Ver:

- *Gestión de incidentes*

2.299.1 CONTENCIÓN

Acciones realizadas durante la gestión de un incidente orientadas a acotar el alcance del mismo, sujetándolo para que no se expanda.

2.299.2 (EN) CONTAINMENT

Actions taken to limit exposure after an incident has been identified and confirmed

ISACA, Cybersecurity Glossary, 2014

2.300 CONTENIDO ACTIVO

Ver:

- *Código móvil*

2.300.1 CONTENIDO ACTIVO

Programa empotrado en una página web. Cuando se accede a la página con un navegador, dicho programa se descarga y ejecuta automáticamente en el equipo del usuario. Ejemplos: applets java, ActiveX.

2.300.2 (EN) ACTIVE CONTENT

Software in various forms that is able to automatically carry out or trigger actions on a computer platform without the intervention of a user. [CNSSI_4009:2010]

2.300.3 (EN) ACTIVE CONTENT

Program code embedded in the contents of a web page. When the page is accessed by a web browser, the embedded code is automatically downloaded and executed on the user's workstation. Ex. Java, ActiveX (MS).

http://www.sans.org/security-resources/glossary-of-terms/

2.301 CONTINUIDAD

Ver:

- *Gestión de la Continuidad del Negocio (BCM)*
- *Plan de continuidad del negocio (BCP)*
- *Plan de recuperación*
- *Plan de recuperación de desastres*
- *Objetivo de tiempo de recuperación*
- *Plan de contingencia*
- *Emergencia*
- *Plan de continuidad de operaciones*
- [NIST-SP800-34:2002]
- *Gestión de crisis*

2.301.1 CONTINUIDAD

Prevenir, mitigar y recuperarse de una interrupción. Los términos 'planear la reanudación del negocio', 'planear la recuperación después de un desastre' y 'planear contingencias' también se pueden usar en este contexto; todos se concentran en los aspectos de recuperación de la continuidad. [COBIT:2006]

2.301.2 (EN) BUSINESS CONTINUITY

strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level. [BS25999-1:2006]

2.301.3 (EN) CONTINUITY

Preventing, mitigating and recovering from disruption. The terms "business resumption planning", "disaster recovery planning" and "contingency planning" also may be used in this context; they all concentrate on the recovery aspects of continuity. [COBIT:2006]

2.302 CONTRA MEDIDA

Ver:

- *Salvaguarda*
- *Control*
- *Mecanismo de seguridad*

2.302.1 MEDIDAS DE SEGURIDAD.

Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación. [ENS:2010]

2.302.1 (EN) COUNTERMEASURE

Actions, devices, procedures, or techniques that meet or oppose(i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

NIST SP 800-53: Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.

[CNSSI_4009:2010]

2.302.2 CONTRAMEDIDA

Puede ser usado para referirse a algún tipo de Control. El término Contramedida es muy usado cuando se refiere a medidas que incrementan la Resistencia, Tolerancia a fallos o Confiabilidad de un Servicio TI. [ITIL:2007]

2.302.3 (EN) COUNTERMEASURE

action, measure, or device that reduces an identified risk

Annotation: A countermeasure can reduce any component of risk -threat, vulnerability, or consequence

DHS Risk Lexicon, September 2008

2.302.4 (EN) COUNTERMEASURE

(I) An action, device, procedure, or technique that meets or opposes (i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken. [RFC4949:2007]

2.302.5 (EN) COUNTERMEASURE

Can be used to refer to any type of Control. The term Countermeasure is most often used when referring to measures that increase Resilience, Fault Tolerance or Reliability of an IT Service. [ITIL:2007]

2.302.1 (EN) COUNTERMEASURE

Action, device, procedure, technique, or other measure that reduces the vulnerability of an information system.[FIPS-200:2006]

2.302.2 (EN) COUNTERMEASURE

Anything which effectively negates or mitigates an adversary's ability to exploit vulnerabilities.

http://www.ioss.gov/docs/definitions.html

2.302.3 (EN) COUNTERMEASURE

Any action, device, procedure, technique, or other measure that mitigates risk by reducing the vulnerability of, threat to, or impact on a system. [TDIR:2003]

2.302.4 (EN) COUNTERMEASURE

a technical or non-technical security measure which contributes to meeting the security objective(s) of a Target of Evaluation. [ITSEM:1993]

2.302.5 (FR) CONTRE-MESURE

Peut faire référence à n'importe quel type de contrôle. Le terme "Contre-mesure" est souvent utilisé pour faire référence à des mesures qui augmente la Résilience, la Tolérance de panne ou la Fiabilité d'un service des TI. [ITIL:2007]

2.303 CONTRASEÑA

Ver:

- *Frase de acceso*
- http://en.wikipedia.org/wiki/Password
- *Contraseña de un solo uso*
- *Reventado de contraseñas*
- *Interceptación de contraseñas*

2.303.1 CONTRASEÑA

1. Seña secreta que permite el acceso a algo, a alguien o a un grupo de personas antes inaccesible.

2. Palabra o signo que, juntamente con el santo y seña, asegura el mutuo reconocimiento de personas, rondas y centinelas.

DRAE. Diccionario de la Lengua Española.

2.303.2 CONTRASEÑA

Información confidencial, a menuco compuesta de una cadena de caracteres, que puede ser usada en la autenticación de un usuario, entidad o recurso (ISO-7498-2) [Ribagorda:1997]

2.303.3 CONTRASEÑA O CLAVE DE ACCESO

Información secreta, en general un grupo de caracteres, utilizada para autenticación. [CESID:1997]

2.303.4 CONTRASEÑA DESECHABLE

Datos usados como medio de autenticación, cuyo uso no se repite más de una vez.

Habitualmente el ordenador ante el que se desea autenticar un usuario le lanza una pregunta (en ocasiones conocida como reto), diferente de vez en vez, constituida por un conjunto de caracteres numéricos obtenidos por un generador de números seudoaleatorios. Estos caracteres son devueltos por el usuario tras su cifrado mediante un algoritmo y clave sólo conocidos por éste y el ordenador.

[Ribagorda:1997]

2.303.5 CONTRASEÑA

Información de autenticación confidencial, usualmente compuesta por una cadena de caracteres. [ISO-7498-2:1989]

2.303.6 (EN) PASSWORD

1. a secret word or phrase that you need to know in order to be allowed into a place

2. a series of letters or numbers that you must type into a computer or computer system in order to be able to use it

Oxford Advanced Learner's Dictionary.

2.303.1 (EN) PASSWORD

A protected/private string of letters, numbers, and/or special characters used to authenticate an identity or to authorize access to data. [CNSSI_4009:2010]

2.303.2 (EN) PASSWORD

1a. (I) A secret data value, usually a character string, that is presented to a system by a user to authenticate the user's identity. (See: authentication information, challenge-response, PIN, simple authentication.)

1b. (O) "A character string used to authenticate an identity." [CSC2]

1c. (O) "A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization." [FP140]

1d. (O) "A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings." [SP63]

[RFC4949:2007]

2.303.3 (EN) PASSWORD

A series of characters grants a unique user access to a secured Web site, files, or application.

http://iab.com//

2.303.4 (EN) PASSWORD

A string of characters (letters, numbers and other symbols) that are used to authenticate an identity or to verify access authorization. [NIST-SP800-57:2007]

2.303.5 (EN) PASSWORD

a string of characters used to authenticate an identity or to verify access authorisation. [ISO-19790:2006]

2.303.6 (EN) PASSWORD

a string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. [FIPS-140-2:2001]

2.303.7 (EN) PASSWORD

A private character string that is used to authenticate an identity. [TCSEC:1985]

2.303.8 (EN) PASSWORD

Confidential authentication information, usually composed of a string of characters. [ISO-7498-2:1989]

2.303.9 (EN) ESCROW PASSWORDS

Escrow Passwords are passwords that are written down and stored in a secure location (like a safe) that are used by emergency personnel when privileged personnel are unavailable.

http://www.sans.org/security-resources/glossary-of-terms/

2.303.10 (FR) MOT DE PASSE

Information d'authentification confidentielle, habituellement composée d'une chaîne de caractères. [ISO-7498-2:1989]

2.303.11 (FR) MOT DE PASSE

Information secrète, personnelle et confidentielle détenue par un utilisateur lui permettant de se connecter à un système d'information et à ses ressources en fonction des droits et privilèges accordés. L'utilisation du mot de passe se fait généralement conjointement avec l'utilisation d'un identifiant enregistré et valide sur le système d'information accédé.

http://www.cases.public.lu/functions/glossaire/

2.303.12 (FR) MOT DE PASSE

Un mot de passe est un moyen utilisé pour authentifier une entité. Il s'agit d'une suite secrète de caractères.

http://securit.free.fr/glossaire.htm

2.304 CONTRASEÑA DE UN SOLO USO

Acrónimos: OTP

Ver:

- *Contraseña*
- http://www.ietf.org/rfc/rfc2289
- *Criptosistema de un solo uso*

2.304.1 CONTRASEÑA DESECHABLE

Datos usados como medio de autenticación, cuyo uso no se repite más de una vez. Habitualmente el ordenador ante el que se desea autenticar un usuario le lanza una pregunta (en ocasiones conocida como reto), diferente de vez en vez, constituida por un conjunto de caracteres numéricos obtenidos por un generador de números seudoaleatorios. Estos caracteres son devueltos por el usuario tras su cifrado mediante un algoritmo y clave sólo conocidos por éste y el ordenador. [Ribagorda:1997]

2.304.2 (EN) ONE-TIME PASSWORD, ONE-TIME PASSWORD (OTP)

1. (I) /not capitalized/ A "one-time password" is a simple authentication technique in which each password is used only once as authentication information that verifies an identity. This technique counters the threat of a replay attack that uses passwords captured by wiretapping.

2. (I) /capitalized/ "One-Time Password" is an Internet protocol [R2289] that is based on S/KEY and uses a cryptographic hash function to generate one-time passwords for use as authentication information in system login and in other processes that need protection against replay attacks.

[RFC4949:2007]

2.304.3 (EN) ONE-TIME PASSWORD - OTP

a password only used once thus countering replay attacks. [ISO-18028-4:2005]

2.304.4 (FR) MOT DE PASSE DYNAMIQUE

Mot de passe qui est créé dynamiquement via un équipement spécifique et transmis à l'utilisateur qui demande un accès à une ressource. Ce type de mot de passe n'est utilisable qu'une seule fois et possède une durée de validité très courte à l'inverse d'un mot de passe statique classique qui est utilisable plusieurs fois et possède une durée de validité beaucoup plus longue. On parle également de OTP signifiant One Time Password. Le mot de passe dynamique permet de sécuriser les accès aux ressources en ne communiquant le mot de passe de connexion qu'à la demande et ne nécessite pas d'être mémorisé puisque celui-ci n'est utilisable qu'une seule fois dans les quelques minutes qui ont suivi sa création. On évite ainsi les risques de partage des mots de passe et le risque de les voir écrits sur des papiers pour s'en souvenir.

http://www.cases.public.lu/functions/glossaire/

2.304.5 (FR) MOT DE PASSE NON RE-JOUABLE

Autrement dénommé One-time-password (OTP) en terminologie anglaise, un mot de passe non re-jouable est un mot de passe éphémère qui ne peut être utilisé qu'une seule fois pour authentifier une entité.

Les jetons (ou token) constituent un exemple typique de générateur de mots de passe non re-jouables.

http://securit.free.fr/glossaire.htm

2.305 CONTRASEÑA PREDETERMINADA

2.305.1 CONTRASEÑA PREDETERMINADA

Contraseña de las cuentas de usuario, servicio o administración de sistemas predefinidas en un sistema, aplicación o dispositivo asociado con la cuenta predeterminada. Las contraseñas y cuentas predeterminadas son de dominio público y, en consecuencia, es fácil averiguarlas.

http://es.pcisecuritystandards.org/

2.305.2 (EN) DEFAULT PASSWORD:

Password on system administration, user, or service accounts predefined in a system, application, or device; usually associated with default account. Default accounts and passwords are published and well known, and therefore easily guessed.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.305.3 (FR) MOT DE PASSE PAR DEFAUT

Mot de passe d'administration de système, d'utilisateur ou de service prédéfinis dans un système, une application ou un dispositif, ordinairement associé à un compte par défaut. Les comptes et mots de passe par défaut sont publiés et bien connus, et par conséquent, facilement devinés.

http://fr.pcisecuritystandards.org/

2.306 CONTROL

Ver:

- *Contra medida*
- *Salvaguarda*
- *Control preventivo*
- *Control que detecta*
- *Control general*
- *Control interno*
- *Control de gestión*
- *Control operativo*
- *Control técnico*
- *Riesgo*

2.306.1 CONTROL

Medida que modifica un riesgo. [UNE-ISO GUÍA 73:2010]

NOTA 1 Los controles incluyen cualquier proceso, política, dispositivo, práctica, u otras acciones que modifiquen un riesgo.

[UNE-ISO/IEC 27000:2014]

2.306.2 CONTROL

Medida que modifica un riesgo.

NOTA 1 Los controles incluyen cualquier proceso, política, dispositivo, práctica, u otras acciones que modifiquen un riesgo.

[UNE Guía 73:2010]

2.306.3 CONTROL

Un medio de gestión de Riesgo, asegurando que el Objetivo de Negocio es alcanzado, o asegurando que un Proceso es seguido. Ejemplos de Controles incluyen Políticas, Procedimientos, Roles, RAID, door-locks etc. Un control es llamado, algunas veces, Contramedida o medida de seguridad.

Control también es un medio de gestionar el uso o comportamiento de un Elemento de Configuración, Sistema o Servicio TI.

[ITIL:2007]

2.306.4 CONTROL

Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para proporcionar una garantía razonable de que los objetivos del negocio se alcanzarán y los eventos no deseados serán prevenidos o detectados. [COBIT:2006]

2.306.5 CONTROL

1. Procedimiento empleado para garantizar que un sistema satisface los requi9sitos de seguridad establecidos en la correspondiente política.

2. Medidas utilizadas para contrarrestar las amenazas previstas.

[Ribagorda:1997]

2.306.6 (EN) CONTROL

measure that is modifying risk [ISO Guide 73:2009]

NOTE 1: Controls include any process, policy, device, practice, or other actions which modify risk.

[ISO/IEC 27000:2014]

2.306.7 (EN) CONTROL

measure that is modifying risk

NOTE 1. Controls include any process, policy, device, practice, or other actions which modify risk.

[ISO Guide 73:2009]

2.306.8 (EN) SECURITY CONTROLS

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [CNSSI_4009:2010]

2.306.9 (EN) SECURITY CONTROLS

(N) The management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information. [FP199] (See: security architecture.) [RFC4949:2007]

2.306.10 (EN) CONTROL

A means of managing a Risk, ensuring that a Business Objective is achieved, or ensuring that a Process is followed. Example Controls include Policies, Procedures, Roles, RAID, door-locks etc. A control is sometimes called a Countermeasure or safeguard.

Control also means to manage the utilization or behaviour of a Configuration Item, System or IT Service.

[ITIL:2007]

2.306.11 (EN) CONTROL

The policies, procedures, practices and organisational structures designed to provide reasonable assurance that the business objectives will be achieved and undesired events will be prevented or detected. [COBIT:2006]

2.306.12 (EN) SECURITY CONTROLS

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [FIPS-200:2006] [FIPS-199:2004]

2.306.13 (EN) SECURITY CONTROL BASELINE

The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system. [CNSSI_4009:2010]

2.306.14 (EN) SECURITY CONTROL BASELINE

The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system. [FIPS-200:2006]

2.306.15 (EN) SECURITY CONTROLS

The management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system which, taken together, satisfy the systems specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information. [NIST-SP800-60V2:2004]

2.306.16 (EN) SECURITY CONTROL

An administrative, operational, technical, physical or legal measure for managing security risk. This term is synonymous with safeguard.

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

2.306.17 (EN) SECURITY CONTROL ASSESSMENT

The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. [NIST-SP800-53:2013]

2.306.18 (EN) SECURITY CONTROL ASSESSMENT

The testing and/or evaluation of the management, operational, and technical security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system or enterprise. [CNSSI_4009:2010]

2.306.19 (FR) CONTRÔLE

Moyen permettant de gérer un risque, en s'assurant que l'objectif business est atteint, ou en s'assurant qu'un processus est suivi. Exemples de contrôles: Polices, Procédures, Rôles, RAID, verrous, etc. Un contrôle est parfois appelé contre-mesure ou mesure de sécurité.

Le terme "contrôle" signifie également un moyen de gérer l'utilisation ou le comportement d'un élément de configuration, d'un système ou d'un service des TI.

[ITIL:2007]

2.306.20 (FR) MOYEN DE MAÎTRISE

mesure qui modifie un risque

NOTE 1. Un moyen de maîtrise du risque inclut n'importe quels processus, politique, dispositif, pratique ou autres actions qui modifient un risque.

[ISO Guide 73:2009]

2.306.21 (FR) CONTRÔLE

Dans le contexte de la sécurité ICT, le terme contrôle est habituellement considéré comme un synonyme de safeguard ou contre-mesure.

http://www.cases.public.lu/functions/glossaire/

2.306.22 (FR) CONTRÔLE DE SÉCURITÉ

Mesure administrative, opérationnelle, technique, physique ou juridique visant à gérer les risques pour la sécurité. Cette expression est synonyme de protection.

http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578

2.307 CONTROL DE ACCESO

Ver:

- *Control de acceso discrecional*
- *Control de acceso obligatorio*
- *Control de acceso por roles*
- *Control de acceso basado en reglas*
- *Mecanismo de control de acceso*
- *Control de acceso basado en atributos*

2.307.1 CONTROL DE ACCESO

Medios para asegurar que el acceso a los activos está autorizado y restringido en función de los requisitos de negocio y de seguridad. [UNE-ISO/IEC 27000:2014]

2.307.2 CONTROL DE ACCESO

Mecanismo que limita la disponibilidad de información o de los recursos necesarios para su procesamiento sólo a personas o aplicaciones autorizadas.

http://es.pcisecuritystandards.org

2.307.3 CONTROL DE ACCESOS

El proceso que limita y controla el acceso a los recursos de un sistema computacional; un control lógico o físico diseñado para brindar protección contra la entrada o el uso no autorizados. [COBIT:2006]

2.307.4 CONTROL DE ACCESO

Limitación del acceso a los recursos exclusivamente a personas, entidades o procesos con la debida autorización. [CCN-STIC-431:2006]

2.307.5 CONTROL DE ACCESO

Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

2.307.6 CONTROL DE ACCESO

Servicio de seguridad que previene el uso de un recurso salvo en los casos y de la manera autorizada (ISO-7498-2) [Ribagorda:1997]

2.307.7 MODELO DE CONTROL DE ACCESOS

Modelo de seguridad que expresa, en forma matricial, los derechos de acceso de los sujetos identificativos en un sistema sobre los objetos presentes en él.

Dos son los principales: Modelo de matriz de accesos de Harrison, Ruzzo y Ullman y Modelo de matriz de accesos de Graham y Denning.

[Ribagorda:1997]

2.307.8 CONTROL DE ACCESO

Servicio de seguridad que asegura que cada persona o entidad sólo pueda tener acceso a la información que está autorizado. Puede ser:

- Discrecional (discretionary): Por Necesidad de conocer.
- Por mandato (mandatory): Por disponer de nivel de habilitación acreditado. Como mecanismo de seguridad que presta dicho servicio incluye diversos procedimientos que lo aseguran (listas de personal y a qué está autorizado, contraseñas, tiempo de intento de acceso, ruta de intento de acceso, duración del acceso, etc.).

[CESID:1997]

2.307.9 CONTROL DE ACCESO

Prevención del uso no autorizado de un recurso, incluida la prevención del uso de un recurso de una manera no autorizada. [ISO-7498-2:1989]

2.307.10 (EN) ACCESS CONTROL

means to ensure that access to assets is authorized and restricted based on business and security requirements [ISO/IEC 27000:2014]

2.307.1 (EN) ACCESS CONTROL

The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances). [CNSSI_4009:2010]

2.307.1 (EN) ACCESS CONTROL MECHANISM

Security safeguards (i.e., hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system. [CNSSI_4009:2010]

2.307.2 (EN) ACESS CONTROL

Mechanisms that limit availability of information or information-processing resources only to authorized persons or applications.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.307.3 (EN) ACCESS CONTROL

1. (I) Protection of system resources against unauthorized access.

2. (I) A process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy. (See: access, access control service, computer security, discretionary access control, mandatory access control, role-based access control.)

3. (I) /formal model/ Limitations on interactions between subjects and objects in an information system.

4. (O) "The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner." [ISO-7498-2]

[RFC4949:2007]

2.307.4 (EN) ACCESS CONTROL

Restricts access to resources only to privileged entities. [NIST-SP800-57:2007]

2.307.5 (EN) ACCESS CONTROL

The process that limits and controls access to resources of a computer system; a logical or physical control designed to protect against unauthorised entry or use. [COBIT:2006]

2.307.6 (EN) ACCESS CONTROL

prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. [ISO-18028-2:2006]

2.307.7 (EN) ACCESS CONTROL

Enable authorized use of a resource while preventing unauthorized use or use in an unauthorized manner. [NIST-SP800-27:2004]

2.307.8 (EN) ACCESS CONTROL

The Access Control Security Dimension protects against unauthorized use of network resources. Access Control ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications. In addition, Role-Based Access Control (RBAC) provides different access levels to guarantee that individuals and devices can only gain access to and perform operations on network elements, stored information, and information flows that they are authorized for. [X.805:2003]

2.307.9 (EN) ACCESS CONTROL

Enable authorized use of a resource while preventing unauthorized use or use in an unauthorized manner. [NIST-SP800-33:2001]

2.307.10 (EN) ACCESS CONTROL

The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. [ISO-7498-2:1989]

2.307.11 (EN) ACCESS CONTROL

Access control refers to the rules and deployment mechanisms which control access to information systems, and physical access to premises. The entire subject of Information Security is based upon Access Control, without which Information Security cannot, by definition, exist.

http://www.passwordnow.com/en/glossary/access-control.html

2.307.12 (EN) ACCESS CONTROL

Access Control ensures that resources are only granted to those users who are entitled to them.

http://www.sans.org/security-resources/glossary-of-terms/

2.307.13 (FR) CONTRÔLE D'ACCÈS

Mécanisme limitant la disponibilité des informations oudes ressources de traitement des informations aux seules personnes ou applications autorisées.

http://fr.pcisecuritystandards.org/

2.307.14 (FR) CONTRÔLE D'ACCÈS

Précaution prise contre l'utilisation non autorisée d'une ressource; cela comprend les précautions prises contre l'utilisation d'une ressource de façon non autorisée. [ISO-7498-2:1989]

2.307.15 (FR) CONTRÔLE D'ACCÈS

Ensemble de mécanismes permettant de s'assurer du bien fondé de la demande de connexion à un système, une application ou une ressource et permettant d'interdire les accès si l'identification ou l'authentification a échoué ou si l'utilisateur demandant la connexion ne dispose pas d'un niveau de privilège suffisamment élevé pour accéder à la ressource demandée.

http://www.cases.public.lu/functions/glossaire/

2.308 CONTROL DE ACCESO BASADO EN ATRIBUTOS

Ver:

- *Control de acceso*

2.308.1 CONTROL DE ACCESO BASADO EN ATRIBUTOS

control de acceso que se basa en atributos relacionados con sujetos, objetos, objetivos, iniciadores, recursos, o con el entorno. Una regla de control de acceso permite o deniega el acceso en base a un conjunto de valores de los atributos. [NIST-SP800-53:2013]

2.308.2 (EN) ATTRIBUTE-BASED ACCESS CONTROL

Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place. [NIST-SP800-53:2013] [CNSSI_4009:2010]

2.309 CONTROL DE ACCESO BASADO EN IDENTIDAD

Ver:

- *Control de acceso*

2.309.1 CONTROL DE ACCESO BASADO EN IDENTIDAD

Control de acceso basado en la identidad del usuario. Típicamente se emplea alguna característica del proceso que requiere el acceso actuando en nombre del usuario final. Los derechos de acceso se conceden en base a la identidad declarada. [NIST-SP800-53:2013]

2.309.2 (EN) IDENTITY-BASED ACCESS CONTROL

Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity. [NIST-SP800-53:2013]

2.309.3 (EN) IDENTITY-BASED ACCESS CONTROL

Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity. [CNSSI_4009:2010]

2.310 CONTROL DE ACCESO BASADO EN POLÍTICAS

Acrónimos: PBAC

Ver:

- *Control de acceso*

2.310.1 CONTROL DE ACCESO BASADO EN POLÍTICAS

Forma de controlar el acceso basada en una utilización flexible de parámetros marcados por la política de autorización: identidad, role, habilitación personal, necesidad operacional, riesgos, heurísticos, etc.

2.310.2 (EN) POLICY BASED ACCESS CONTROL (PBAC)

A form of access control that uses an authorization policy that is flexible in the types of evaluated parameters (e.g., identity, role, clearance, operational need, risk, heuristics). [CNSSI_4009:2010]

2.311 CONTROL DE ACCESO BASADO EN REGLAS

Acrónimos: RSBAC

Ver:

- *Control de acceso*
- *Política de seguridad basada en reglas*

2.311.1 CONTROL DE ACCESO BASADO EN REGLAS

Control de acceso definido por medio de reglas que se imponen a los que acceden.

2.311.2 (EN) RULE SET BASED ACCESS CONTROL (RSBAC)

Rule Set Based Access Control targets actions based on rules for entities operating on objects.

http://www.sans.org/security-resources/glossary-of-terms/

2.312 CONTROL DE ACCESO DISCRECIONAL

Acrónimos: DAC

Ver:

- *Control de acceso*
- *Control de acceso obligatorio*

2.312.1 CONTROL DE ACCESO DISCRECIONAL

Procedimiento para restringir el acceso a los objetos de un sistema basado en la identidad de los sujetos.

El control se denomina discrecional, pues un sujeto con ciertos derechos de acceso puede pasar éstos, quizás indirectamente y siempre que no lo impida un control de acceso obligatorio, a otro sujeto cualquiera (TCSEC).

Se instrumenta para aplicar una política de seguridad basada en identidades.

[Ribagorda:1997]

2.312.1 (EN) DISCRETIONARY ACCESS CONTROL (DAC)

A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control). [CNSSI_4009:2010]

2.312.2 (EN) DISCRETIONARY ACCESS CONTROL

1a. (I) An access control service that (a) enforces a security policy based on the identity of system entities and the authorizations associated with the identities and (b) incorporates a concept of ownership in which access rights for a system resource may be granted and revoked by the entity that owns the resource. (See: access control list, DAC, identity-based security policy, mandatory access control.)

Derivation: This service is termed "discretionary" because an entity can be granted access rights to a resource such that the entity can by its own volition enable other entities to access the resource.

1b. (O) /formal model/ "A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject." [DoD1]

[RFC4949:2007]

2.312.3 (EN) DISCRETIONARY ACCESS CONTROL

A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control). [TCSEC:1985]

2.312.4 (EN) DISCRETIONARY ACCESS CONTROL (DAC)

Discretionary Access Control consists of something the user can manage, such as a document password.

http://www.sans.org/security-resources/glossary-of-terms/

2.313 CONTROL DE ACCESO OBLIGATORIO

Acrónimos: MAC

Ver:

- *Control de acceso*
- *Control de acceso discrecional*

2.313.1 CONTROL DE ACCESO OBLIGATORIO

Procedimiento para restringir el acceso a los objetos de un sistema. Está basado en la sensibilidad de la información contenida o tratada en éstos (expresada en una etiqueta de seguridad) y la autorización (denominada habilitación) de los sujetos que pretenden acceder (TCSEC).

Se instrumenta para aplicar una política de seguridad basada en reglas.

[Ribagorda:1997]

2.313.2 CONTROL DE ACCESO OBLIGATORIO

Modelo de seguridad en el que un responsable clasifica los objetos y sujetos según sus respectivos niveles de seguridad y habilitación y los compartimenta según el principio de mínimo privilegio. [Ribagorda:1997]

2.313.1 (EN) MANDATORY ACCESS CONTROL (MAC)

A means of restricting access to objects based on the sensitivity (as represented by a security label) of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals, and need-to-know) of subjects to access information of such sensitivity. [CNSSI_4009:2010]

2.313.2 (EN) MANDATORY ACCESS CONTROL

1. (I) An access control service that enforces a security policy based on comparing (a) security labels, which indicate how sensitive or critical system resources are, with (b) security clearances, which indicate that system entities are eligible to access certain resources. (See: discretionary access control, MAC, rule-based security policy.)

Derivation: This kind of access control is called "mandatory" because an entity that has clearance to access a resource is not permitted, just by its own volition, to enable another entity to access that resource.

[RFC4949:2007]

2.313.3 (EN) MANDATORY ACCESS CONTROL

A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity. [TCSEC:1985]

2.313.4 (EN) MANDATORY ACCESS CONTROL (MAC)

Mandatory Access Control controls is where the system controls access to resources based on classification levels assigned to both the objects and the users. These controls cannot be changed by anyone.

http://www.sans.org/security-resources/glossary-of-terms/

2.314 CONTROL DE ACCESO POR ROLES

Acrónimos: RBAC

Ver:

- *Control de acceso*
- *Rol*
- *Política de seguridad basada en la identidad*
- *Política de seguridad basada en reglas*

2.314.1 CONTROL DE ACCESO POR ROLES

Método de control de acceso en el que los derechos concedidos a un usuario dependen del role (o roles) a los que esté adscrito.

2.314.2 (EN) ROLE-BASED ACCESS CONTROL

Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals. [NIST-SP800-53:2013]

2.314.3 (EN) ROLE-BASED ACCESS CONTROL (RBAC)

Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals. [CNSSI_4009:2010]

2.314.4 (EN) ROLE-BASED ACCESS CONTROL

(I) A form of identity-based access control wherein the system entities that are identified and controlled are functional positions in an organization or process. [Sand] (See: authorization, constraint, identity, principal, role.) [RFC4949:2007]

2.314.5 (EN) RBAC

Acronym for “role-based access control.” Control used to restrict access by specific authorized users based on their job responsibilities.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.314.6 (EN) ROLE-BASED ACCESS CONTROL

method of access control management whereby the level of clearance and permission is primarily determined by the job or role that the individual fulfills in the organization.

2.314.7 (EN) ROLE BASED ACCESS CONTROL

Role based access control assigns users to roles based on their organizational functions and determines authorization based on those roles.

http://www.sans.org/security-resources/glossary-of-terms/

2.315 CONTROLES COMPENSATORIOS

2.315.1 CONTROLES DE COMPENSACIÓN

Es posible que los controles de compensación se consideren cuando una entidad no puede cumplir un requisito de manera explícita según lo establecido, debido a limitaciones técnicas legítimas o comerciales documentadas, pero ha mitigado de manera suficiente el riesgo asociado con el requisito a través de la implementación de controles. Los controles de compensación deben:

(1) Cumplir con el propósito y el rigor del requisito original de las PCI DSS;

(2) Proporcionar un nivel similar de defensa, como el requisito original de las PCI DSS;

(3) Superar ampliamente otros requisitos de las PCIDSS (no simplemente en cumplimiento de otros requisitos de las PCI DSS); y

(4) Ser cuidadoso con el riesgo adicional que impone la no adhesión al requisito de las PCI DSS.

Para obtener información acerca del uso de los controles de compensación, consulte los Anexos B y C de los Controles de compensación que se encuentran en los Requisitos de las PCI DSS y procedimientos para la evaluación de la seguridad.

http://es.pcisecuritystandards.org/

2.315.2 (EN) COMPENSATING CONTROLS:

Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must:

(1) Meet the intent and rigor of the original PCI DSS requirement;

(2) Provide a similar level of defense as the original PCI DSS requirement;

(3) Be “above and beyond” other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and

(4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

See “Compensating Controls” Appendices B and C in PCI DSS Requirements and Security Assessment Procedures for guidance on the use of compensating controls.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.315.3 (EN) COMPENSATING CONTROLS:

The term “compensating controls” is typically used within regulatory standards or guidelines to indicate when an alternative method than those specifically addressed by the standard or guideline is used. [knapp:2014]

2.315.4 (EN) COMPENSATING SECURITY CONTROL

A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system.

NIST SP 800.53: A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines described in NIST Special Publication 800-53 or in CNSS Instruction 1253, that provides equivalent or comparable protection for an information system.

[CNSSI_4009:2010]

2.315.5 (EN) COMPENSATING SECURITY CONTROLS

The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST SP 800-53, that provide equivalent or comparable protection for an information system. [NIST-SP800-18:2006]

2.315.6 (FR) CONTRÔLES COMPENSATOIRES

Il est possible d'envisager des contrôles compensatoires lorsqu'une entité ne peut pas remplir une condition exactement comme elle est stipulée, en raison de contraintes techniques légitimes ou de contraintes commerciales documentées, mais qu'elle a suffisamment atténué les risques associés par la mise en œuvre d'autres contrôles. Les contrôles compensatoires doivent:

(1) Respecter l'intention et la rigueur de la condition initiale de la normePCI DSS;

(2) Fournir une protection similaire à celle de la condition initiale de la norme PCI DSS;

(3) Excéder les autres conditions de la norme PCI DSS (et non être en simple conformité aux autres conditions de la norme).

(4) Correspondre aux risques supplémentaires qu'implique la non-conformité à la condition de la norme PCI DSS.

Voir les annexes B et C sur les «contrôles compensatoires» dans les Conditions et procédures d'évaluation de sécurité PCI DSS pour plus d'informations sur leur utilisation.

http://fr.pcisecuritystandards.org/

2.316 CONTROL DE CONFIGURACIÓN

Ver:

- *Configuración*
- *Gestión de la configuración*

2.316.1 CONTROL DE CONFIGURACIÓN

(Transición del Servicio) Actividad responsable de asegurar que la adición, modificación o eliminación de un CI se gestiona adecuadamente, por ejemplo enviando una Petición de Cambio o una Petición de Servicio. [ITIL:2007]

2.316.2 GESTIÓN DE LA CONFIGURACIÓN

Conjunto de procedimientos que regulan el almacenamiento y la modificación de la configuración y juego de reglas de los dispositivos. [CCN-STIC-401:2007]

2.316.3 CONTROL DE CONFIGURACIÓN

Sistema de control de cambios de los objetos durante el desarrollo, producción y mantenimiento del Objeto de Evaluación (ITSEC). [Ribagorda:1997]

2.316.1 (EN) CONFIGURATION CONTROL

Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications prior to, during, and after system implementation. [CNSSI_4009:2010]

2.316.2 (EN) CONFIGURATION CONTROL

(I) The process of regulating changes to hardware, firmware, software, and documentation throughout the development and operational life of a system. (See: administrative security, harden, trusted distribution.) [RFC4949:2007]

2.316.3 (EN) CONFIGURATION CONTROL

(Service Transition) The Activity responsible for ensuring that adding, modifying or removing a CI is properly managed, for example by submitting a Request for Change or Service Request. [ITIL:2007]

2.316.4 (EN) CONFIGURATION CONTROL

a system of controls imposed on changing controlled objects produced during the development, production and maintenance processes for a Target of Evaluation. [ITSEC:1991]

2.316.5 (FR) CONTRÔLE DES CONFIGURATIONS

(Transition de Services) Activité ayant en charge la gestion pertinente, des ajouts, modifications ou suppressions de CI. Par exemple, en soumettant une demande de changement ou une demande de service. [ITIL:2007]

2.317 CONTROL DE ENCAMINAMIENTO

2.317.1 CONTROL DE ENCAMINAMIENTO

Aplicación de las reglas oportunas durante el proceso de encaminamiento para escoger o evitar determinadas redes, enlaces o repetidores (ISO-7498-2). Es un control de utilidad cuando se sospecha el compromiso de alguno de los elementos citados. [Ribagorda:1997]

2.317.2 CONTROL DE ENCAMINAMIENTO

Aplicación de reglas durante el proceso de encaminamiento con el fin de elegir o evitar redes, enlaces o relevadores específicos. [ISO-7498-2:1989]

2.317.3 (EN) ROUTING CONTROL

The application of rules during the process of routing so as to chose or avoid specific networks, links or relays. [ISO-7498-2:1989]

2.317.4 (FR) CONTRÔLE DE ROUTAGE

Application de règles, au cours du processus de routage, afin de choisir ou d'éviter, des réseaux, liaisons ou relais spécifiques. [ISO-7498-2:1989]

2.318 CONTROL DE GESTIÓN

Ver:

- *Control*

2.318.1 CONTROL DE GESTIÓN

Controles o salvaguardas de un sistema de información relacionados con la gestión de riesgos y de la seguridad de la información.

2.318.2 (EN) MANAGEMENT CONTROLS

The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security. [FIPS-200:2006]

2.319 CONTROL DUAL

2.319.1 CONTROL DUAL

Proceso que consiste en utilizar dos o más entidades distintas (por lo general, personas) de manera coordinada para proteger funciones o información confidenciales. Ambas entidades son igualmente responsables de la protección física de los materiales que intervienen en transacciones vulnerables. Ninguna persona tiene permitido obtener acceso a o utilizar estos materiales (por ejemplo, la clave criptográfica). Para generar, transferir, cargar, almacenar y recuperar manualmente una clave, el proceso de control dual requiere que se divida el conocimiento de la clave entre las entidades. (Consulte también Conocimiento parcial).

http://es.pcisecuritystandards.org/

2.319.2 (EN) DUAL CONTROL:

Process of using two or more separate entities (usually persons) operating in concert to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person is permitted to access or use the materials (for example, the cryptographic key). For manual key generation, conveyance, loading,

storage, and retrieval, dual control requires dividing knowledge of the key among the entities. (See also Split Knowledge).

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.319.3 (EN) DUAL CONTROL

(I) A procedure that uses two or more entities (usually persons) operating in concert to protect a system resource, such that no single entity acting alone can access that resource. (See: no-lone zone, separation of duties, split knowledge.) [RFC4949:2007]

2.319.4 (FR) DOUBLE CONTRÔLE

Processus d'utilisation de deux ou plusieurs entités distinctes (habituellement des personnes) opérant de concert pour protéger des fonctions ou des informations sensibles. Les deux entités sont également responsables de la protection physique des documents impliqués dans des transactions vulnérables. Aucun individu n'est autorisé à accéder seul aux supports (par exemple, une clé cryptographique) ni à les utiliser. Pour la génération manuelle, le transfert, le chargement, le stockage et la récupération de clés, le double contrôle exige un partage des connaissances des clés entre les entités concernées. (Voir également Connaissance partagée).

http://fr.pcisecuritystandards.org/

2.320 CONTROL GENERAL

Ver:

- *Control*

2.320.1 CONTROL GENERAL

Control que afecta al funcionamiento global de la organización.

2.320.2 CONTROL GENERAL

También control general de TI. Un control que se aplica al funcionamiento general de los sistemas de TI de la organización y a un conjunto amplio de soluciones automatizadas (aplicaciones). [COBIT:2006]

2.320.3 (EN) GENERAL CONTROL

A control that applies to the overall functioning of the organisation's IT systems and to a broad set of automated solutions (applications). [COBIT:2006]

2.321 CONTROL INTERNO

Ver:

- *Control*

2.321.1 CONTROL INTERNO

Conjunto de políticas, procedimientos y estructuras organizativas diseñado para garantizar que se alcanzarán los objetivos de negocio, así como que los potenciales incidentes serán evitados o detectados y corregidos.

2.321.2 CONTROL INTERNO

Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una garantía razonable de que los objetivos del negocio se alcanzarán y de que los eventos indeseables serán prevenidos o detectados y corregidos [COBIT:2006]

2.321.3 (EN) INTERNAL CONTROL

The policies, procedures, practices and organisational structures designed to provide reasonable assurance that business will be achieved and undesired events will be prevented or detected and corrected. [COBIT:2006]

2.322 CONTROL OPERATIVO

Ver:

- *Control*

2.322.1 CONTROL OPERATIVO

Controles o salvaguardas de seguridad implementados y ejecutados por medio de personas. Se diferencias de los controles técnicos o automatizados.

2.322.2 (EN) OPERATIONAL CONTROLS

The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems). [FIPS-200:2006]

2.323 CONTROL PREVENTIVO

Ver:

- *Control*

2.323.1 CONTROL PREVENTIVO

Un control interno que se usa para prevenir eventos indeseables, errores u otras ocurrencias que pudieran tener un efecto material negativo sobre un proceso o producto final, de acuerdo a la organización. [COBIT:2006]

2.323.2 (EN) PREVENTIVE CONTROL

An internal control that is used to prevent undesirable events, errors and other occurrences than an organisation has determined could have a negative material effect on a process or end product. [COBIT:2006]

2.324 CONTROL QUE DETECTA

Ver:

- *Control*

2.324.1 CONTROL QUE DETECTA

Control utilizado para identificar incidentes o errores que la organización ha determinado como de interés en base a que hay posibles consecuencias en procesos o productos.

2.324.2 CONTROL DE DETECCIÓN

Un control que se usa para identificar eventos (indeseables o deseados), errores u otras ocurrencias con efecto material sobre un proceso o producto final, de acuerdo a lo definido por la empresa. [COBIT:2006]

2.324.3 (EN) DETECTIVE CONTROL

A control that is used to identify events (undesirable or desired), errors and other occurrences that an enterprise has determined to have a material effect on a process or end product. [COBIT:2006]

2.325 CONTROL TÉCNICO

Ver:

- *Salvaguarda*

2.325.1 CONTROL TÉCNICO

Salvaguarda o contramedida que básicamente está implementada con medios técnicos (equipos o programas).

2.325.2 (EN) TECHNICAL CONTROLS

The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. [FIPS-200:2006]

2.326 COOKIE

2.326.1 COOKIE

Pequeña cantidad de información que se le manda al navegador del cliente y que permite que éste quede identificado en conexiones sucesivas.

2.326.2 (EN) COOKIE

A character string, placed in a web browser’s memory, which is available to websites within the same Internet domain as the server that placed them in the web browser.

Cookies are used for many purposes and may be assertions or may contain pointers to assertions.

[NIST-SP800-63:2013]

2.326.3 (EN) COOKIE

Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use. [CNSSI_4009:2010]

2.326.4 (EN) COOKIE

1. (I) /HTTP/ Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use.

2. (I) /IPsec/ Data objects exchanged by ISAKMP to prevent certain denial-of-service attacks during the establishment of a security association.

[RFC4949:2007]

2.326.5 (EN) COOKIE

A file transmitted to a users browser to uniquely identify the users browser.

http://iab.com/

2.326.6 (EN) SESSION COOKIES

Temporary cookies which are only loaded for the active browser session and erased upon exiting the browser.

http://iab.com/

2.326.7 (EN) PERSISTENT COOKIE

A cookie that does not automatically gets erased and remains on the users system even after the user disconnects.

http://iab.com/

2.326.8 (EN) COOKIE

Small amount of data sent by the web server, to a web client, which can be stored and retrieved at a later time. Typically cookies are used to keep track of a users state as they traverse a web site. See also Cookie Manipulation.

http://www.webappsec.org/projects/glossary/

2.326.9 (EN) COOKIE MANIPULATION

Altering or modification of cookie values, on the clients web browser, to exploit security issues within a web application. Attackers will normally manipulate cookie values to fraudulently authenticate themselves to a web site. This is an example of the problem of trusting the user to provide reasonable input.

http://www.webappsec.org/projects/glossary/

2.327 COPIA DE SEGURIDAD

Ver:

- *Disponibilidad*
- *Plan de recuperación de desastres*

2.327.1 COPIA DE SEGURIDAD

Copia duplicada de datos que se realiza con el fin de archivarla o protegerla de daños o pérdidas.

http://es.pcisecuritystandards.org

2.327.2 COPIA DE SEGURIDAD

(Diseño del Servicio) (Operación del Servicio) Copiar los datos para proteger los originales de pérdidas de Integridad o Disponibilidad. [ITIL:2007]

2.327.3 COPIA DE RESPALDO

Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

2.327.4 COPIA DE SEGURIDAD

Réplicas de datos que nos permiten recuperar la información original en caso de ser necesario.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.327.5 (EN) BACKUP

Duplicate copy of data made for archiving purposes or for protecting against damage or loss.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.327.1 (EN) BACKUP

Copy of files and programs made to facilitate recovery, if necessary. [CNSSI_4009:2010]

2.327.2 (EN) BACK UP

(I) /verb/ Create a reserve copy of data or, more generally, provide alternate means to perform system functions despite loss of system resources. (See: contingency plan. Compare: archive.)

(I) /noun or adjective/ Refers to alternate means of performing system functions despite loss of system resources. (See: contingency plan).

[RFC4949:2007]

2.327.3 (EN) BACKUP

(Service Design) (Service Operation) Copying data to protect against loss of Integrity or Availability of the original. [ITIL:2007]

2.327.4 (EN) BACKUP

A copy of files and programs made to facilitate recovery if necessary. [NIST-SP800-34:2002]

2.327.5 (FR) SAUVEGARDE

Copie de données en double réalisée à des fins d'archivage ou de protection contre d'éventuels dommages ou pertes.

http://fr.pcisecuritystandards.org/

2.327.6 (FR) COPIE DE SAUVEGARDE (BACKUP)

(Conception de services) (Exploitation de Services) Copie des données permettant de protéger l'original de toute perte d'intégrité ou de disponibilité. [ITIL:2007]

2.328 CORRECCIÓN

2.328.1 CORRECCIÓN

Cumplimiento de las exigencias de seguridad desde el punto de vista de construcción del sistema, incluyendo el entorno, el proceso de desarrollo y el funcionamiento del sistema. [CESID:1997]

2.328.2 (EN) CORRECTNESS

(I) "The property of a system that is guaranteed as the result of formal verification activities." [Huff] (See: correctness proof, verification.) [RFC4949:2007]

2.328.3 (EN) CORRECTNESS

for specified security requirements, the representation of a product or system that shows the implementation of the requirement is correct. [ISO-21827:2007]

2.329 CORRESPONDENCIA DE POLÍTICAS

Ver:

- *Política*

2.329.1 CORRESPONDENCIA DE POLÍTICAS

Reconocimiento de que, cuando una autoridad de certificación en un dominio certifica una autoridad de certificación en otro dominio, una determinada política de certificación en el segundo dominio puede ser considerada por la autoridad del primer dominio como equivalente (pero no necesariamente idéntica en todos los aspectos) a una determinada política de certificado en el primer dominio. [X.509:2005]

2.329.2 (EN) POLICY MAPPING

Recognizing that, when a CA in one domain certifies a CA in another domain, a particular certificate policy in the second domain may be considered by the authority of the first domain to be

equivalent (but not necessarily identical in all respects) to a particular certificate policy in the first domain. [X.509:2005]

2.329.3 (FR) MAPPAGE DE POLITIQUE

reconnaissance du fait que, lorsqu'une autorité de certification d'un domaine certifie une autorité de certification d'un autre domaine, une politique de certificat propre au deuxième domaine peut être considérée par l'autorité du premier domaine comme équivalente (mais pas nécessairement comme identique sous tous ses aspects) à une politique de certificat dans le premier domaine. [X.509:2005]

2.330 CORTAFUEGOS

Ver:

- *Protección del perímetro*
- *Pasarela de seguridad*
- *Dispositivo de protección perimetral*
- http://en.wikipedia.org/wiki/Firewall_%28networking%29
- *Cortafuegos personal*
- *Pasarela*
- *Proxy (agente)*

2.330.1 FIREWALL

Tecnología de hardware y/o software que protege los recursos de red contra el acceso no autorizado. Un firewall autoriza o bloquea el tráfico de computadoras entre redes con diferentes niveles de seguridad basándose en un conjunto de reglas y otros criterios.

http://es.pcisecuritystandards.org

2.330.2 FIREWALL

Hardware o software cuya misión es la de proteger una red de otra. Normalmente una red local de Internet. [CCN-STIC-671:2006]

2.330.3 CORTAFUEGOS

Dispositivo de red físico o lógico que se utiliza para permitir, denegar o analizar las comunicaciones entre redes de datos, de acuerdo con las políticas de seguridad de la organización o del usuario. [CCN-STIC-614:2006]

2.330.4 CORTAFUEGOS

Sistema hardware / software que permite inspeccionar los paquetes que lo atraviesan y en función de un conjunto de reglas permitir o denegar el paso del mismo. [CCN-STIC-641:2006]

2.330.5 CORTAFUEGOS

Sistema formado por aplicaciones, dispositivos o combinación de estos encargado de hacer cumplir una política de control de acceso en las comunicaciones entre dispositivos según una política de seguridad existente. [CCN-STIC-400:2006]

2.330.6 CORTAFUEGOS DE SISTEMA

Cortafuegos centrado en el control de acceso local de un determinado nodo. [CCN-STIC-400:2006]

2.330.7 CORTAFUEGOS PERSONAL

Cortafuegos de sistema utilizado en estaciones de usuario. [CCN-STIC-400:2006]

2.330.8 CORTAFUEGOS TRANSPARENTE

Propiedad de un equipo cortafuegos que le permite ser "invisible" a los clientes y servidores de la comunicación residiendo en la capa de enlace de datos aunque sea capaz de intervenir a nivel de red. [CCN-STIC-400:2006]

2.330.9 CORTAFUEGOS VIRTUALES

Plataforma que permite la definición de cortafuegos lógicos o virtuales sobre un solo sistema físico pudiendo implementarse en ellos políticas de seguridad diferentes y ser gestionados individualmente. [CCN-STIC-400:2006]

2.330.10 CORTAFUEGOS

Dispositivo físico o lógico que canaliza todo el tráfico entre la red privada de una institución e Internet, para garantizar que dicho tráfico es conforme con la política de seguridad de la institución. [Ribagorda:1997]

2.330.1 (EN) FIREWALL

A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy. [CNSSI_4009:2010]

2.330.2 (EN) FIREWALL

1. (I) An internetwork gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall). (See: guard, security gateway.)

2. (O) A device or system that controls the flow of traffic between networks using differing security postures. [SP41]

[RFC4949:2007]

2.330.3 (EN) FIREWALL

A system using either hardware or software designed to prevent unauthorized access to or from a private network by examining each transmission block to see if it meets certain security criteria.

//http://iab.com/

2.330.4 (EN) FIREWALL

A firewall is some kind of security barrier placed between network environments. It may be a dedicated device, or a composite of several components and techniques. It has the properties so that all traffic from one network environment to another, and vice versa, must traverse through the firewall and only authorized traffic, as defined by the local security policy, will be allowed to pass. [ISO-18028-1:2006]

2.330.5 (EN) FIREWALL

Hardware and/or software technology that protects network resources from unauthorized access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.330.6 (EN) FIREWALL

A device or program that protects the permimeter of a network. Firewalls are placed at network gateways to prevent unwanted or malicious traffic from entering the organization's network and block unauthorised traffic from leaving the internal traffic.

2.330.7 (EN) WEB APPLICATION FIREWALL

An intermediary device, sitting between a web-client and a web server, analyzing OSI Layer-7 messages for violations in the programmed security policy. A web application firewall is used as a security device protecting the web server from attack.

http://www.webappsec.org/projects/glossary/

2.330.8 (EN) APPLICATION FIREWALL

An application firewall is an enhanced firewall that limits access by applications to the operating system (OS) of a computer. Conventional firewalls merely control the flow of data to and from the central processing unit (CPU), examining each packet and determining whether or not to forward it toward a particular destination. An application firewall offers additional protection by controlling the execution of files or the handling of data by specific applications.

http://searchsoftwarequality.techtarget.com/glossary/

2.330.9 (EN) FIREWALL

A logical or physical discontinuity in a network to prevent unauthorized access to data or resources.

http://www.sans.org/security-resources/glossary-of-terms/

2.330.10 (EN) NEXT-GENERATION FIREWALLS (NGFWS)

Next-generation firewalls (NGFWs) are deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall. An NGFW should not be confused with a stand-alone network intrusion prevention system (IPS), which includes a commodity or nonenterprise firewall, or a firewall and IPS in the same appliance that are not closely integrated.

http://www.gartner.com/it-glossary/

2.330.11 (EN) NEXT-GENERATION FIREWALL (NGFW):

A firewall beyond traditional port-based controls that enforces policy based on application, user, and content regardless of port or protocol.

Cybersecurity for Dummies, Palo Alto Networks Edition, 2014

2.330.12 (EN) DEEP-PACKET INSPECTION

The process of inspecting a network packet all the way to the application layer (Layer 7) of the OSI model. That is, past datalink, network or session headers to inspect all the way into the payload of the packet. Deep-packet inspection is used by most intrusion detection and prevention systems (IDS/ IPS), newer firewalls, and other security devices. [knapp:2014]

2.330.13 (FR) PARE-FEU

Technologie matérielle et/ou logicielle protégeant les ressources réseau contre les accès non autorisés. Un pare-feu autorise ou bloque le trafic informatique circulant entre des réseaux de différents niveaux de sécurité, selon un ensemble de règles et d'autres critères.

http://fr.pcisecuritystandards.org/

2.330.14 (FR) PARE-FEU

Mécanisme de sécurité localisé entre une zone de confiance (réseau local ou une machine personnelle) et un réseau externe non digne de confiance (par exemple Internet). La tâche du firewall est de contrôler et de filtrer, d'accepter ou de bloquer, en fonction de règles de sécurité définies par un administrateur, les communications entrantes et sortantes passant par lui. Les firewalls peuvent être de type hardware (firewall physique) mais aussi software (notamment pour la protection des ordinateurs personnels).

http://www.cases.public.lu/functions/glossaire/

2.331 CORTAFUEGOS PERSONAL

Ver:

- *Cortafuegos*
- http://en.wikipedia.org/wiki/Personal_firewall

2.331.1 CORTAFUEGOS PERSONAL

Cortafuegos para equipos personales.

2.331.2 (EN) PERSONAL FIREWALLS

Personal firewalls are those firewalls that are installed and run on individual PCs.

http://www.sans.org/security-resources/glossary-of-terms/

2.332 CPS - DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Acrónimos: CPS

Ver:

- *Política de certificación*
- http://www.ietf.org/rfc/rfc3647

2.332.1 DECLARACIÓN DE PRÁCTICA DE CERTIFICACIÓN

Declaración de las prácticas que aplica una autoridad de certificación para la expedición de certificados. [X.509:2005]

2.332.1 (EN) CERTIFICATION PRACTICE STATEMENT (CPS)

A listing of the practices that a Certification Authority employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this Certificate Policy, or requirements specified in a contract for services). [CNSSI_4009:2010]

2.332.2 (EN) CERTIFICATION PRACTICE STATEMENT (CPS)

(I) "A statement of the practices which a certification authority employs in issuing certificates." [DSG, R3647] (See: certificate policy.) [RFC4949:2007]

2.332.3 (EN) CERTIFICATION PRACTICE STATEMENT

A statement of the practices that a Certification Authority employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in a certificate policy or requirements specified in a contract for services). [NIST-SP800-53:2013]

2.332.4 (EN) CERTIFICATION PRACTICE STATEMENT (CPS)

A statement of the practices that a Certification Authority employs in issuing certificates. [X.509:2005]

2.332.5 (FR) DECLARATION DE PRATIQUE DE CERTIFICATION

déclaration des pratiques d'émission de certificats utilisées par une autorité de certification. [X.509:2005]

2.333 CRACKER

Ver:

- *Hacker*
- *Script kiddy*
- http://en.wikipedia.org/wiki/Black_hat

2.333.1 CRACKER

El cracker es una figura emparentada con el hacker. Su conducta va dirigida al acceso a sistemas informáticos de forma no autorizada, del mismo modo que los hackers, y con una finalidad clara: menoscabar la integridad, la disponibilidad y el acceso a la información disponible en dicho sitio web o en el sistema informático.

El desarrollo de esta actividad implica que se está cometiendo un acto delictivo, violándose la intimidad del afectado, la confidencialidad de la información y, específicamente en el caso del cracking, por el hecho de haber causado daños, cambios y/o destrucción de información así como por haber inhabilitado soportes físicos como puedan ser: servidores, discos duros, etc.

http://www.inteco.es/glossary/Formacion/Glosario/

2.333.2 CRACKER

Experto en seguridad, en general o en detalles muy concretos, que utiliza sus conocimientos con ánimo de sobrepasar la seguridad de los sistemas de información y alcanzar sus propios propósitos sin el consentimiento de los auténticos propietarios.

2.333.3 (EN) CRACKER

(I) Someone who tries to break the security of, and gain unauthorized access to, someone else's system, often with malicious intent. (See: adversary, intruder, packet monkey, script kiddy. Compare: hacker.) [RFC4949:2007]

2.333.4 (EN) CRACKER

A malicious hacker who uses their skills to do bad things.

http://www.getsafeonline.org/

2.333.5 (EN) BLACK HAT

A black hat (also called a cracker or Darkside hacker) is a malicious or criminal hacker. This term is seldom used outside of the security industry and by some modern programmers. The general public uses the term hacker to refer to the same thing. In computer jargon the meaning of "hacker" can be much broader. The name comes from the opposite of White Hat hackers.

Usually a Black Hat is a person who uses their knowledge of vulnerabilities and exploits for private gain, rather than revealing them either to the general public or the manufacturer for correction. Many Black Hats promote individual freedom and accessibility over privacy and security[citation needed]. Black Hats may seek to expand holes in systems; any attempts made to patch software are generally done to prevent others from also compromising a system they have already obtained secure control over. A Black Hat hacker may have access to 0-day exploits (private software that exploits security vulnerabilities; 0-day exploits have not been distributed to the public). In the most

extreme cases, Black Hats may work to cause damage maliciously, and/or make threats to do so as blackmail.

Black-hat hacking is the act of compromising the security of a system without permission from an authorized party, usually with the intent of accessing computers connected to the network (the somewhat similar activity of defeating copy prevention devices in software - which may or may not be legal depending on the laws of the given country - is actually software cracking). The term cracker was coined by Richard Stallman to provide an alternative to using the existing word hacker for this meaning. Use of the term "cracker" is mostly limited (as is "black hat") to some areas of the computer and security field and even there is considered controversial. A definition of a group that calls themselves hackers refers to "a group that consists of skilled computer enthusiasts". The other, and more common usage, refers to those who attempt to gain unauthorized access to computer systems. Many members of the first group attempt to convince people that intruders should be called crackers rather than hackers, but the common usage remains ingrained.

http://en.wikipedia.org/wiki/Black_hat

2.333.6 (EN) BLACK HAT

Black hat is used to describe a hacker (or, if you prefer, cracker) who breaks into a computer system or network with malicious intent. Unlike a white hat hacker, the black hat hacker takes advantage of the break-in, perhaps destroying files or stealing data for some future purpose. The black hat hacker may also make the exploit known to other hackers and/or the public without notifying the victim. This gives others the opportunity to exploit the vulnerability before the organization is able to secure it.

http://searchsecurity.techtarget.com/

2.333.7 (EN) CRACKER

A cracker is either a piece of software (program) whose purpose is to 'crack' the code to, say, a password; or 'cracker' refers to a person who attempts to gain unauthorised access to a computer system. Such persons are usually ill intentioned and perform malicious acts of techno-crime and vandalism.

http://www.passwordnow.com/en/glossary/cracker.html

2.333.8 (FR) CRACKER

Pirate informatique adepte du cracking.

http://www.cases.public.lu/functions/glossaire/

2.334 CREDENCIAL

2.334.1 CREDENCIALES DE AUTENTICACIÓN

Combinación del ID de usuario o ID de la cuenta más el (los) factor(es) utilizado(s) para autenticar a un individuo, dispositivo o proceso.

http://es.pcisecuritystandards.org

2.334.2 CREDENCIAL

Conjunto de datos transferidos entre entidades para comprobar la identidad alegada por una de ellas (ISO-7498-2). [Ribagorda:1997]

2.334.3 CREDENCIALES

Datos que se transfieren para establecer la identidad alegada de una entidad. [ISO-7498-2:1989]

2.334.4 (EN) AUTHENTICATION CREDENTIALS

Combination of the user ID or account ID plus the authentication factor(s) used to authenticate an individual, device, or process.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.334.5 (EN) CREDENTIAL

An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber.

While common usage often assumes that the credential is maintained by the Subscriber, this document also uses the term to refer to electronic records maintained by the CSP which establish a binding between the Subscriber's token and identity.

[NIST-SP800-63:2013]

2.334.6 (EN) CREDENTIAL SERVICE PROVIDER (CSP)

A trusted entity that issues or registers Subscriber tokens and issues electronic credentials to Subscribers. The CSP may encompass Registration Authorities (RAs) and Verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use. [NIST-SP800-63:2013]

2.334.1 (EN) CREDENTIAL

Evidence or testimonials that support a claim of identity or assertion of an attribute and usually are intended to be used more than once. [CNSSI_4009:2010]

2.334.2 (EN) CREDENTIAL

1. (I) /authentication/ "identifier credential": A data object that is a portable representation of the association between an identifier and a unit of authentication information, and that can be presented for use in verifying an identity claimed by an entity that attempts to access a system. Example: X.509 public-key certificate. (See: anonymous credential.)

2. (I) /access control/ "authorization credential": A data object that is a portable representation of the association between an identifier and one or more access authorizations, and that can be presented for use in verifying those authorizations for an entity that attempts such access. Example: X.509 attribute certificate. (See: capability token, ticket.)

3. (D) /OSIRM/ "Data that is transferred to establish the claimed identity of an entity." [ISO-7498-2]

[RFC4949:2007]

2.334.3 (EN) CREDENTIALS

Data that is transferred to establish the claimed identity of an entity. [ISO-7498-2:1989]

2.334.4 (FR) ÉLÉMENTS D'AUTHENTIFICATION

Combinaison de l'ID utilisateur ou de l'ID compte et du ou des facteurs d'authentification utilisés pour authentifier une personne, un dispositif ou un processus,

http://fr.pcisecuritystandards.org/

2.334.5 (FR) JUSTIFICATIF D'IDENTITÉ

Données transférées pour établir l'identité déclarée d'une entité. [ISO-7498-2:1989]

2.335 CRIBA DE SEGURIDAD

2.335.1 CRIBA DE SEGURIDAD

Cualquier medida orientada a garantizar que un individuo es fiable a los efectos de concederle unos determinados derechos de acceso a información sensible.

2.335.2 (EN) SECURITY SCREENING

Any measure resulting in a high level of assurance that an individual can be granted specific access privileges within the context of the federal government.

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

2.335.3 (FR) ENQUÊTE DE SÉCURITÉ

Toute mesure permettant d'obtenir un degré élevé d'assurance qu'une personne peut se voir accorder des privilèges d'accès spécifiques au sein du gouvernement fédéral.

http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578

2.336 CRIPTOANÁLISIS

Ver:

- *Criptología*
- *Ataques a la criptografía*
- *Criptografía robusta*
- *Criptoanálisis diferencial*
- *Criptoanálisis lineal*

2.336.1 CRIPTOANÁLISIS

Análisis de un sistema criptográfico, sus entradas y salidas, o ambas, para obtener variables o datos sensibles, incluyendo el texto en claro (ISO-7498-2) [Ribagorda:1997]

2.336.2 CRIPTOANÁLISIS

Pasos y operaciones orientadas a transformar un criptograma en el texto claro original pero sin conocer inicialmente el sistema de cifrado utilizado y/o la clave. [CESID:1997]

2.336.3 CRIPTOANALISTA O DESCRIPTADOR

Persona que efectúa criptoanálisis. [CESID:1997]

2.336.4 CRIPTOANÁLISIS (O ANÁLISIS CRIPTOGRÁFICO)

Análisis de un sistema criptográfico y/o sus entradas y salidas para derivar variables confidenciales y/o datos sensibles, incluido texto claro. [ISO-7498-2:1989]

2.336.1 (EN) CRYPTANALYSIS

1. Operations performed in defeating cryptographic protection without an initial knowledge of the key employed in providing the protection.

2. The study of mathematical techniques for attempting to defeat cryptographic techniques and/or information systems security. This includes the process of looking for errors or weaknesses in the implementation of an algorithm or of the algorithm itself.

[CNSSI_4009:2010]

2.336.2 (EN) CRYPTANALYSIS

1. (I) The mathematical science that deals with analysis of a cryptographic system to gain knowledge needed to break or circumvent the protection that the system is designed to provide. (See: cryptology, secondary definition under "intrusion".)

2. (O) "The analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including cleartext." [ISO-7498-2]

[RFC4949:2007]

2.336.3 (EN) CRYPTANALYSIS

1. Operations performed in defeating cryptographic protection without an initial knowledge of the key employed in providing the protection.

2. The study of mathematical techniques for attempting to defeat cryptographic techniques and information system security. This includes the process of looking for errors or weaknesses in the implementation of an algorithm or of the algorithm itself.

[NIST-SP800-57:2007]

2.336.4 (EN) CRYPTANALYSIS

The mathematical science that deals with analysis of a cryptographic system in order to gain knowledge needed to break or circumvent the protection that the system is designed to provide. In other words, convert the cipher text to plaintext without knowing the key.

http://en.wikipedia.org/wiki/Cryptanalysis

2.336.5 (EN) CRYPTANALYSIS

The analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including cleartext. [ISO-7498-2:1989]

2.336.6 (EN) CRYPTANALYSIS

The mathematical science that deals with analysis of a cryptographic system in order to gain knowledge needed to break or circumvent the protection that the system is designed to provide. In other words, convert the cipher text to plaintext without knowing the key.

http://www.sans.org/security-resources/glossary-of-terms/

2.336.7 (EN) CRYPTANALYSIS

The part of cryptology that deals with studying a secret message or a group of secret messages and breaking the system so you can read what it says without first knowing the key.

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.336.8 (FR) ANALYSE CRYPTOGRAPHIQUE

Analyse d'un système cryptographique, et/ou de ses entrées et sorties, pour en déduire des variables confidentielles et/ou des données sensibles (y compris un texte en clair). [ISO-7498-2:1989]

2.336.9 (FR) CRYPTANALYSE

Processus de déchiffrement sans utiliser les mécanismes prévus, comme par exemple sans être en possession de la clé.

http://www.cases.public.lu/functions/glossaire/

2.337 CRIPTOANÁLISIS DIFERENCIAL

Ver:

- *Ataques a la criptografía*
- *Criptoanálisis*

2.337.1 CRIPTOANÁLISIS DIFERENCIAL

Técnica critoanalítica de tipo estadístico, consistente en cifrar parejas de texto en claro escogidas con la condición de que su producto o-exclusivo obedezca a un patrón definido previamente. Los patrones de los correspondientes textos cifrados suministran información con la que conjeturar la clave criptográfica.

Se aplica en los cifrados de tipo DES, aunque es de destacar que precisamente éste es relativamente inmune al citado ataque.

[Ribagorda:1997]

2.337.2 (EN) DIFFERENTIAL CRYPTANALYSIS

A chosen plaintext attack relying on the analysis of the evolution of the differences between two plaintexts.

http://www.rsasecurity.com/rsalabs/faq

2.338 CRIPTOANÁLISIS LINEAL

Ver:

- *Ataques a la criptografía*
- *Criptoanálisis*
- *Ataque con texto en claro conocido*

2.338.1 CRIPTOANÁLISIS LINEAL

Técnica criptoanalítica de tipo estadístico, consistente en operar o-exclusivo dos bits del texto en claro, hacer lo mismo con otros dos del texto cifrado y volver a operar o-exclusivo los dos bits obtenidos. Se obtiene un bit que es el resultado de componer con la misma operación dos bits de la clave. Si se usan textos en claro recopilados y los correspondientes textos cifrados, se pueden conjeturar los bits de la clave. Cuantos más datos se tengan más fiable será el resultado.

Se aplica a los cifrados tipo DES.

[Ribagorda:1997]

2.338.2 (EN) LINEAR CRYPTANALYSIS

A known plaintext attack that uses linear approximations to describe the behavior of the block cipher.

http://www.rsasecurity.com/rsalabs/faq

2.339 CRIPTOCUSTODIO

Ver:

- *Responsable de seguridad corporativa*
- *Responsable de seguridad de la información*
- *Responsable de seguridad del sistema*

2.339.1 CRIPTOCUSTODIO

Responsable de la inicialización y la gestión de funciones y módulos criptográficos.

2.339.2 CUSTODIO CRIPTO

Persona designada como responsable de una cuenta cripto. [CESID:1997]

2.339.3 (EN) CRYPTO OFFICER

a role taken by an individual or a process (i.e., subject) acting on behalf of an individual allowing to perform cryptographic initialisation or management functions of a cryptographic module. [ISO-19790:2006]

2.339.4 (EN) CRYPTO OFFICER

An operator or process (subject), acting on behalf of the operator, performing cryptographic initialization or management functions. [FIPS-140-2:2001]

2.340 CRIPTÓFONO

Ver:

- *Cifrado digital de voz*

2.340.1 CRIPTÓFONO

Equipo de cifra que realiza un cifrado digital de la voz. (v. Secráfono). [CESID:1997]

2.340.2 CRIPTOFONÍA

Rama de la cifra que trata la voz. [CESID:1997]

2.340.3 (EN) CRYPTOPHONE

Cryptographic equipment for voice encryption.

2.341 CRIPTOGRAFÍA

Ver:

- *Criptología*

2.341.1 CRIPTOGRAFÍA

Disciplina matemática e informática relacionada con la seguridad de la información, particularmente con el cifrado y la autenticación. En cuanto a la seguridad de aplicaciones y redes, es una herramienta para el control de acceso, la confidencialidad de la información y la integridad.

http://es.pcisecuritystandards.org

2.341.2 CRIPTOGRAFÍA

Disciplina que estudia los principios, métodos y medios de transformar los datos con objeto de ocultar la información contenida en los mismos, detectar su modificación no autorizada y/o prevenir su uso no permitido (ISO-7498-2)

Disciplina que estudia los principios, métodos y medios de transformar los datos para ocultar la información contenida en ellos, garantizar su integridad, establecer su autenticidad y prevenir su repudio.

[Ribagorda:1997]

2.341.3 CRIPTOGRAFÍA

Rama de la cifra que trata la información escrita. [CESID:1997]

2.341.4 CRIPTOGRAFÍA

Disciplina que abarca los principios, medios y métodos para la transformación de los datos con el fin de esconder su contenido de información, impedir su modificación no detectada y/o su uso no autorizado.

NOTA. La criptografía determina los métodos utilizados en el cifrado y descifrado. Un ataque a los principios, medios y métodos criptográficos es criptoanálisis.

[ISO-7498-2:1989]

2.341.1 (EN) CRYPTOGRAPHY

Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form. [CNSSI_4009:2010]

2.341.2 (EN) CRYPTOGRAPHY

1. (I) The mathematical science that deals with transforming data to render its meaning unintelligible (i.e., to hide its semantic content), prevent its undetected alteration, or prevent its unauthorized use. If the transformation is reversible, cryptography also deals with restoring encrypted data to intelligible form. (See: cryptology, steganography.)

2. (O) "The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.... Cryptography determines the methods used in encipherment and decipherment." [ISO-7498-2]

[RFC4949:2007]

2.341.3 (EN) CRYPTOGRAPHY

discipline that embodies principles, means, and mechanisms for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. [ISO-7498-2:1989]

2.341.4 (EN) CRYPTOGRAPHY

Discipline of mathematics and computer science concerned with information security, particularly encryption and authentication. In applications and network security, it is a tool for access control, information confidentiality, and integrity.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.341.5 (EN) CRYPTOGRAPHY

The part of cryptology that deals with making codes or cipher systems so that others cannot read what is in the secret message.

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.341.6 (FR) CRYPTOGRAPHIE

Discipline mathématique et informatique concernant la sécurité des informations, en particulier le cryptage et l'authentification. Dans le cadre des applications et de la sécurité du réseau, la cryptographie est un outil de contrôle d'accès, de confidentialité et d'intégrité de l'information.

http://fr.pcisecuritystandards.org/

2.341.7 (FR) CRYPTOGRAPHIE

Discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification passe inaperçue et/ou d'empêcher leur utilisation non autorisée.

Remarque. La cryptographie détermine les méthodes de chiffrement et de déchiffrement. Une attaque portant sur les principes, moyens et méthodes de cryptographie est appelée analyse cryptographique.

[ISO-7498-2:1989]

2.341.8 (FR) CRYPTOGRAPHIE

Discipline qui englobe tous principes, moyens et méthodes destinés à la transformation de données afin de cacher leur contenu, d'empêcher leur modification et leur utilisation frauduleuse. [ISO-8732:1999]

2.342 CRIPTOGRAFÍA CUÁNTICA

2.342.1 CRIPTOGRAFÍA CUÁNTICA

Rama incipiente de la criptografía que estudia la aplicación de la mecánica cuántica a la misma. Según el principio de indeterminación de Heisenberg toda medida en un canal –por ejemplo, una interceptación- por el que circulan fotones provoca perturbaciones que delatan dicha medida. De esta manera, se pueden intercambiar claves secretas, para ser usadas en criptosistemas simétricos, mediante fotones portadores de bits, siendo su interceptación percibida por los interlocutores, quienes así podrán iniciar un nuevo intercambio. [Ribagorda:1997]

2.342.2 (EN) QUANTUM CRYPTOGRAPHY

Quantum cryptography, or quantum key distribution (QKD), uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages.

An important and unique property of quantum cryptography is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. This

results from a fundamental part of quantum mechanics: the process of measuring a quantum system in general disturbs the system. A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. By using quantum superpositions or quantum entanglement and transmitting information in quantum states, a communication system can be implemented which detects eavesdropping. If the level of eavesdropping is below a certain threshold a key can be produced which is guaranteed as secure (i.e. the eavesdropper has no information about), otherwise no secure key is possible and communication is aborted.

The security of quantum cryptography relies on the foundations of quantum mechanics, in contrast to traditional public key cryptography which relies on the computational difficulty of certain mathematical functions, and cannot provide any indication of eavesdropping or guarantee of key security.

Quantum cryptography is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. The algorithm most commonly associated with QKD is the one-time pad, as it is provably unbreakable when used with a secret, random key.

http://en.wikipedia.org/wiki/Quantum_cryptography

2.343 CRIPTOGRAFÍA DE CLAVE PÚBLICA

Acrónimos: PKC

Ver:

- *Técnica criptográfica asimétrica*
- *Certificado de clave pública*

2.343.1 CIFRA DE CLAVE PÚBLICA

Sistema en el que las claves para cifrar son distintas a las de descifrar, y en el que parte de las claves son conocidas (clave pública de cada usuario), y otra parte permanece en secreto (clave privada de cada usuario). Se basa en problemas criptográficos. [CESID:1997]

2.343.2 (EN) PUBLIC KEY CRYPTOGRAPHY (PKC)

Encryption system that uses a public-private key pair for encryption and/or digital signature. [CNSSI_4009:2010]

2.343.3 (EN) PUBLIC KEY CRYPTOGRAPHY

An encryption system utilizing asymmetric keys (for encryption/decryption) in which the keys have a mathematical relationship to each other which cannot be reasonably calculated. [H.235:2005]

2.343.4 (FR) CRYPTO-SYSTEME A CLE PUBLIQUE (OU ASYMETRIQUE)

Système cryptographique consistant en deux opérations complémentaires, chacune utilisant l'une des deux clés distinctes mais associées, la clé publique et la clé privée et possédant la propriété

selon laquelle il est impossible de déterminer, par un calcul sur ordinateur, la clé privée à partir de la clé publique. [ISO-11568-4:2007]

2.344 CRIPTOGRAFÍA DE CLAVE SECRETA

Ver:

- *Cifrado simétrico*

2.344.1 CIFRA DE CLAVE SECRETA O CIFRA SIMÉTRICA

Sistema en el que las claves para cifrar son iguales a las de descifrar, y en el que la totalidad o la mayor parte de las claves permanecen en secreto (clave secreta). [CESID:1997]

2.344.2 (EN) SECRET-KEY CRYPTOGRAPHY

(D) Synonym for "symmetric cryptography". [RFC4949:2007]

2.344.3 (EN) SECRET KEY (SYMMETRIC) CRYPTOGRAPHIC ALGORITHM

a cryptographic algorithm that uses a single secret key for both encryption and decryption. [FIPS-140-2:2001]

2.345 CRIPTOGRAFÍA DE CURVAS ELÍPTICAS

Acrónimos: ECC

Ver:

- *Criptografía de clave pública*

2.345.1 ECC

Acrónimo de “Elliptic Curve Cryptography” (criptografía de curva elíptica).

Método de criptografía de clave pública basado en curvas elípticas sobre campos finitos. Consulte Criptografía sólida.

http://es.pcisecuritystandards.org

2.345.2 CURVA ELÍPTICA

Función matemática que cuando se aplica sobre campos finitos proporciona un medio adecuado sobre el que se pueden implementar algoritmos de cifra de clave pública. [CESID:1997]

2.345.3 (EN) ECC

Acronym for “Elliptic Curve Cryptography.” Approach to public-key cryptography based on elliptic curves over finite fields. See Strong Cryptography.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.345.4 (EN) ECC (ELLIPTIC CURVE CRYPTOSYSTEM)

A method for creating public key algorithms, which some experts claim provides the highest strength-per-bit of any cryptosystem known today. Its algorithms accept an encryption key but then add extra numbers representing the coordinates of points on an imaginary wiggly curve as it crosses an imaginary line. Its complicated algebraic approach allows shorter keys to produce security equivalent to longer keys in other cryptosystems (such as RSA). Shorter keys mean the encryption and decryption can be performed relatively quickly and with less computer hardware. Numerous experts believe ECC will eventually enjoy widespread use.

http://www.watchguard.com/glossary/

2.345.5 (FR) ECC

Acronyme d'«Elliptic Curve Cryptography», cryptographie sur les courbes elliptiques. Approche de la cryptographie à clé publique basée sur des courbes elliptiques sur des champs finis. Voir Cryptographie robuste.

http://fr.pcisecuritystandards.org/

2.346 CRIPTOGRAFÍA ROBUSTA

Ver:

- *Criptoanálisis*

2.346.1 CRIPTOGRAFÍA SÓLIDA

Criptografía basada en algoritmos probados y aceptados por la industria, extensiones de clave sólidas (mínimos de 112 bits de solidez efectiva de clave) y prácticas adecuadas de administración de claves. La criptografía es un método de protección de datos e incluye tanto cifrado (reversible) como hashing (no reversible o de un solo uso). Al momento de la publicación, algunos ejemplos de normas y algoritmos de cifrado probados y aceptados por la industria incluyen: AES (128 bits y superior), TDES (claves mínimas de triple extensión), RSA (2048 bits y superior), ECC (160 bits y superior) y ElGamal (2048 bits y superior).

Para obtener más información respecto de la solidez de las claves y sobre los algoritmos, consulte la publicación especial de NIST 800-57 (http://csrc.nist.gov/publications/).

http://es.pcisecuritystandards.org

2.346.2 (EN) STRONG CRYPTOGRAPHY

Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key-management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or "one way"). Examples of industry-tested and accepted standards and algorithms for encryption include

- AES (128 bits and higher),
- TDES (minimum double-length keys),
- RSA (1024 bits and higher),
- ECC (160 bits and higher), and ElGamal (1024 bits and higher).

See NIST Special Publication 800-57 (www.csrc.nist.gov/publications/) for more information.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.346.3 (FR) CRYPTOGRAPHIE ROBUSTE

Cryptographie basée sur des algorithmes éprouvés et acceptés par le secteur, ainsi que sur une longueur de clés robustes (minimum 112 bits de robustesse effective de clé) et des pratiques appropriées de gestion des clés. La cryptographie est une méthode deprotection des données, comprenant à la fois un cryptage (réversible) et un hachage (non réversible, ou «unilatéral»). Au moment de la publication, les exemples de normes et d'algorithmes éprouvés et acceptés par le secteur du point de vue de la robustesse minimale de cryptage comprennent AES (128 bits et plus), TDES (clés à triple longueur minimum), RSA (2048 bits et plus), ECC (160 bits et plus) et ElGamal (2048 bits et plus).

Voir la publication spéciale NIST 800-57 Partie 1 (http://csrc.nist.gov/publications/) pour des recommandations plus approfondies sur la robustesse des clés cryptographiques et les algorithmes.

http://fr.pcisecuritystandards.org/

2.347 CRIPTOGRAMA

Ver:

- *Texto cifrado*

2.347.1 CRIPTOGRAMA

Texto cifrado formateado y listo para su transmisión.

Aunque usualmente se considera sinónimo de texto cifrado, este último enfatiza el simple resultado de cifrar sin ulterior preparación para la transmisión, mientras que criptograma pone el acento en la transmisión (como ocurre con telegrama).

En la actualidad es un término que está cayendo en desuso.

[Ribagorda:1997]

2.347.2 CRIPTOGRAMA

Texto cifrado ya formateado y preparado para la transmisión. [CESID:1997]

2.347.3 CRIPTOGRAMA (O TEXTO CIFRADO)

Datos producidos mediante cifrado. El contenido semántico de los datos resultantes no está disponible.

NOTA. Un criptograma puede ser cifrado, de nuevo, para obtener un criptograma supercifrado.

[ISO-7498-2:1989]

2.347.4 (EN) CRYPTOGRAM

A message that has been written in a secret cipher.

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.348 CRIPTOLOGÍA

Ver:

- *Criptografía*
- *Criptoanálisis*

2.348.1 CRIPTOLOGÍA

Estudio de los sistemas, claves y lenguajes ocultos o secretos.

DRAE. Diccionario de la Lengua Española.

2.348.2 CRIPTOLOGÍA

Ciencia que estudia los principios, métodos y medios del cifrado y descifrado de la información.

Comprende dos ramas principales: la Criptografía y el Criptoanálisis.

[Ribagorda:1997]

2.348.3 CRIPTOLOGÍA

Ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones, e inversamente la obtención de la información protegida. Comprende la cifra y el criptoanálisis. [CESID:1997]

2.348.4 CRIPTÓLOGO

Persona especialista en criptología, generalmente en el campo de la cifra. [CESID:1997]

2.348.1 (EN) CRYPTOLOGY

The mathematical science that deals with cryptanalysis and cryptography. [CNSSI_4009:2010]

2.348.2 (EN) CRYPTOLOGY

(I) The science of secret communication, which includes both cryptography and cryptanalysis. [RFC4949:2007]

2.348.3 (EN) CRYPTOLOGY

The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence. [NIST-SP800-60V2:2004]

2.348.4 (EN) CRYPTOLOGIST

A person who makes and/or breaks codes.

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.348.5 (EN) CRYPTOLOGY

The art and science of making (cryptography) and breaking (cryptanalysis) codes.

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.348.6 (FR) CRYPTOLOGIE

Étude des procédés de chiffrement. Ensemble de la cryptanalyse et de la cryptographie.

http://securit.free.fr/glossaire.htm

2.349 CRIPTOLÓGICO

2.349.1 CRIPTOLÓGICO

Perteneciente o relativo a la criptología.

DRAE. Diccionario de la Lengua Española.

2.350 CRIPTOSISTEMA

2.350.1 SISTEMA CRIPTOGRÁFICO, CRIPTOSISTEMA

Colección de transformaciones de texto claro en texto cifrado y viceversa, en la que la transformación o transformaciones que se han de utilizar son seleccionadas por claves. Las transformaciones son definidas normalmente por un algoritmo matemático. [X.509:2005]

2.350.2 CRIPTOSISTEMA

Conjunto de claves y equipos de cifra que utilizados coordinadamente ofrecen un medio para cifrar y descifrar. (v. Red de cifra). [CESID:1997]

2.350.3 CRIPTOSISTEMA CUÁNTICO

Criptosistema basado en aspectos de la física cuántica, utilizando la transmisión de fotones. [CESID:1997]

2.350.4 CRIPTOSISTEMA DE USO ÚNICO (ONE-TIME-CRYPTOSYSTEM)

Criptosistema que utiliza las claves una sola vez. [CESID:1997]

2.350.5 CRIPTOSISTEMA ELECTRÓNICO

Criptosistema en que el equipo de cifra es electrónico. [CESID:1997]

2.350.6 CRIPTOSISTEMA MANUAL

Criptosistema que carece de equipo de cifra, siendo sustituido por una serie de operaciones efectuadas manualmente. [CESID:1997]

2.350.7 CRIPTOSISTEMA MECÁNICO

Criptosistema en que el equipo de cifra es mecánico. [CESID:1997]

2.350.8 CRIPTOSISTEMA PROBABILÍSTICO

Criptosistema basado en que al cifrar un mismo mensaje, con la misma clave, no se obtiene siempre el mismo mensaje cifrado. [CESID:1997]

2.350.9 (EN) CRYPTOGRAPHIC SYSTEM

1. (I) A set of cryptographic algorithms together with the key management processes that support use of the algorithms in some application context.

2. (O) "A collection of transformations from plain text into cipher text and vice versa [which would exclude digital signature, cryptographic hash, and key-agreement algorithms], the particular transformation(s) to be used being selected by keys. The transformations are normally defined by a mathematical algorithm." [X509]

[RFC4949:2007]

2.350.10 (EN) CRYPTOGRAPHIC SYSTEM, CRYPTOSYSTEM

A collection of transformations from plain text into ciphertext and vice versa, the particular transformation(s) to be used being selected by keys. The transformations are normally defined by a mathematical algorithm. [X.509:2005]

2.350.11 (EN) CRYPTOSYSTEM

A method or process for changing regular text to hide its real meaning.

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.350.12 (FR) SYSTÈME DE CHIFFREMENT

ensemble de transformations d'un texte en clair pour obtenir un texte chiffré et réciproquement, le choix de la ou des transformations particulières à utiliser se faisant au moyen de clés. Les transformations sont définies en général par un algorithme mathématique. [X.509:2005]

2.351 CRIPTOSISTEMA DE UN SOLO USO

Ver:

- *Clave de un solo uso*
- *Máscara de un solo uso*
- *Contraseña de un solo uso*

2.351.1 CRIPTOSISTEMA DE UN SOLO USO

Criptosistema que utiliza una clave una sola vez.

2.351.2 (EN) ONE-TIME CRYPTOSYSTEM

Cryptosystem employing key used only once. [CNSSI_4009:2010]

2.352 CRITERIOS COMUNES

Acrónimos: CC (es), CC

Ver:

- *ITSEC - Information Technology Security Evaluation Criteria*
- *TCSEC - Trusted Computer System Evaluation Criteria*
- http://en.wikipedia.org/wiki/Common_Criteria
- *Nivel de garantía de evaluación*
- *Perfil de protección*
- *Declaración de seguridad*
- *Objeto de evaluación*
- *Administrador*
- *Activo*
- *Garantía*
- *Ataque*
- *Ampliación*
- *Información de autenticación*
- *Autorización*
- *Bypass*
- *Canal encubierto*
- *Evaluación*
- *Autoridad de evaluación*
- *Esquema de evaluación*
- *Evidencia*
- *Identidad*
- *Ataques por monitorización*
- *Prueba*
- *Rol*
- *Dominio de seguridad*
- *Objetivo de seguridad*
- *Política de seguridad*
- *Confianza*
- *Canal confiable*
- *Acceso fiable*
- *Vulnerabilidad*
- *Informativo*
- *Formal*
- *Informal*
- *Semiformal*
- *Obligatorio*

2.352.1 CRITERIOS COMUNES

Este estándar, los Criterios Comunes (CC), tiene como finalidad el ser usado como base para la evaluación de las propiedades de seguridad de los productos y sistemas de Tecnologías de la Información (TI). Estableciendo esta base de criterios comunes, los resultados de una evaluación de seguridad de TI será significativa para una mayor audiencia.

Los CC permitirán la comparación entre los resultados de evaluaciones de seguridad independientes, al proporcionar un conjunto común de requisitos para las funciones de seguridad de los productos y sistemas de TI y para las medidas de garantía aplicadas a éstos durante la evaluación de seguridad. El proceso de evaluación establece un nivel de confianza del grado en que las funciones de seguridad de tales productos y sistemas y las medidas de garantía aplicadas coinciden con aquellos requisitos. Los resultados de la evaluación pueden ayudar a los consumidores a determinar si el producto o sistema de TI es suficientemente seguro para la aplicación pretendida y si los riesgos de seguridad implícitos en su uso son aceptables.

Los CC son útiles como guía para el desarrollo de productos o sistemas con funciones de seguridad de TI y para la adquisición de productos y sistemas comerciales con dichas funciones. Durante la evaluación, el producto o sistema de TI es conocido como el objeto de evaluación o TOE (Target Of Evaluation). Este TOE incluye, por ejemplo, sistemas operativos, redes de ordenadores, sistemas distribuidos y aplicaciones.

Los CC tratan la protección de la información contra la revelación no autorizada, modificación o pérdida de uso. Las categorías de protección relacionadas con estos tres tipos de fallos de seguridad son llamadas normalmente confidencialidad, integridad y disponibilidad respectivamente. Los CC pueden ser también aplicables en aspectos de seguridad de TI distintos a estos tres. Los CC se concentran en aquellas amenazas que provienen de una actividad humana, ya sea maliciosa o de otro tipo, pero también pueden ser aplicables a otras amenazas no humanas. Además, los CC pueden ser aplicados en otras áreas distintas de TI pero no se hace ninguna declaración de competencia fuera del estricto ámbito de la seguridad de TI.

Los CC son aplicables a las medidas de seguridad de TI implementadas en hardware, firmware o software. Cuando se pretenda tratar aspectos particulares de evaluación a aplicar sólo en determinados métodos de implementación, se indicará expresamente en las declaraciones de los criterios correspondientes.

Algunos temas, porque involucran técnicas especializadas o porque son, de alguna manera, adyacentes a la seguridad de TI, son considerados ajenos a la finalidad de los CC. Entre estos cabe destacar los siguientes:

- Los CC no contienen criterios de evaluación de la seguridad correspondientes a medidas de seguridad administrativa no relacionadas directamente con las medidas de seguridad de TI. Sin embargo, se reconoce que una parte significativa de la seguridad de un TOE puede, a menudo, proporcionarse a través de medidas administrativas (organizativas, de personal, físicas y control de procedimientos). Las medidas de seguridad administrativas, en el entorno operativo del TOE, son tratadas como hipótesis de un uso seguro donde éstas tienen un impacto importante en la capacidad de las medidas de seguridad de TI para contrarrestar las amenazas identificadas.
- La evaluación de aspectos técnicos físicos de la seguridad de TI como control de radiaciones electromagnéticas no se trata específicamente, aunque varios de los conceptos tratados serán aplicables en este área. En particular, los CC tratan algunos aspectos de la protección física del TOE.

- Los CC no tratan ni la metodología de evaluación ni el marco administrativo y legal bajo el cual los criterios pueden ser aplicados por las autoridades de evaluación. Sin embargo, se espera que los CC sean usados para propósitos de evaluación en el contexto de un determinado marco administrativo y con una determinada metodología.
- Los procedimientos para el uso de los resultados de la evaluación en la acreditación de productos o sistemas están fuera del objetivo de los CC. La acreditación de un producto o sistema es el proceso administrativo por el que se autoriza el uso de dicho producto o sistema de TI en su entorno operativo. La evaluación se centra en las partes de seguridad de TI del producto o sistema y en aquellas partes del entorno operativo que pueden afectar directamente el seguro uso de los elementos de TI. Los resultados del proceso de evaluación son, por lo tanto, un dato de valor para el proceso de acreditación. Sin embargo, como hay otras técnicas más apropiadas para la valoración, tanto de las propiedades de seguridad de un producto o sistema no relacionadas con TI, como de su relación con las partes de seguridad de TI, los acreditadores deberán establecer separadamente estos aspectos.
- Los criterios para la valoración de las cualidades inherentes de los algoritmos criptográficos no se tratan en los CC. Si se necesita una valoración independiente de las propiedades matemáticas de la criptografía introducida en un TOE, deberá ser proporcionada por el esquema bajo el cual se están aplicando los CC.

[CC:2006]

2.352.2 (EN) COMMON CRITERIA

Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems. [CNSSI_4009:2010]

2.352.3 (EN) COMMON CRITERIA

The CC will permit comparability between the results of independent security evaluations. It does so by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. The evaluation process establishes a level of confidence that the security functions of such products and systems and the assurance measures applied to them meet these requirements. The evaluation results may help consumers to determine whether the IT product or system is secure enough for their intended application and whether the security risks implicit in its use are tolerable. [CC:2006]

2.352.4 (EN) COMMON CRITERIA

Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems

The Tallinn Manual, 2013

2.353 CRITERIOS DE EVALUACIÓN DE RIESGOS

Ver:

- *Evaluación de riesgos*
- *Riesgo*

2.353.1 CRITERIOS DE RIESGO:

Términos de referencia respecto a los que se evalúa la importancia de un riesgo. [UNE-ISO GUÍA 73:2010]

NOTA 1 Los criterios de riesgo se basan en los objetivos de la organización, y en el contexto externo e interno.

NOTA 2 Los criterios de riesgo se pueden obtener de normas, leyes, políticas y otros requisitos.

[UNE-ISO/IEC 27000:2014]

2.353.2 CRITERIOS DE EVALUACIÓN DE RIESGOS

Términos de referencia que permiten evaluar la importancia de los riesgos.

NOTA. Los criterios de evaluación pueden incluir los costes y los beneficios asociados, los requisitos legales o reglamentarios, los aspectos socioeconómicos y ambientales, las preocupaciones de las partes interesadas, las prioridades y otros datos utilizados en la evaluación de los riesgos.

[UNE-71504:2008]

2.353.3 CRITERIOS DE RIESGO

Términos de referencia respecto a los que se evalúa la importancia de un riesgo. [UNE Guía 73:2010]

2.353.4 (EN) RISK CRITERIA

terms of reference against which the significance of risk is evaluated [ISO Guide 73:2009]

NOTE 1: Risk criteria are based on organizational objectives, and external and internal context.

NOTE 2: Risk criteria can be derived from standards, laws, policies and other requirements

[ISO/IEC 27000:2014]

2.353.5 (EN) RISK CRITERIA

terms of reference against which the significance of a risk is evaluated. [ISO Guide 73:2009]

2.353.6 (FR) CRITÈRES DE RISQUE

termes de référence vis-à-vis desquels l'importance d'un risque est évaluée. [ISO Guide 73:2009]

2.354 CRITICIDAD

2.354.1 CRITICIDAD

Término que se emplea para referirse a las consecuencias de un comportamiento incorrecto del sistema. El nivel de criticidad es mayor cuanto más graves sean las consecuencias directas e indirectas de un comportamiento erróneo.

2.354.2 (EN) CRITICALITY LEVEL

Refers to the (consequences of) incorrect behavior of a system. The more serious the expected direct and indirect affects of incorrect behavior, the higher the criticality level. [CNSSI_4009:2010]

2.354.3 (EN) CRITICAL ASSETS

Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. [NERC:2014]

2.355 CRL COMPLETA

Ver:

- *Lista de revocación de certificados*
- *CRL incremental*

2.355.1 CRL COMPLETA

Lista íntegra de todos los certificados revocados en un momento dado, en un cierto ámbito.

lista de revocación de certificados completa

Lista de revocación completa que contiene asientos para todos los certificados que han sido revocados en un ámbito determinado.

[X.509:2005]

2.355.2 (EN) FULL CRL

A complete revocation list that contains entries for all certificates that have been revoked for the given scope. [X.509:2005]

2.355.3 (FR) LISTE CRL COMPLÈTE

liste de révocation complète contenant des éléments pour tous les certificats qui ont été révoqués pour le domaine d'application donné. [X.509:2005]

2.356 CRL INCREMENTAL

Ver:

- *Lista de revocación de certificados*
- *CRL completa*

2.356.1 CRL INCREMENTAL

Fragmento de una lista de revocación (CRL). La fragmentación se hace de tal forma que sólo incorpore los cambios respecto de la versión anterior. De esta forma se ahorra tiempo y volumen de transmisión, a costa de que el verificador debe guardar copia de las deltas previas.

lista de revocación de certificados-delta (dCRL, delta-CRL)

Lista de revocación de certificados parcial que contiene únicamente asientos para certificados cuyo estado de revocación ha sido modificado después de la expedición de la lista de revocación de certificados básica referenciada.

[X.509:2005]

2.356.2 (EN) DELTA CRL

(I) A partial CRL that only contains entries for certificates that have been revoked since the issuance of a prior, base CRL [X509]. This method can be used to partition CRLs that become too large and unwieldy. (Compare: CRL distribution point.) [RFC4949:2007]

2.356.3 (EN) DELTA-CRL

A dCRL is a partial revocation list that only contains entries for certificates that have had their revocation status changed since the issuance of the referenced base CRL. [X.509:2005]

2.356.4 (FR) LISTE CRL DELTA (LISTE DCRL)

liste de révocation partielle contenant uniquement des éléments pour des certificats dont le statut de révocation a été modifié depuis la publication de la liste CRL de base référencée. [X.509:2005]

2.357 CRL INDIRECTO

Ver:

- *Lista de revocación de certificados*

2.357.1 CRL INDIRECTO

Lista de revocación que contiene, al menos, información de revocación de certificados emitidos por entidades diferentes de la que emite la lista de revocación en consideración.

lista de revocación de certificados indirecta

Lista de revocación que contiene por lo menos información de revocación sobre certificados expedidos por autoridades distintas de la que expidió esta lista de revocación de certificados.

[X.509:2005]

2.357.2 (EN) INDIRECT CRL

An iCRL is a revocation list that at least contains revocation information about certificates issued by authorities other than that which issued this CRL. [X.509:2005]

2.357.3 (FR) LISTE CRL INDIRECTE

liste de révocation qui contient au moins une information de révocation concernant des certificats émis par des autorités autres que l'émetteur de cette liste. [X.509:2005]

2.358 CROSS-SITE REQUEST FORGERY

Acrónimos: CSRF, XSRF

2.358.1 FALSIFICACIÓN DE SOLICITUDES ENTRE DISTINTOS SITIOS (CSRF)

Estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y que permiten que se ejecuten acciones no deseadas mediante una sesión que ha sido autenticada. Suele utilizarse junto con XSS o inyección SQL.

http://es.pcisecuritystandards.org

2.358.2 CROSS SITE REQUEST FORGERY

El CSRF (del inglés Cross-site request forgery o falsificación de petición en sitios cruzados) es un tipo de exploit malicioso de un sitio web en el que comandos no autorizados son transmitidos por un usuario en el cual el sitio web confía. Esta vulnerabilidad es conocida también por otros nombres como XSRF, enlace hostil, ataque de un click, cabalgamiento de sesión, y ataque automático.

http://es.wikipedia.org/wiki/Cross_Site_Request_Forgery

2.358.3 (EN) CROSS-SITE REQUEST FORGERY (CSRF):

Vulnerability that is created from insecure coding methods that allows for the execution of unwanted actions through an authenticated session. Often used in conjunction with XSS and/or SQL injection.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.358.4 (EN) CROSS-SITE REQUEST FORGERY

Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.

http://en.wikipedia.org/wiki/Cross-site_request_forgery

2.358.5 (FR) ATTAQUES CROSS-SITE REQUEST FORGERY (CSRF)

Vulnérabilité qui est créée par des méthodes de codage non sécurisées qui permettent l'exécution d'actions indésirables au moyen d'une session d'authentification. Souvent utilisées avec une injection XSS et/ou SQL.

http://fr.pcisecuritystandards.org/

2.359 CROSS SITE SCRIPTING

Acrónimos: XSS

Ver:

- *Cross-zone scripting*

2.359.1 LENGUAJE DE COMANDOS ENTRE DISTINTOS SITIOS (XSS)

Estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y que tiene como resultado una validación de entradas inapropiada. Suele utilizarse junto con CSRF o inyección SQL.

http://es.pcisecuritystandards.org

2.359.2 XSS

Secuencias de comandos en sitios cruzados (Cross-site Scripting) es una brecha de seguridad que se produce en páginas Web generadas dinámicamente. En un ataque por XSS, una aplicación Web se envía con un script que se activa cuando lo lee el navegador de un usuario o una aplicación vulnerable. Dado que los sitios dinámicos dependen de la interacción del usuario, es posible ingresar un script malicioso en la página, ocultándolo entre solicitudes legítimas. Los puntos de entrada comunes incluyen buscadores, foros, blogs y todo tipo de formularios en línea en general. Una vez iniciado el XSS, el atacante puede cambiar configuraciones de usuarios, secuestrar cuentas, envenenar cookies, exponer conexiones SSL, acceder sitios restringidos y hasta instalar publicidad en el sitio víctima.

http://www.inteco.es/glossary/Formacion/Glosario/

2.359.3 XSS (CROSS-SITE SCRIPTING)

Es una brecha de seguridad que se produce en páginas Web generadas dinámicamente. En un ataque por XSS, una aplicación Web se envía con un "script" que se activa cuando lo lee el navegador de un usuario o una aplicación vulnerable. Dado que los sitios dinámicos dependen de la interacción del usuario, es posible ingresar un "script" malicioso en la página, ocultándolo entre solicitudes legítimas. Los puntos de entrada comunes incluyen buscadores, foros, "blogs" y todo tipo de formularios "online" en general. Una vez iniciado el XSS, el atacante puede cambiar configuraciones de usuarios, secuestrar cuentas, envenenar "cookies", exponer conexiones SSL, acceder sitios restringidos y hasta instalar publicidad en el sitio víctima.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.359.4 VULNERABILIDAD CROSS-SITE-SCRIPTING

Esta falla permite a un atacante introducir en el campo de un formulario o código embebido en una página, un "script" (perl, php, javascript, asp) que tanto al almacenarse como al mostrarse en el navegador, puede provocar la ejecución de un código no deseado.

http://www.vsantivirus.com/vul-webcamxp.htm

2.359.5 (EN) CROSS SITE SCRIPTING (XSS)

A vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and client. Websites are vulnerable if they display user supplied data from requests or forms without sanitizing the data so that it is not executable. [NIST-SP800-63:2013]

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.359.6 (EN) CROSS-SITE SCRIPTING (XSS)

A type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites

Scope Note: Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encodingit. (OWASP)

ISACA, Cybersecurity Glossary, 2014

2.359.7 (EN) CROSS-SITE SCRIPTING (XSS)

Is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy.

http://en.wikipedia.org/wiki/XSS

2.359.8 (EN) CROSS-SITE SCRIPTING

An attack technique that forces a web site to echo client-supplied data, which execute in a users web browser. When a user is Cross-Site Scripted, the attacker will have access to all web browser content (cookies, history, application version, etc).

http://www.webappsec.org/projects/glossary/

2.359.9 (FR) ATTAQUES CROSS-SITE SCRIPTING (XSS)

Vulnérabilité qui est créée par des techniques de codage non sécurisées, ce qui provoque la validation d'une entrée incorrecte. Souvent utilisées avec une injection CSRF et/ou SQL.

http://fr.pcisecuritystandards.org/

2.360 CROSS-ZONE SCRIPTING

Ver:

- *Escalada de privilegios*
- *Cross site scripting*

2.360.1 CROSS-ZONE SCRIPTING

Vulnerabilidad de un navegador www consistente en que páginas web con código ejecutable (scripts) ejecutan este en unza zona de seguridad que no le corresponde, aprovechando que la página se abre en una zona privilegiada.

Se trata de un problema de escalado de privilegios.

2.360.2 (EN) CROSS-ZONE SCRIPTING

is a browser exploit taking advantage of a vulnerability within a zone-based security solution. The attack allows content (scripts) in unprivileged zones to be executed with the permissions of a privileged zone - i.e. a privilege escalation within the client (web browser) executing the script. The vulnerability could be:

- a web browser bug which under some conditions allows content (scripts) in one zone to be executed with the permissions of a higher privileged zone.
- a web browser configuration error; unsafe sites listed in privileged zones.
- a cross-site scripting vulnerability within a privileged zone

A common attack scenario involves two steps. The first step is to use a Cross Zone Scripting vulnerability to get scripts executed within a privileged zone. To complete the attack, then perform malicious actions on the computer using insecure ActiveX components.

This type of vulnerability has been exploited to silently install various malware (such as spyware, remote control software, worms and such) onto computers browsing a malicious web page.

http://en.wikipedia.org/wiki/Cross_Zone_Scripting

2.360.3 (EN) CROSS-ZONE SCRIPTING

An attacker is able to cause a victim to load content into their web-browser that bypasses security zone controls and gain access to increased privileges to execute scripting code or other web objects such as unsigned ActiveX controls or applets. This is a privilege elevation attack targeted at zone-based web-browser security. In a zone-based model, pages belong to one of a set of zones corresponding to the level of privilege assigned to that page. Pages in an untrusted zone would have a lesser level of access to the system and/or be restricted in the types of executable content it was allowed to invoke. In a cross-zone scripting attack, a page that should be assigned to a less privileged zone is granted the privileges of a more trusted zone. This can be accomplished by exploiting bugs in the browser, exploiting incorrect configuration in the zone controls, through a cross-site scripting attack that causes the attacker's content to be treated as coming from a more trusted page, or by leveraging some piece of system functionality that is accessible from both the trusted and less trusted zone. This attack differs from "Restful Privilege Escalation" in that the latter correlates to the inadequate securing of RESTful access methods (such as HTTP DELETE) on the server, while cross-zone scripting attacks the concept of security zones as implemented by a browser.

Attack Pattern 104

http://capec.mitre.org/data/index.html

2.361 CRYPTOKI

Ver:

- *PKCS #11*
- *CAPI - Cryptographic Application Programming Interface*

2.361.1 CRYPTOKI

Una interfaz de programación para servicios criptográficos. Ver PKCS #11.

2.361.2 (EN) CRYPTOKI

(N) A CAPI defined in PKCS #11. Pronunciation: "CRYPTO-key". Derivation: Abbreviation of "cryptographic token interface". [RFC4949:2007]

2.362 CTR - CIFRADO MODO CON CONTADOR

Acrónimos: CTR

Ver:

- *Modo de operación (1)*
- [NIST-SP800-38A:2001]
- [FIPS-81:1980]
- *Criptografía de clave secreta*
- http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

2.362.1 CTR - CIFRADO MODO CON CONTADOR

Al igual que el modo OFB, el modo CTR transforma un algoritmo de cifrado por bloques en un algoritmo de cifrado de flujo. La máscara de cifrado se genera cifrando un contador. Además de las ventajas del modo OFB, permite un acceso aleatorio a la información.

2.362.2 (EN) COUNTER MODE (CTR)

(N) A block cipher mode that enhances ECB mode by ensuring that each encrypted block is different from every other block encrypted under the same key. [SP38A] (See: block cipher.) [RFC4949:2007]

2.362.3 (EN) CTR - COUNTER ENCRYPTION MODE

Like OFB, counter mode turns a block cipher into a stream cipher. It generates the next keystream block by encrypting successive values of a "counter". The counter can be any simple function which produces a sequence which is guaranteed not to repeat for a long time, although an actual counter is the simplest and most popular. CTR mode has similar characteristics to OFB, but also allows a random access property during decryption, and is believed to be as secure as the block cipher being used. Note that the nonce in this graph is the same thing as the initialization vector (IV) in the other graphs. The IV/nonce and the counter can be concatenated, added, or XORed together to produce the actual unique counter block for encryption.

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

2.363 CUADRO DE MANDO INTEGRAL

2.363.1 CUADRO DE MANDO INTEGRAL

El concepto de Cuadro de Mando Integral - CMI (Balanced Scorecard - BSC) fue presentado en el número de Enero/Febrero de 1992 de la revista Harvard Business Review, en base a un trabajo realizado para una empresa de semiconductores (La empresa en cuestión era Analog Devices Inc.).

Sus autores, Robert S. Kaplan y David P. Norton, plantean que el CMI es un sistema de administración o sistema administrativo (Management system), que va más allá de la perspectiva financiera con la que los gerentes acostumbran evaluar la marcha de una empresa.

Es un método para medir las actividades de una compañía en términos de su visión y estrategia. Proporciona a los administradores una mirada abarcativa de las prestaciones del negocio.

http://es.wikipedia.org/wiki/Cuadro_de_mando_integral

2.363.2 MARCADOR DE PUNTUACIÓN BALANCEADO

Un método para medir las actividades de una empresa en términos de su visión y estrategias, proporcionando una vista rápida e integral del desempeño del negocio a la gerencia. Es una herramienta administrativa cuyo fin es medir un negocio desde las siguientes perspectivas: financiera, del cliente, del negocio y del aprendizaje (Robert S. Kaplan y David Norton, 1992). [COBIT:2006]

2.363.3 (EN) BALANCED SCORECARD

A method for measuring an enterprise's activities in terms of its vision and strategies by giving managers a fast, comprehensive view of the performance of the business. It is a management tool that seeks to measure a business from the following perspectives: financial, customer, business and learning. (Robert S. Kaplan and David Norton, 1992). [COBIT:2006]

2.364 CUARENTENA

Ver:

- *Virus*

2.364.1 CUARENTENA

1. Aislamiento preventivo a que se somete durante un período de tiempo, por razones sanitarias, a personas o animales.

2. Suspensión del asenso a una noticia o hecho, por algún espacio de tiempo, para asegurarse de su certidumbre.

DRAE. Diccionario de la Lengua Española.

2.364.2 CUARENTENA

Dicho término originalmente, fue utilizado para determinar el aislamiento de un virus biológico o un ente infectado por él. Tiempo mas tarde, con la aparición de virus informáticos, algunos productos antivirus comenzaron a usar dicho término para indicar que un archivo infectado haba sido aislado del resto del sistema. Esto es útil cuando nuestro antivirus ha detectado con su heurística un posible virus aún no incluido en su base de datos. Por lo tanto, enviar un archivo en Cuarentena consiste en proteger nuestro equipo dejando aislado a uno o varios archivos infectados con el propósito de poder desinfectarlos en próximas actualizaciones de nuestro producto antivirus si fuese posible. Si las nuevas actualizaciones no nos han permitido repararlo ya sea porque el archivo es un virus en sí o porque el archivo original ha sido dañado, podremos optar por eliminar el archivo, restaurarlo a su ubicación original o bien continuar dejándolo aislado. También se puede llamar

así al área, generalmente una carpeta, donde se mueve un fichero infectado (o supuestamente infectado) por un virus para que no pueda causar daños.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.364.3 (EN) QUARANTINING

Storing files containing malware in isolation for future disinfection or examination. [NIST-SP800-83:2005]

2.364.4 (EN) QUARENTINE

a period of time when an animal or a person that has or may have a disease is kept away from others in order to prevent the disease from spreading

Oxford Advanced Learner's Dictionary.

2.364.5 (EN) QUARANTINE

A holding area to which suspicious or infected files are moved so that they are unavailable to the user, but not lost forever. This allows organizations to remove infected files from circulation without deleting them permanently.

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.364.6 (EN) QUARANTINING A COMPUTER

Quarantining a computer means isolating a computer into a special network until it has reached a certain security level. The computer is offered to install updates for anti-virus signature files or install software patches.

http://www.enisa.europa.eu/

2.364.7 (EN) QUARANTINE

To isolate files suspected to contain a virus, so that the files cannot be opened or executed. The Symantec AntiVirus Corporate Edition heuristically detects suspect files and virus-infected files that cannot be repaired with the current set of virus definitions. From the Quarantine on the local computer, quarantined files can be forwarded to a central network quarantine and submitted to Symantec Security Response for analysis. If a new virus is discovered, the updated virus definitions are automatically returned.

http://www.symantec.com/avcenter/refa.html

2.365 CUENTAS PREDETERMINADAS

2.365.1 CUENTAS PREDETERMINADAS

Cuenta de inicio de sesión que se encuentra predefinida en un sistema, aplicación o dispositivo que ermite obtener accesopor primera vez al momento en que el sistema comienza a funcionar. El sistema también puede generar cuentas predeterminadas adicionales como parte del proceso de instalación.

http://es.pcisecuritystandards.org/

2.365.2 (EN) DEFAULT ACCOUNTS

Login account predefined in a system, application, or device to permit initial access when system is first put into service. Additional default accounts may also be generated by the system as part of the installation process.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.365.3 (FR) COMPTE PAR DÉFAUT

Compte de connexion prédéfini dans un système, une application ou un dispositif, permettant l'accès au système lors de sa mise en service initiale.

Des comptes par défaut supplémentaires peuvent également être générés par le système dans le cadre du processus d'installation.

http://fr.pcisecuritystandards.org/

2.366 CUSTODIO

Ver:

- *Datos*
- *Propietario de la información*

2.366.1 ENCARGADO DEL TRATAMIENTO

la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2.366.2 RESPONSABLE DE SEGURIDAD

persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

2.366.3 (EN) CUSTODIAN

Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. The custodians of information resources, including entities providing outsourced information resources services to the university, must:

- Implement the controls specified by the owner(s).
- Provide physical and procedural safeguards for the information resources.
- Assist owners in evaluating the cost-effectiveness of controls and monitoring.

- Implement the monitoring techniques and procedures for detecting, reporting, and investigating incidents.

http://www.utexas.edu/its/policies/glossary.html

2.366.4 (EN) DATA CUSTODIAN

A Data Custodian is the entity currently using or manipulating the data, and therefore, temporarily taking responsibility for the data.

http://www.sans.org/security-resources/glossary-of-terms/

2.367 CVE

2.367.1 CVE

Common Vulnerabilities and Exposures, siglas CVE, es una lista de información registrada sobre conocidas vulnerabilidades de seguridad, donde cada referencia tiene un número de identificación único.1 De esta forma provee una nomenclatura común para el conocimiento público de este tipo de problemas y así facilitar la compartición de datos sobre dichas vulnerabilidades.

Fue definido y es mantenido por The MITRE Corporation (por eso a veces a la lista se la conoce por el nombre MITRE CVE List) con fondos de la National Cyber Security Division del gobierno de los Estados Unidos de América. Forma parte del llamado Security Content Automation Protocol.

La información y nomenclatura de esta lista es usada en la National Vulnerability Database, el repositorio de los Estados Unidos de América de información sobre vulnerabilidades.

https://es.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

2.367.2 (EN) CVE

The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures. MITRE Corporation maintains the system, with funding from the National Cyber Security Division of the United States Department of Homeland Security. CVE is used by the Security Content Automation Protocol, and CVE IDs are listed on MITRE's system as well as the US National Vulnerability Database.

https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

2.367.3 (FR) CVE

Common Vulnerabilities and Exposures ou CVE est un dictionnaire des informations publiques relatives aux vulnérabilités de sécurité. Le dictionnaire est maintenu par l'organisme MITRE, soutenu par le département de la Sécurité intérieure des États-Unis.

https://fr.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

2.368 CVSS

Acrónimos: CVSS

Ver:

- *Vulnerabilidad*

2.368.1 CVSS

Acrónimo de “Common Vulnerability Scoring System” (sistema de puntaje de vulnerabilidad común). Un estándar abierto y neutro de la industria para los proveedores cuya finalidad es transmitir la gravedad que presentan las vulnerabilidades en la seguridad de un sistema informático y ayudar a determinar tanto la urgencia como la prioridad de la respuesta. Para obtener más información, consulte la Guía del programa ASV

http://es.pcisecuritystandards.org

2.368.2 (EN) CVSS

Acronym for “Common Vulnerability Scoring System.” A vendor agnostic, industry open standard designed to convey the severity of computer system security vulnerabilities and help determine urgency and priority of response. Refer to ASV Program Guide for more information.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.368.3 (FR) CVSS

Acronyme de «Common Vulnerability Scoring System», système de notation de vulnérabilité courante. Une norme ouverte de l’industrie indépendante des fournisseurs conçue pour retranscrire la sévérité des vulnérabilités des systèmes de sécurité informatiques et pour aider à déterminer l’urgence et la priorité de la réponse. Consultez le Guide du programme ASV pour de plus amples informations.

http://fr.pcisecuritystandards.org/

2.369 CWIN

Acrónimos: CWIN

Ver:

- *Infraestructuras críticas de información (protección de)*

2.369.1 (EN) CWIN - CRITICAL INFRASTRUCTURE WARNING INFORMATION NETWORK

a backup communications system established for critical infrastructures in the event of a major crisis or national catastrophe if normal communications go down.

2.370 CYBERSLACKING

2.370.1 PERDER EL TIEMPO

Dícese de los empleados que en jornada laboral se dedican a navegar por Internet por motivos diferentes de sus obligaciones laborales.

2.370.2 (EN) CYBERSLACKING

Wasting time, usually at work, using the Internet.

http://www.getsafeonline.org/

2.370.3 (EN) CYBERSLACKING

Cyberslacking is the practice of employees using the Internet or other employer-provided resources for leisure during work hours, contributing to inefficiency.

http://en.wikipedia.org/wiki/Cyberslacking

2.371 DAÑO

Ver:

- *Vulnerabilidad*

2.371.1 DAÑAR

Dicho de un aparato, un objeto, etc.: estropearse (deteriorarse).

DRAE. Diccionario de la Lengua Española.

2.371.2 (EN) DAMAGE

physical harm caused to sth which makes it less attractive, useful or valuable

Oxford Advanced Learner's Dictionary.

2.371.3 (EN) POTENTIAL DAMAGE

A rating used to calculate a vulnerability, based on the relative damage incurred if a threat exploits a vulnerability. For example, if a threat can obtain root privileges by exploiting a vulnerability, the potential damage is rated high. If a vulnerability only lets the threat browse a portion of a file system, and this type of activity causes little or no damage to the network, the potential damage is rated low.

http://www.symantec.com/avcenter/refa.html

2.372 DATOS

Ver:

- *Información*
- *Custodio*
- *Propietario de la información*

2.372.1 DATOS

Información codificada de alguna manera para poder recuperar su significado.

2.372.2 (EN) DATA

A subset of information in an electronic format that allows it to be retrieved or transmitted. [CNSSI_4009:2010]

2.372.3 (EN) DATA

(I) Information in a specific representation, usually as a sequence of symbols that have meaning. [RFC4949:2007]

2.372.4 (EN) DATA / INFORMATION

In the area of Information Security, data (and the individual elements that comprise the data) is processed, formatted and re-presented, so that it gains meaning and thereby becomes information. Information Security is concerned with the protection and safeguard of that information which, in its various forms can be identified as Business Assets or Information Assets.

http://www.passwordnow.com/en/glossary/data--information.html

2.373 DATOS DE CARÁCTER PERSONAL

2.373.1 DATOS DE CARÁCTER PERSONAL

Cualquier información concerniente a personas físicas identificadas o identificables.

LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. (Vigente hasta el 14 de enero de 2000)

2.373.2 INFORMACIÓN DE IDENTIFICACIÓN PERSONAL

Información que se puede utilizar para identificar a una persona incluyendo, pero sin limitarse a, nombre, dirección, número del seguro social, número de teléfono, etc.

http://es.pcisecuritystandards.org/

2.373.3 PERSONA IDENTIFICABLE

Persona física cuyos datos de carácter personal establezcan de forma directa o indirecta un perfil más o menos detallado de su identidad personal, familiar o profesional, tal y como establece el artículo 3 a. de la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

http://www.inteco.es/glossary/Formacion/Glosario/

2.373.4 (EN) PERSONALLY IDENTIFIABLE INFORMATION:

Information that can be utilized to identify an individual including but not limited to name, address, social security number, phone number, etc.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.373.5 (EN) PERSONALLY IDENTIFIABLE INFORMATION (PII)

Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. [CNSSI_4009:2010]

2.373.6 (EN) PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

http://whatis.techtarget.com/

2.373.7 (FR) INFORMATIONS PERMETTANT UNE IDENTIFICATION PERSONNELLE

L'information qui peut être utilisée pour identifier ou retracer l'identité d'un individu, notamment le nom, l'adresse, le numéro de sécurité sociale, les données biométriques, la date de naissance, etc.

http://fr.pcisecuritystandards.org/

2.374 DATOS DE CREACIÓN DE FIRMA

Ver:

- *Firma electrónica*
- *Dispositivo de creación de firma*

2.374.1 DATOS DE CREACIÓN DE FIRMA

son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica. [Ley-59:2003]

2.374.2 (EN) SIGNATURE-CREATION DATA

means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.

[Directive-1999/93/EC:1999]

2.375 DATOS DE VALIDACIÓN

Ver:

- *Firma electrónica*
- *Datos de verificación de firma*

2.375.1 DATOS DE VALIDACIÓN

«datos de validación», los datos utilizados para validar una firma electrónica o un sello electrónico; [PE-CONS 60/14]

2.375.2 (EN) VALIDATION DATA

'validation data' means data that is used to validate an electronic signature or an electronic seal; [PE-CONS 60/14]

2.375.3 (FR) DONNÉES DE VALIDATION

"données de validation", des données qui servent à valider une signature électronique ou un cachet électronique; [PE-CONS 60/14]

2.376 DATOS DE VERIFICACIÓN DE FIRMA

Ver:

- *Firma electrónica*
- *Dispositivo de verificación de firma*
- *Datos de validación*

2.376.1 DATOS DE VERIFICACIÓN DE FIRMA

son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica. [Ley-59:2003]

2.376.2 (EN) SIGNATURE-VERIFICATION-DATA

means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;

[Directive-1999/93/EC:1999]

2.377 DE-ANONYMIZATION

Ver:

- *Anonymizer*

2.377.1 DESANONIMIZAR

Estrategia de minería de datos en la que los datos anónimos se cruzan con otras fuentes de datos para volver a identificar la fuente de los datos anónimos. Cualquier información que distingue una fuente de datos de otro se puede utilizar para desanonimizar.

2.377.2 (EN) DE-ANONYMIZATION (DEANONYMIZATION)

De-anonymization is a data mining strategy in which anonymous data is cross-referenced with other data sources to re-identify the anonymous data source. Any information that distinguishes one data source from another can be used for de-anonymization.

http://whatis.techtarget.com/

2.378 DECLARACIÓN DE APLICABILIDAD

Acrónimos: SoA

2.378.1 DECLARACIÓN DE APLICABILIDAD

Documento formal en el que, para un conjunto de salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido. [Magerit:2012]

2.379 DECLARACIÓN DE REQUISITOS DE SEGURIDAD

Acrónimos: DRS (es), DRSI (es), DRES (es)

2.379.1 DECLARACIÓN DE REQUISITOS DE SEGURIDAD

Es el documento base para la acreditación. Consiste en la exposición completa y detallada de los principios de seguridad que deben observarse y de los requisitos de seguridad que se han de implantar conforme al correspondiente análisis de riesgos realizado previamente. [CCN-STIC-202:2006] [CCN-STIC-204:2006]

2.379.2 DECLARACIÓN DE REQUISITOS DE SEGURIDAD DE LA INTERCONEXIÓN

Documento base para la acreditación de la interconexión de sistemas. Consiste en la exposición completa y detallada de los principios de seguridad que deben observarse en la interconexión, y de los requisitos de seguridad que se han de implantar conforme al correspondiente análisis de riesgos realizado previamente. [CCN-STIC-302:2012]

2.380 DECLARACIÓN DE SEGURIDAD

Acrónimos: ST

Ver:

- *Criterios comunes*

2.380.1 DECLARACIÓN DE SEGURIDAD

Conjunto de requisitos de seguridad y especificaciones utilizados como base de la evaluación de un TOE identificado.

TOE - Target of Evaluation

[CC:2006]

2.380.2 (EN) SECURITY TARGET (ST)

an implementation-dependent statement of security needs for a specific identified TOE.

TOE - Target of Evaluation

[CC:2006]

2.381 DECLARANTE DE PRIVILEGIOS

Ver:

- *Privilegio*

2.381.1 ASERTOR DE PRIVILEGIOS

Titular de un privilegio que utiliza su certificado de atributo o su certificado de clave pública para aseverar un privilegio. [X.509:2005]

2.381.2 (EN) PRIVILEGE ASSERTER

A privilege holder using their attribute certificate or public-key certificate to assert privilege. [X.509:2005]

2.381.3 (FR) DÉCLARANT DE PRIVILÈGE

détenteur de privilège utilisant son certificat d'attribut de clé publique pour déclarer un privilège. [X.509:2005]

2.382 DECRIPCIÓN

Ver:

- *Descifrado*

2.382.1 DECRIPCIÓN

Véase descrifrado. [ISO-7498-2:1989]

2.382.2 (EN) DECRYPTION

The process of changing ciphertext into plaintext using a cryptographic algorithm and key. [NIST-SP800-57:2007]

2.382.3 (EN) DECRYPTION

reversal of a corresponding encipherment [ISO/IEC ISO-11770-1:1996]. [ISO-18033-1:2005]

2.383 DECRYPT

Ver:

- *Descodificar*
- *Descifrar*

2.383.1 (EN) DECRYPT

(I) Cryptographically restore cipher text to the plaintext form it had before encryption. [RFC4949:2007]

2.383.2 (EN) DECRYPT

Generic term encompassing decode and decipher. [CNSSI_4009:2010]

2.383.3 (FR) DÉCRYPTER

Action consistant à retrouver un ensemble de données en clair à partir d'un message chiffré, sans connaître le code secret de chiffrement.

http://securit.free.fr/glossaire.htm

2.384 DEFACEMENT

2.384.1 DESFIGURAR

Ataque sobre un servidor web como consecuencia del cual se cambia su apariencia. El cambio de imagen puede ser a beneficio del atacante, o por mera propaganda (a beneficio del atacante o para causar una situación embarazosa al propietario de las páginas).

2.384.2 (EN) DEFACEMENT

Defacement is the method of modifying the content of a website in such a way that it becomes "vandalized" or embarrassing to the website owner.

http://www.sans.org/security-resources/glossary-of-terms/

2.384.3 (FR) DEFACEMENT

Action illicite ayant pour but de défigurer un site web. La page d'accueil des sites Internet est la cible de prédilection des pirates pour des raisons de visibilité du defacement. Le but pour le pirate est de prouver la pénétration du site Internet de la victime. Les motivations diffèrent quant à ces actions illégales.

http://www.cases.public.lu/functions/glossaire/

2.385 DEFECTO (EN PROGRAMAS)

Ver:

- *Bug*
- *Flaw*

2.385.1 DEFECTO (EN PROGRAMAS)

Vulnerabilidad en el diseño o en la implementación. Un defecto puede no ser detectado durante años y de repente aparecer en un sistema en producción con graves consecuencias.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/risk/248-BSI.html

2.385.2 (EN) DEFECT (SOFTWARE)

An implementation or design vulnerability. A defect may lie dormant in software for years and then surface in a fielded system with major consequences.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/risk/248-BSI.html

2.386 DEFENSA EN PROFUNDIDAD

Ver:

- http://en.wikipedia.org/wiki/Defence_in_depth

2.386.1 DEFENSA EN PROFUNDIDAD

Estrategia de protección consistente en introducir múltiples capas de seguridad que permitan reducir la probabilidad de compromiso en caso de que una de las capas falle y en el peor de los casos minimizar el impacto. [CCN-STIC-400:2006]

2.386.2 (EN) DEFENSE IN DEPTH

The practice of layering defenses to provide added protection

Defense in depth increases security by raising the effort needed in an attack. This strategy places multiple barriers between an attacker and an enterprise's computing and information resources.barriers between an attacker and an enterprise’s computing and information resources.

ISACA, Cybersecurity Glossary, 2014

2.386.3 (EN) DEFENSE-IN-DEPTH

Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. [NIST-SP800-53:2013]

2.386.4 (EN) DEFENSE-IN-DEPTH

Information Security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. [CNSSI_4009:2010]

2.386.5 (EN) DEFENSE-IN-BREADTH

A planned, systematic set of multi-disciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component lifecycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement). [CNSSI_4009:2010]

2.386.6 (EN) DEFENSE IN DEPTH

(N) "The siting of mutually supporting defense positions designed to absorb and progressively weaken attack, prevent initial observations of the whole position by the enemy, and [enable] the commander to maneuver the reserve." [JP1] [RFC4949:2007]

2.386.7 (EN) DEFENSE IN-DEPTH

Defense In-Depth is the approach of using multiple layers of security to guard against failure of a single security component.

http://www.sans.org/security-resources/glossary-of-terms/

2.386.8 (EN) DEFENSE IN DEPTH

Defense in depth is the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier.

http://searchsecurity.techtarget.com/

2.387 DELEGACIÓN

Ver:

- *Cadena de delegación*

2.387.1 DELEGAR

Dicho de una persona: Dar la jurisdicción que tiene por su dignidad u oficio a otra, para que haga sus veces o para conferirle su representación.

DRAE. Diccionario de la Lengua Española.

2.387.2 DELEGACIÓN

Envío de un privilegio desde una entidad que tiene dicho privilegio a otra entidad. [X.509:2005]

2.387.3 (EN) DELEGATION

Conveyance of privilege from one entity that holds such privilege, to another entity. [X.509:2005]

2.387.4 (FR) DÉLÉGATION

transfert d'un privilège d'une entité détentrice vers une autre entité. [X.509:2005]

2.388 DENEGACIÓN DE SERVICIO

Acrónimos: DoS

Ver:

- *Denegación de servicio distribuida*
- http://www.cert.org/advisories/CA-99-17-denial-of-service-tools.html
- *Inundación*
- *Extorsión en la red*

2.388.1 DENEGACIÓN DE SERVICIO

Se entiende como denegación de servicio, en términos de seguridad informática, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo.

Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma no permitir que sus legítimos usuarios puedan utilizar los servicios por prestados por él.

El ataque consiste en, saturar con peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso.

Un método mas sofisticado es el Ataque de Denegación de Servicio Distribuido (DDoS), mediante el cual las peticiones son enviadas, de forma coordinada entre varios equipos, que pueden estar siendo utilizados para este fin sin el conocimiento de sus legitimos dueños.

Esto puede ser así mediante el uso de programas malware que permitan la toma de control del equipo de forma remota, como puede ser en los casos de ciertos tipos de gusano o bien porque el atacante se ha encargado de entrar directamente en el equipo de la victima.

http://www.inteco.es/glossary/Formacion/Glosario/

2.388.2 DENEGACIÓN DE SERVICIO

Rechazo de un acceso autorizado a los recursos del sistema o demora en las operaciones críticas en el tiempo. (ISO-7498-2) [Ribagorda:1997]

2.388.3 DENEGACIÓN DE SERVICIO

Acción de impedir el acceso, estando autorizado, a recursos o retrasar las operaciones. [CESID:1997]

2.388.4 NEGACIÓN (O DENEGACIÓN) DE SERVICIO

Prevención de acceso autorizado a recursos o retardo deliberado de operaciones críticas desde el punto de vista del tiempo. [ISO-7498-2:1989]

2.388.5 (EN) DENIAL OF SERVICE (DOS):

The non-availability ofcomputer resources to the intended or usual customers of a computer service, normally as a result of a cyber operation.

The Tallinn Manual, 2013

2.388.6 (EN) DENIAL OF SERVICE

A denial-of-service attack (DoS) is an attempt to make a resource unavailable to its users. A distributed denial-of-service attack (DDoS) occurs when multiple attackers launch simultaneous DoS attacks against a single target. In DDoS attacks, attackers use as much firepower as possible (usually through compromised computer systems/botnets) in order to make the attack difficult to defend. The perpetrators of DoS attacks usually either target high profile websites/services or use these attacks as part of bigger ones in order achieve their malicious goals. As stated, despite the fact that these kinds of attacks do not target directly the confidentiality or integrity of the information resources of a target, they can result in significant financial and reputation loss.

ENISA Threat Landscape [Deliverable – 2012-09-28]

2.388.7 (EN) DENIAL OF SERVICE (DOS) ATTACK

Denial of service (DOS) attacks are attempts to render a computer system unavailable to users through a variety of means. These may include saturating the target computers or networks with external communication requests, thereby hindering service to legitimate users. Distributed denial of service (DDOS) attacks are denial of service attacks executed by many computers at the same time. There are currently a number of common ways by which DOS and DDOS attacks may be conducted. They include, for example, sending malformed queries to a computer system; exceeding the capacity limit for users; and sending more e-mails to e-mail servers than the system can receive and handle.

Budapest Convention on Cybercrime

2.388.1 (EN) DENIAL OF SERVICE

The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.). [CNSSI_4009:2010]

2.388.2 (EN) DENIAL OF SERVICE

(I) The prevention of authorized access to a system resource or the delaying of system operations and functions. (See: availability, critical, flooding.) [RFC4949:2007]

2.388.3 (EN) DENIAL OF SERVICE

the prevention of authorized access to a system resource or the delaying of system operations and functions. [ISO-18028-1:2006]

2.388.4 (EN) DENIAL OF SERVICE - DOS

an attack against a system to deter its availability. [ISO-18028-4:2005]

2.388.5 (EN) DENIAL OF SERVICE (DOS)

An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. [NIST-SP800-61:2004]

2.388.6 (EN) DENIAL OF SERVICE

The prevention of authorized access to resources or the delaying of timecritical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.) [NIST-SP800-27:2004]

2.388.7 (EN) DENIAL OF SERVICE

The prevention of authorized access to resources or the delaying of time-critical operations. [NIST-SP800-33:2001]

2.388.8 (EN) DENIAL OF SERVICE

Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service. [IRM-5239-8:1995]

2.388.9 (EN) DENIAL OF SERVICE

The prevention of authorized access to resources or the delaying of time-critical operations. [ISO-7498-2:1989]

2.388.10 (EN) DENIAL OF SERVICE (DOS)

Overwhelming a host with spurious data in order to cause legitimate connection attempts to fail. DoS attacks do not reveal sensitive data to the attacker, however they can cause untold damage to reputation as well as a lost business. According to the March 2000 Computer Crime and Security Survey of the FBI's Computer Institute, 60% of detection of Denial of Service attacks.

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.388.11 (EN) DENIAL OF SERVICE

The prevention of authorized access to a system resource or the delaying of system operations and functions.

http://www.sans.org/security-resources/glossary-of-terms/

2.388.12 (EN) DENIAL OF SERVICE PROTECTION

An IT defense strategy implemented to provide a business network with security against denial of service (DoS) attacks, which harm the network by flooding it with additional requests, ultimately slowing or completely interrupting traffic.

Denial of service protection offers businesses a way to guard against the threat of DoS attacks that hinder the functionality of a network by disrupting the availability of network resources. When a network falls under a DoS attack and is flooded with malicious traffic, network service could be interrupted for long periods of time, making business-critical information unavailable. Along with guarding against standard DoS attacks, businesses should also provide their networks with Distributed Denial of Service (DDoS) Protection. DDoS employs a host of compromised computers to launch a large-scale attack on company networks. For common victims of DoS attacks, such as online businesses, service providers and service carriers, damages from DoS attacks can be felt as loss of revenue through network downtime, and tainted business reputations. For these reasons in particular it is important that companies have proper denial of service protection implemented as part of their network security measures.

http://www.radware.com/Resources/Glossary/denial_of_service_protection.aspx

2.388.13 (FR) DÉNI DE SERVICE

Impossibilité d'accès à des ressources pour des utilisateurs autorisés ou introduction d'un retard pour le traitement d'opérations critiques. [ISO-7498-2:1989]

2.388.14 (FR) DÉNI DE SERVICE (DOS)

Méthode de piratage réseau qui consiste à provoquer un refus d'accès à un service en ligne pour tout utilisateur souhaitant se connecter. La conséquence de cet acte réside dans une atteinte à la disponibilité de la cible.

http://www.cases.public.lu/functions/glossaire/

2.388.15 (FR) REFUS DE SERVICE OU DENI DE SERVICE

Type d´attaque, utilisé sur un réseau comme Internet, visant à empêcher le bon fonctionnement d´un service sans en altérer son contenu. Par exemple, le résultat peut-être l´inaccessiblité pendant plusieurs heures d´un site Internet. Plusieurs moyens sont utilisés afin d´y parvenir: saturation des ressources du serveur, saturation de la bande passante...

http://www.indexel.net/1_6_1990__3_/7/27/1/Petit_Glossaire_de_la_securite_informatique.htm

2.388.16 (FR) DÉNI DE SERVICE

Attaque consistant à saturer une ressource en effectuant de manière malveillante des demandes de réservation excessives ou en occupant le service illicitement. Parmi les attaques de déni de service les plus connues: SYN flooding, UDP flooding, ping of death, LAND attack, SMURF attack, mail bombing...

http://securit.free.fr/glossaire.htm

2.389 DENEGACIÓN DE SERVICIO DISTRIBUIDA

Acrónimos: DDoS

Ver:

- *Denegación de servicio*
- http://en.wikipedia.org/wiki/Denial-of-service_attack
- http://xforce.iss.net/alerts/advise40.php
- *Botnet*

2.389.1 DENEGACIÓN DE SERVICIO DISTRIBUIDA

Ataque de denegación de servicio que se realiza utilizando múltiples puntos de ataque simultánea-mente.

2.389.2 DENEGACIÓN DE SERVICIO DISTRIBUIDA

Ataque DoS en el que participan gran cantidad de máquinas atacantes. [CCN-STIC-612:2006]

2.389.3 (EN) DISTRIBUTED DENIAL OF SERVICE (DDOS):

A technique that employs two or more computers, such as the bots of a botnet, to achieve a denial of service from a single or multiple targets.

The Tallinn Manual, 2013

2.389.4 (EN) DISTRIBUTED DENIAL OF SERVICE (DDOS)

Denial of Service technique that uses numerous hosts to perform the attack.

[CNSSI_4009:2010]

2.389.5 (EN) DISTRIBUTED DENIAL OF SERVICE (DDOS)

A DoS technique that uses numerous hosts to perform the attack.

[NIST-SP800-61:2004]

2.389.6 (EN) DISTRIBUTED DENIAL OF SERVICE

When more than one system is used to attack resources of a single server to create a denial of service attack.

2.389.7 (EN) DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK

A DoS attack launched against a site from multiple sources. Generally the attacker places client software on a number of unsuspecting remote computers, then later uses these computers to launch an attack. A DDoS attack is more effective than a simple DoS attack and is more difficult to prevent.

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.389.8 (EN) DISTRIBUTED DENIAL OF SERVICE

On the Internet, a distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

http://searchsoftwarequality.techtarget.com/glossary/

2.389.9 (EN) DDOS - DISTRIBUTED DENIAL OF SERVICE

Attack is a means for attackers, using multiple attack points or multiple attackers, to attempt to shut down a given website or online activity with massive and overwhelming numbers of requests to the server that hosts the site or activity; this attack method is often used by cyber criminals for online extortion.

2.389.10 (FR) DDOS (DISTRIBUTED DENIAL OF SERVICES)

Denial of Service de type distribué, c'est-à-dire en provenance de multiples sources permettant ainsi d'accroître l'efficacité de l'attaque et les dégâts causés à la cible.

http://www.cases.public.lu/functions/glossaire/

2.389.11 (FR) DÉNI DE SERVICE DISTRIBUÉ

Le déni de service distribué (DDOS, Distributed Denial of Service) est une forme particulière de déni de service, simple et efficace, particulièrement répandue.

Un déni de service distribué consiste en l'utilisation synchronisée de plusieurs machines, en général des victimes de chevaux de Troie qui, a leur insu, déclenchent une attaque par déni de service sur une cible particulière.

Les outils classiquement utilisés pour générer des dénis de service distribués sont:

- TFN/TFN2K (Tribe Flood Network) permettant de générer des attaques de type ICMP echo, SYN flooding et SMURF attack.
- TrinOO génère des attaques distribuées de type UDP flooding.

Ce type d'attaque a notamment été utilisé par le hacker canadien MafiaBoy contre les sites de CNN, Yahoo...

http://securit.free.fr/glossaire.htm

2.390 DEPÓSITO DE CLAVES

Ver:

- *Recuperación de claves*
- *Clave*
- *Clave criptográfica*

2.390.1 DEPÓSITO DE CLAVES

Sistema de gestión de claves en el que una clave o partes de la misma se distribuyen entre una o varias terceras partes confiables o agentes de depósito. Posteriormente será posible que, personal autorizado y siguiendo un determinado procedimiento, obtenga, a partir de la clave depositada, la clave de cifrado empleada en una comunicación. [CESID:1997]

2.390.2 (EN) KEY ESCROW

1. The processes of managing (e.g., generating, storing, transferring, auditing) the two components of a cryptographic key by two key component holders.

2. A key recovery technique for storing knowledge of a cryptographic key, or parts thereof, in the custody of one or more third parties called "escrow agents," so that the key can be recovered and used in specified circumstances.

[CNSSI_4009:2010]

2.390.3 (EN) KEY ESCROW SYSTEM

A system that entrusts the two components comprising a cryptographic key (e.g., a device unique key) to two key component holders (also called “escrow agents”). [CNSSI_4009:2010]

2.390.4 (EN) KEY ESCROW

(N) A key recovery technique for storing knowledge of a cryptographic key or parts thereof in the custody of one or more third parties called "escrow agents", so that the key can be recovered and used in specified circumstances. (Compare: key encapsulation.) [RFC4949:2007]

2.391 DER - DISTINGUISHED ENCODING RULES

Acrónimos: DER

Ver:

- *ASN.1 - Abstract Syntax Notation One*
- *BER - Basic Encoding Rules*
- *CER - Canonical Encoding Rules*
- *PER - Packet Encoding Rules*
- *XER - XML Encoding Rules*

2.392 DER - DISTINGUISHED ENCODING RULES

Conjunto de reglas para formatear en binario datos descritos en ASN.1.

2.392.1 (EN) DER - DISTINGUISHED ENCODING RULES

a set of ASN.1 encoding rules for formatting data in binary.

http://en.wikipedia.org/wiki/Distinguished_Encoding_Rules

2.392.2 (EN) DISTINGUISHED ENCODING RULES

encoding rules that may be applied to values of types defined using the ASN.1 notation

NOTE. Application of these encoding rules produces a transfer syntax for such values. It is implicit that the same rules are also to be used for decoding. The DER is more suitable if the encoded value is small enough to fit into the available memory and there is a need to rapidly skip over some nested values. [ISO-8825-1:2002]

2.393 DERECHO DE ACCESO

Ver:

- *Control de acceso*
- *Privilegios de acceso*

2.393.1 DERECHOS DE ACCESO

Privilegios de acceso de sujeto a un objeto. Por ejemplo, los derechos pueden ser: escritura, lectura, ejecución, borrado, etc. [Ribagorda:1997]

2.393.2 (EN) ACCESS RIGHT

Capability of a user on an object: to read, write, execute, remove,

2.394 DERIVACIÓN DE UNA CLAVE A PARTIR DE OTRA

Acrónimos: KDF

Ver:

- *Clave*

- *Clave criptográfica*

2.394.1 DERIVACIÓN DE UNA CLAVE A PARTIR DE OTRA

Proceso por el que se genera una clave a partir de cierta información secreta y, opcionalmente, alguna información adicional.

2.394.2 (EN) KEY DERIVATION

A function in the lifecycle of keying material; the process by which one or more keys are derived from a shared secret and other information. [NIST-SP800-57:2007]

2.394.3 (EN) KEY DERIVATION FUNCTION

a function that maps octet strings of any length to octet strings of an arbitrary, specified length, such that it is computationally infeasible to find correlations between inputs and outputs, and such that given one part of the output, but not the input, it is computationally infeasible to predict any bit of the remaining output. The precise security requirements depend on the application. [ISO-18033-2:2006]

2.394.4 (EN) KEY DERIVATION FUNCTION

a key derivation function outputs one or more shared secrets, used as keys, given shared secrets and other mutually known parameters as input. [ISO-15946-3:2002]

2.395 DERRAME

2.395.1 DERRAME

Incidente de seguridad consistente en que información clasificada se vierte en un sistemas que no está autorizado para hospedarla.

2.395.2 (EN) SPILLAGE

Security incident that results in the transfer of classified or CUI information onto an information system not accredited (i.e., authorized) for the appropriate security level. [CNSSI_4009:2010]

2.396 DESASTRE

Ver:

- *Continuidad*

2.396.1 CATÁSTROFE

1. Suceso que produce gran destrucción o daño.

2. Cambio brusco de estado de un sistema dinámico, provocado por una mínima alteración de uno de sus parámetros.

DRAE. Diccionario de la Lengua Española.

2.396.2 CATÁSTROFE

Suceso que produce gran destrucción o daño.

DRAE. Diccionario de la Lengua Española.

2.396.3 (EN) DISASTER

1. A sudden, unplanned calamitous event causing great damage or loss. Any event that creates an inability on an enterprise's part to provide critical business functions for some predetermined period of time. Similar terms are business interruption, outage and catastrophe.
2. The period when enterprise management decides to divert from normal production responses and exercises its disaster recovery plan (DRP). It typically signifies the beginning of a move from a primary location to an alternate location.

ISACA, Cybersecurity Glossary, 2014

2.396.4 (EN) DISASTER

1. An unexpected event, such as a very bad accident, a flood or a fire, that kills a lot of people or causes a lot of damage

2. a very bad situation that causes problems

3. (informal) a complete failure

Oxford Advanced Learner's Dictionary.

2.396.5 (EN) DISASTER

An event, accidental or intentional, that interrupts normal operations for a period long enough to have a significative impact of services or business processes.

2.397 DESASTRE NATURAL

2.397.1 DESASTRE NATURAL

Ataque accidental a los sistemas de información cuyo origen es la propia naturaleza: fuego, inundaciones, terremotos, tormentas, viento, etc.

2.397.2 (EN) NATURAL DISASTER

Any "act of God" (e.g., fire, flood, earthquake, lightning, or wind) that disables a system component.

2.398 DESBORDAMIENTO DE MEMORIA

2.398.1 DESBORDAMIENTO DE BUFFER

Estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y en el que un programa desborda el límite del buffer y escribe datos en el espacio de memoria adyacente. Los

desbordamientos de buffer son aprovechados por los atacantes para obtener acceso no autorizado a los sistemas o datos.

http://es.pcisecuritystandards.org

2.398.2 DESBORDAMIENTO DE BÚFER

En relación con la programación y seguridad informática, es un tipo de vulnerabilidad que afecta al software y es muy utilizada para realizar ataques dirigidos a conseguir que el programa realice las acciones que el atacante, y no el propio programa, quiera. Son defectos en la programación que provocan un error o el cuelgue del sistema pero son provocados de forma intencionada.

Si hiciéramos una comparación, el desbordamiento de búfer provoca algo similar a lo que ocurre cuando llenamos un vaso mas allá de su capacidad: éste se desborda y el contenido se derrama. Cuando el programador no incluye las medidas necesarias para comprobar el tamaño del búfer en relación con el volumen de datos que tiene que alojar, se produce también el derramamiento de estos datos que se sobrescriben en otros puntos de la memoria, lo cual puede hacer que el programa de errores o incluso se cuelgue.

El atacante calcula qué cantidad de datos necesita enviar para conseguir saber cuándo se producirá el desbordamiento y dónde se reescribirán los datos y posteriormente consigue el desbordamiento, en definitiva, que el programa ejecute el código que él ha enviado.

Este tipo de vulnerabilidad, dado que se produce por un defecto en el código del programa, sólo puede ser solventada mediante las actualizaciones o parches del programa en cuestión, lo cual hace muy necesario mantener actualizados todos los programas instalados en nuestro equipo.

http://www.inteco.es/glossary/Formacion/Glosario/

2.398.3 DESBORDAMIENTO DE MEMORIA

Se dice que un buffer se desborda cuando, de forma incontrolada, al intentar meter en él más datos de los que caben el exceso se vierte en otras zonas del sistema causando daños y perjuicios. A veces se trata de un mero accidente con consecuencias desagradables. A veces se trata de un ataque planificado que habilita alguna ventaja para el atacante.

Los desbordamientos de memoria pueden considerarse defectos de programación. Algunos lenguajes impiden con más o menos éxito que los desbordamientos puedan ocurrir; en otros lenguajes se requiere una precaución explícita por parte del programador que acaba siendo el último responsable de que el sistema sea o no vulnerable a este tipo de incidentes.

(en) buffer overflow

A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system . [CNSSI_4009:2010]

2.398.4 (EN) BUFFER OVERFLOW

(I) Any attack technique that exploits a vulnerability resulting from computer software or hardware that does not check for exceeding the bounds of a storage area when data is written into a sequence of storage locations beginning in that area. [RFC4949:2007]

2.398.5 (EN) BUFFER OVERFLOW

The result of a programming flaw. Some computer programs expect input from the user (for example, a Web page form might accept phone numbers from prospective customers). The program allows some virtual memory for accepting the expected input. If the programmer did not write his program to discard extra input (e.g., if instead of a phone number, someone submitted one thousand characters), the input can overflow the amount of memory allocated for it, and break into the portion of memory where code is executed. A skillful hacker can exploit this flaw to make someone's computer execute the hacker's code. Used interchangeably with the term, "buffer overrun."

http://www.watchguard.com/glossary/

2.398.6 (EN) BUFFER OVERRUN

Attack where a hacker exploits an unchecked buffer in a program to overwrite the program code. If the hacker overwrites the program code with new executables code, the hacker can change the program's operation. If the hacker enters other data, it usually causes the program to crash.

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.398.7 (EN) BUFFER OVERFLOW

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.

2.398.8 (EN) BUFFER OVERRUN

A condition that results from adding more information to a buffer than it was designed to hold. An attacker may exploit this vulnerability to take over a system.

http://www.getsafeonline.org/

2.398.9 (EN) BUFFER OVERFLOW

An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer Overflows are a common cause of malfunctioning software. If the data written into a buffer exceeds its size, adjacent memory space will be corrupted and normally produce a fault. An attacker may be able to utilize a buffer overflow situation to alter an application's process flow. Overfilling the buffer and rewriting memory-stack pointers could be used to execute arbitrary operating-system commands.

http://www.webappsec.org/projects/glossary/

2.398.10 (EN) BUFFER OVERFLOW

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through

programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

http://searchsoftwarequality.techtarget.com/glossary/

2.398.11 (EN) BUFFER OVERFLOW

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.

http://www.sans.org/security-resources/glossary-of-terms/

2.398.12 (EN) OVERFLOW BUFFERS

Buffer Overflow attacks target improper or missing bounds checking on buffer operations, typically triggered by input injected by an attacker. As a consequence, an attacker is able to write past the boundaries of allocated buffer regions in memory, causing a program crash or potentially redirection of execution as per the attacker's choice.

Attack Execution Flow

- The attacker identifies a buffer to target. Buffer regions are either allotted on the stack or the heap, and the exact nature of attack would vary depending on the location of the buffer
- Next, the attacker identifies an injection vector to deliver the excessive content to the targeted buffer.
- The attacker crafts the content to be injected. If the intent is to simply cause the software to crash, the content need only consist of an excessive quantity of random data. If the intent is to leverage the overflow for execution of arbitrary code, the attacker will craft a set of content that not only overflows the targeted buffer but does so in such a way that the overwritten return address is replaced with one of the attacker's choosing which points to code injected by the attacker.
- The attacker injects the content into the targeted software.
- Upon successful exploitation, the system either crashes or control of the program is returned to a location of the attacker's choice. This can result in execution of arbitrary code or escalated privileges, depending upon the exploited target.

Attack Pattern 100

http://capec.mitre.org/data/index.html

2.398.13 (FR) SATURATION DE LA MEMOIRE TAMPON

Une vulnérabilité qui est créée par des méthodes de codage non sécurisées, lorsqu'un programme sature la limite de la mémoire tampon et inscrit des données dans un espace de mémoire adjacent.

Les saturations de mémoire tampon sont utilisées par les pirates pour obtenir un accès non autorisé aux systèmes ou aux données.

http://fr.pcisecuritystandards.org/

2.398.14 (FR) DÉBORDEMENT DE TAMPON

Faille d'un système provoquée par l'envoi à un buffer de plus d'informations qu'il ne peut en contenir. Ceci permet, dans certains cas des comportements non prévus pas les développeurs du programme vulnérable pouvant conduire à l'obtention de droits et privilèges particuliers sur la machine qui héberge l'application vulnérable.

http://www.cases.public.lu/functions/glossaire/

2.398.15 (FR) DÉBORDEMENT DE PILE

Est une attaque classique consistant à exploiter la mauvaise gestion de la pile mémoire (réservation et relâche des espaces mémoires) dans un programme.

La personne malveillante envoie délibérément trop d'informations dans un champs ou une variable spécifique, entraînant un dépassement de la zone mémoire allouée à cette variable. La personne malveillante peut alors obtenir des droits d'accès élevés (ex.: root) ou disposer du code exécutable malicieux dans la zone de mémoire débordée.

http://securit.free.fr/glossaire.htm

2.399 DESCIFRADO

Ver:

- *Decripción*
- *Descifrar*

2.399.1 DESCIFRADO

1. Operación inversa de un cifrado reversible (ISO-7498-2)

2. Proceso ejecutado mediante técnicas criptográficas por el que se obtiene un texto en claro a partir del correspondiente texto cifrado.

[Ribagorda:1997]

2.399.2 DESCIFRADO

Operación inversa de un cifrado reversible correspondiente. [ISO-7498-2:1989]

2.399.3 (EN) DECIPHERMENT

(D) Synonym for "decryption". [RFC4949:2007]

2.399.4 (EN) DECIPHERMENT

alternative term for decryption. [ISO-18033-1:2005]

2.399.5 (EN) DECIPHERMENT (DECRYPTION)

Decipherment (decryption) is the reverse operation by which ciphertext is transformed to plaintext. [H.235:2005]

2.399.6 (EN) DECIPHERMENT

The reversal of a corresponding encipherment. [ISO-11770-1:1996]

2.399.7 (EN) DECIPHERMENT OR DECRYPTION

The reversal of a corresponding reversible encipherment. [ISO-7498-2:1989]

2.399.8 (FR) DÉCHIFFREMENT

Opération inverse d'un chiffrement réversible. [ISO-7498-2:1989]

2.400 DESCIFRAR

Ver:

- *Decripción*

2.400.1 DESCIFRAR

Declarar lo que está escrito en cifra o en caracteres desconocidos, sirviéndose de clave dispuesta para ello, o sin clave, por conjeturas y reglas críticas.

DRAE. Diccionario de la Lengua Española.

2.400.2 DESCIFRAR

Transformar un texto cifrado en el claro equivalente conociendo el procedimiento y clave de descifrado. Incluye la transformación de los textos cifrados mediante un código secreto. [CE-SID:1997]

2.400.1 (EN) DECIPHER

Convert enciphered text to plain text by means of a cryptographic system. [CNSSI_4009:2010]

2.400.2 (EN) DECIPHER

(D) Synonym for "decrypt". [RFC4949:2007]

2.400.3 (EN) DECIPHER

To change a secret encoded message back to the real text so you can read it.

Pssst! The words decode or decrypt mean the same thing as decipher!

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.401 DESCLASIFICACIÓN

Ver:

- *Información clasificada*
- *Desclasificar*

2.401.1 DESCLASIFICACIÓN

Proceso por el que una información es desclasificada de forma controlada.

2.401.2 (EN) DECLASSIFICATION

(I) An authorized process by which information is declassified. (Compare: classification.) [RFC4949:2007]

2.401.3 (EN) DECLASSIFICATION.

The determination that classified information no longer requires, in the interest of national security, any degree of protection against unau-thorized disclosure, together with removal or cancellation of the classification designation. [DoD 5220:2006]

2.402 DESCLASIFICAR

Ver:

- *Información clasificada*
- *Rebajar el nivel*

2.402.1 DESCLASIFICAR

Eliminar de forma autorizada la característica de "clasificada" de una cierta información.

2.402.2 (EN) DECLASSIFY

(I) To officially remove the security level designation of a classified information item or information type, such that the information is no longer classified (i.e., becomes unclassified). (See: classified, classify, security level. Compare: downgrade.) [RFC4949:2007]

2.403 DESCODIFICAR

Ver:

- *Código*
- *Codificar*

2.403.1 DESCODIFICAR

Aplicar inversamente las reglas de su código a un mensaje codificado para obtener la forma primitiva de este.

DRAE. Diccionario de la Lengua Española.

2.403.2 DESCODIFICAR

Operación inversa de la codificación. Recupera la información codificada.

2.403.3 (EN) DECODE

Convert encoded text to plain text by means of a code. [CNSSI_4009:2010]

2.404 DESCRIPTAR

Ver:

- *Decripción*

2.404.1 DESCRIPTAR

Anglicismo, de uso frecuente, con el que se designa las transformaciones de descifrado de un texto sin el conocimiento de la correspondiente clave. Es por tanto la tarea propia del criptoanalista. [Ribagorda:1997]

2.404.2 DESCRIPTAR

Resultado positivo del proceso de criptoanálisis. [CESID:1997]

2.405 DES - DATA ENCRYPTION STANDARD

Acrónimos: DES, DEA

Ver:

- *Cifrado en bloque*
- *Criptografía de clave secreta*
- [FIPS-43-3:1999]
- *Triple DES*

2.405.1 DES - DATA ENCRYPTION STANDARD

Algoritmo de cifra basado en un secreto compartido (clave). Cifra el texto en bloques de 64 bits. Utiliza claves de 56 bits.

2.405.2 DES

Algoritmo normalizado por EE UU para el cifrado de informaciones sensibles no clasificadas. Su nombre se corresponde con las siglas de Data Encryption Standard. Es un cifrado simétrico de bloque, que cifra bloques de texto en claro de 64 bits. La clave es de 64 bits (en realidad 56 bits, pues 8 de los anteriores son de paridad) y utiliza permutaciones, operaciones o-exclusivo y sustituciones. Una de éstas, expresada en la caja S, es no lineal y a ella debe el DES su fortaleza.

El DES está también normalizado por ISO (ISO 8731-1) para su uso como función resumen en el sector bancario con el nombre de Data Encryption Algorithm, usualmente conocido como DEA.

[Ribagorda:1997]

2.405.1 (EN) DATA ENCRYPTION STANDARD DES

Cryptographic algorithm designed for the protection of unclassified data and published by the National Institute of Standards and Technology (NIST) in Federal Information Processing Standard (FIPS) Publication 46. See Triple DES. [CNSSI_4009:2010]

2.405.2 DES

Algoritmo público de clave secreta, admitido como estándar en Estados Unidos para información sensible pero sin grado de clasificación oficial y por la norma ISO 8731-1, para autentificación de mensajes bancarios. Sus modos de funcionamiento (ECB, CBC, CFB, OFB) están regulados por la norma FIPS PUB 81. [CESID:1997]

2.405.3 (EN) DATA ENCRYPTION STANDARD - DES

a well-known symmetric encryption mechanism using a 56 bit key. Due to its short key length DES was replaced by the AES, but is still used in multiple encryption mode, e.g., 3DES or Triple DES (FIPS 46-3). [ISO-18028-4:2005]

2.405.4 (EN) DES

An older NIST-standard cryptographic cipher that uses a 56-bit key. Adopted by the NIST in 1977, it was replaced by AES in 2001 as the official standard. DES is a symmetric block cipher that processes 64-bit blocks in four different modes of operation, with the electronic code book (ECB) being the most popular. Triple DES (or 3DES) increased security by adding several multiple-pass methods; for example, encrypting with one key, decrypting the results with a second key and encrypting it again with a third. However, the extra passes added considerable computing time to the process. DES is still used in applications that do not require the strongest security.

http://www.spectralogic.com/index.cfm?fuseaction=home.displayFile&DocID=1235

2.405.5 (FR) DES (DATA ENCRYPTION STANDARD / ANSI X3.92)

Algorithme de chiffrement symétrique développé par IBM en 1973, reposant sur une clé à 56 bits.

http://www.cases.public.lu/functions/glossaire/

2.405.6 (FR) DES - DATA ENCRYPTION STANDARD.

Algorithme de chiffrement basé sur la technique de cryptographie symétrique publié par IBM et adopté par le département de la défense américaine en 1977. DES repose sur une clé symétrique de 56 bits et effectue un chiffrement par blocs de 64 bits. Du fait de sa vulnérabilité aux attaques de type force brute, l'usage de DES décline au profit d'autres algorithmes, notamment 3-DES et AES (Rijndael).

http://securit.free.fr/glossaire.htm

2.406 DESCUBRIMIENTO ELECTRÓNICO

2.406.1 DESCUBRIMIENTO ELECTRÓNICO

El descubrimiento electrónico, o e-discovery, se refiere a todo proceso por el cual se buscan, ubican, aseguran y revisan datos electrónicos con el objeto de utilizarlos como evidencia en un caso legal civil o penal. El e-discovery se puede realizar fuera de línea, en un ordenador particular o dentro de la red La piratería por orden judicial o sancionada por el gobierno con el objeto de obtener evidencia crucial es también un modo de e-discovery.

http://www.recall.es/why-recall/data-protection-terminology

2.406.2 (EN) ELECTRONIC DISCOVERY

process that includes the identification, preservation, collection, processing, review, analysis, and production of Electronically Stored Information

Note 1: Although electronic discovery is often considered a legal process, its use is not limited to the legal domain. [ISO-27050:2015]

2.406.3 (EN) E-DISCOVERY

Electronic discovery (also called e-discovery or ediscovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. E-discovery can be carried out offline on a particular computer or it can be done in a network. Court-ordered or government sanctioned hacking for the purpose of obtaining critical evidence is also a type of e-discovery.

http://whatis.techtarget.com/

2.407 DESDUPLICACIÓN

2.407.1 DESDUPLICACIÓN

La desduplicación de datos es un método de reducción de las necesidades de almacenamiento mediante la eliminación de datos redundantes. En realidad, sólo una única instancia de datos se retiene en medios de almacenamiento, como el disco o la cinta Los datos redundantes se reemplazan con un indicador en la única copia de datos Por ejemplo, un típico sistema de correo electrónico puede contener 100 instancias del mismo archivo adjunto de un megabyte Si la plataforma del correo electrónico tiene copia de seguridad o está archivada, todas las instancias están guardadas; se requiere 100 MB de espacio de almacenamiento En realidad, con la de-duplicación de datos sólo una instancia del adjunto se almacena. Cada instancia posterior hace referencia a la copia original guardada En este ejemplo, una demanda de almacenamiento de 100 MB se puede reducir en sólo un MB.

http://www.recall.es/why-recall/data-protection-terminology

2.407.2 (EN) DATA DEDUPLICATION

Data deduplication looks for redundancy of sequences of bytes across very large comparison windows. Sequences of data (over 8 KB long) are compared to the history of other such sequences. The first uniquely stored version of a sequence is referenced rather than stored again. This process is completely hidden from users and applications so the whole file is readable after it's written.

http://www.emc.com/corporate/glossary/index.htm

2.408 DESENCRIPTAR

Ver:

- *Decripción*

2.408.1 DESENCRIPTAR

Anglicismo que parece referirse al término "descifrar".

2.409 DESINFECCIÓN

Ver:

- *Virus*

2.409.1 DESINFECCIÓN

Acción que realizan los programas anti-virus cuando, tras detectar un virus, lo eliminan del sistema y, en la medida de lo posible, recuperan o restauran la información infectada.

2.409.2 (EN) DISINFECTING

Removing malware from within a file. [NIST-SP800-83:2005]

2.409.3 (EN) DISINFECTION

Eliminación de un virus que se había adosado a un programa o unos datos, recuperando la información en la medida de lo posible.

2.409.4 (FR) UTILITAIRE DE DÉSINFECTION

Petit programme permettant de rechercher et d'éliminer un nombre limité de virus. Il s'agit exclusivement d'un scanner à la demande utilisant une analyse par signatures et dont les définitions de virus ont été limitées à un seul voire quelques virus. Mis à disposition par les éditeurs d'antivirus, principalement lors des épidémies importantes, il permet aux utilisateurs ne possédant pas d'antivirus ou dont l'antivirus aurait été rendu inutilisable de tout de même désinfecter leur ordinateur. Ne disposant pas de moniteur pour surveiller le système en temps réel, l'utilitaire de désinfection est incapable d'empêcher une recontamination si l'utilisateur exécute à nouveau un fichier contaminé ou s'il ne comble pas la faille logicielle possiblement utilisée par le virus pour s'exécuter automatiquement.

http://www.secuser.com/glossaire/

2.410 DESMAGNETIZADOR

Ver:

- *Borrado*
- *Terminación de soportes de información*
- *Soporte*

2.410.1 DESMAGNETIZADOR

Equipo para el borrado de los datos almacenados en soportes magnéticos. Actúa aplicando al soporte un campo magnético creciente desde cero hasta un valor máximo prefijado para volver después nuevamente a cero. [Ribagorda:1997]

2.410.2 DESTRUCCIÓN MAGNÉTICA

También denominada “destrucción magnética de disco”. Proceso o técnica que desmagnetiza un disco para destruir permanentemente toda la información almacenada en éste.

http://es.pcisecuritystandards.org/

2.410.1 (EN) DEGAUSS

Procedure to reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing. [CNSSI_4009:2010]

2.410.2 (EN) DEGAUSS

1a. (N) Apply a magnetic field to permanently remove data from a magnetic storage medium, such as a tape or disk [NCS25]. (Compare: erase, purge, sanitize.)

1b. (N) Reduce magnetic flux density to zero by applying a reversing magnetic field. (See: magnetic remanence.)

[RFC4949:2007]

2.410.3 (EN) DEGAUSSER

(N) An electrical device that can degauss magnetic storage media. [RFC4949:2007]

2.410.4 (EN) DEGAUSS

To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing. Degaussing any current generation hard disk (including but not limited to IDE, EIDE, ATA, SCSI and Jaz) will render the drive permanently unusable since these drives store track location information on the hard drive in dedicated regions of the drive in between the data sectors. [NIST-SP800-88:2006]

2.410.5 (EN) DEGAUSSING

Also called “disk degaussing.” Process or technique that demagnetizes the disk such that all data stored on the disk is permanently destroyed.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.410.6 (EN) DEGAUSSER

An electrical device that can generate a magnetic field for the purpose of degaussing magnetic storage media. [IRM-5239-8:1995]

2.410.7 (FR) DÉMAGNÉTISATION

Également nommé «démagnétisation de disque». Processus ou technique qui démagnétisent le disque, de sorte que toutes les données qui y sont stockées soient supprimées de façon permanente.

http://fr.pcisecuritystandards.org/

2.411 DETECCIÓN DE ANOMALÍAS

Ver:

- *Sistema de detección de intrusiones*

2.411.1 DETECCIÓN DE ANOMALÍA

Detección basada en la actividad de Sistema que coincide con la definida como anormal. [CCN-STIC-432:2006]

2.411.2 DETECCIÓN DE ANOMALÍAS

Detección de desviaciones de lo que sería el comportamiento esperado de algo. Para que funcione es necesario definir previamente qué comportamiento cabe caracterizar como "normal" y así poder identificar desviaciones. La definición previa puede ser una especificación, o resultado de un proceso de aprendizaje tutelado.

2.411.3 (EN) ANOMALY DETECTION

(I) An intrusion detection method that searches for activity that is different from the normal behavior of system entities and system resources. (See: IDS. Compare: misuse detection.) [RFC4949:2007]

2.411.4 (EN) ANOMALY-BASED DETECTION

The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. [NIST-SP800-94:2007]

2.411.5 (EN) ANOMALY DETECTION

Detects any unacceptable deviation from expected behavior. A profile of expected behavior is defined in advance, either manually or automatically. Software that collects and processes characteristics of system behavior over time and forms a statistically valid sample of such behavior is used to create automatically-developed profiles. Some of these deviations do not require further examination and some do. An anomaly might include

- Users logging on at strange hours or from unfamiliar sites on the network.

- Unexplained reboots or changes to system clocks.
- Unusual error messages from mailers, daemons, or other servers.
- Multiple, failed logon attempts with bad passwords.
- Unauthorized use of the /su /command to gain UNIX root access.

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.412 DETECCIÓN DE INCIDENTES

Ver:

- *Evento*

2.412.1 DETECCIÓN DE SUCESOS

Capacidad para la percepción tanto de acciones normales como de aparente violación de un sistema de información.

[CESID:1997]

2.412.2 (EN) EVENT DETECTION

Capability to detect the occurrence of either normal events, and incidentes that may violate the security policy.

2.413 DETECCIÓN DE MANIPULACIONES

Ver:

- *Manipulación*

2.413.1 DETECCIÓN DE MANIPULACIONES

Determinación automática de que un módulo criptográfico ha sido objeto de un ataque.

2.413.2 (EN) TAMPER-EVIDENT

(I) A characteristic of a system component that provides evidence that an attack has been attempted on that component or system.

Usage: Usually involves physical evidence. (See: tamper.)

[RFC4949:2007]

2.413.3 (EN) TAMPER DETECTION

Automatic determination by a cryptographic module that an attempt has been made to compromise the security of the module. [ISO-19790:2006]

2.413.4 (EN) TAMPER EVIDENCE

the external indication that an attempt has been made to compromise the security of a cryptographic module. [ISO-19790:2006]

2.413.5 (EN) TAMPER DETECTION

the automatic determination by a cryptographic module that an attempt has been made to compromise the physical security of the module. [FIPS-140-2:2001]

2.413.6 (EN) TAMPER EVIDENCE

the external indication that an attempt has been made to compromise the physical security of a cryptographic module. (The evidence of the tamper attempt should be observable by an operator subsequent to the attempt.) [FIPS-140-2:2001]

2.414 DETECTOR DE MANIPULACIÓN

Ver:

- *Código de autenticación de mensajes*

2.414.1 DETECTOR DE MANIPULACIÓN

Mecanismo de seguridad usado para detectar las modificaciones accidentales o intencionadas de datos (ISO-7498-2). [Ribagorda:1997]

2.414.2 DETECCIÓN DE MANIPULACIÓN

Mecanismo que se utiliza para detectar si una unidad de datos ha sido modificada, sea accidental o intencionalmente. [ISO-7498-2:1989]

2.414.3 (EN) MANIPULATION DETECTION

A mechanism which is used to detect whether a data unit has been modified (either accidentally or intentionally). [ISO-7498-2:1989]

2.414.4 (FR) DÉTECTION DE MODIFICATION

Mécanisme utilisé pour détecter les modifications, accidentelles ou intentionnelles, d'une unité de données. [ISO-7498-2:1989]

2.415 DÍA CERO

Ver:

- *Código dañino*

2.415.1 ZERO-DAY

Son aquellas vulnerabilidades en sistemas o programas informáticos que son conocidas por determinados atacantes pero no lo son por los fabricantes o por los usuarios. Son las más peligrosas ya que un atacante puede explotarlas sin que el usuario sea consciente de que es vulnerable.

http://www.inteco.es/glossary/Formacion/Glosario/

2.415.2 DÍA CERO

Aprovechamiento de una vulnerabilidad inmediatamente después de haber sido descubierta. Se beneficia del lapso de tiempo requerido por los fabricantes para reparar las vulnerabilidades reportadas.

2.415.3 (EN) ZERO-DAY EXPLOIT

A zero-day exploit is one that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known. Ordinarily, after someone detects that a software program contains a potential exposure to exploitation by a hacker, that person or company can notify the software company and sometimes the world at large so that action can be taken to repair the exposure or defend against its exploitation. Given time, the software company can repair and distribute a fix to users. Even if potential hackers also learn of the vulnerability, it may take them some time to exploit it; meanwhile, the fix can hopefully become available first.

http://searchsoftwarequality.techtarget.com/glossary/

2.415.4 (EN) DAY ZERO

The "Day Zero" or "Zero Day" is the day a new vulnerability is made know. In some cases, a "zero day" exploit is refered to an exploit for which no patch is available yet. ("day one"-> day at which the patch is made available).

http://www.sans.org/security-resources/glossary-of-terms/

2.415.5 (EN) ZERO-DAY EXPLOIT

Malware designed to exploit a newly discovered security hole unknown to the software developer. "Zero-day" refers to the amount of time a developer has between learning of a security hole and the time it becomes public or when black hat hackers find out about it and try to use the security hole for nefarious purposes.

http://cyber.law.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas

2.416 DIARIO REMOTO

2.416.1 DIARIO REMOTO

Proceso utilizado para transmitir diario o diarios de transacciones en tiempo real a una ubicación de copia de seguridad.

2.416.2 (EN) REMOTE JOURNALING

Process used to transmit journal or transaction logs in real time to a back-up location.

http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-b-glossary.aspx

2.417 DIFUSIÓN

Ver:

- *Confusión*

- *Efecto avalancha*

2.417.1 DIFUSIÓN

Propiedad que se predica de aquellos métodos criptográficos en los que la influencia de un símbolo en claro se dispersa sobre un gran número de símbolos cifrados.

De esta manera, las propiedades estadísticas de los caracteres delo mensaje se diseminan por todo el texto cifrado.

[Ribagorda:1997]

2.417.2 DIFUSIÓN

Técnica destinada a disipar las características del idioma en un texto cifrado. Principalmente se consigue mediante transposiciones. [CESID:1997]

2.417.3 (EN) DIFFUSION

Diffusion is the property of an operation such that changing one bit (or byte) of the input will change adjacent or near-by bits (or bytes) after the operation. In a block cipher, diffusion propagates bit-changes from one part of a block to other parts of the block. Diffusion requires mixing, and the step-by-step process of increasing diffusion is described as avalanche. Diffusion is in contrast to confusion.

http://www.ciphersbyritter.com/GLOSSARY.HTM

2.418 DIODO

2.418.1 DISPOSITIVO DE SENTIDO ÚNICO

Este tipo de dispositivo interconecta las redes rompiendo la continuidad de los protocolos de comunicaciones, obligando a que el flujo de información sea en un solo sentido.

Un ejemplo de dispositivo de sentido único sería la interconexión de dos redes mediante un diodo basado en comunicaciones unidireccionales. El acceso a información de Internet, sería el ejemplo más evidente de flujo de información en un solo sentido que podría implicar el uso de este tipo de dispositivos.

[CCN-STIC-302:2012]

2.418.2 (EN) DATA DIODE:

A data diode is a "one-way" data communication device. often consisting of a physical-layer unidirectional limitation. Using only 1/2 of a fiber optic "transmit/receive" pair would enforce unidirectional communication at the physical layer. while proper con-figuration of a network firewall could logically enforce unidirectional communication at the network layer. [knapp:2014]

2.418.3 (EN) UNIDIRECTIONAL GATEWAY

A network gateway device that only allows communication in one direction, such as a Data Diode. [knapp:2014]

2.418.4 (EN) UNIDIRECTIONAL NETWORK

A unidirectional network (also referred to as a unidirectional security gateway or data diode) is a network appliance or device allowing data to travel only in one direction, used in guaranteeing information security. They are most commonly found in high security environments such as defense, where they serve as connections between two or more networks of differing security classifications. This technology can now be found at the Industrial Control level for such facilities as nuclear power plants, and electric power generation.

http://en.wikipedia.org/wiki/Unidirectional_network

2.418.5 (EN) DATA DIODE

Data Diode security products offer one-way communications, allowing secure transfers from a "low security" network to a "high security" network without allowing a path for information to travel back. The most common form of a data diode (unidirectional network) is a simple modified fiber optic cable, with send and receive transceivers removed for one direction. Most commercial products add other software functionality.

The benefit of this type of network connection is it allows networks with sensitive information stored to have access to the Internet as well. There are some drawbacks to this design, unless the vendor builds in software to overcome the drawbacks. TCP/IP communications that require acknowledgements can't flow successfully over a purely hardware data diode, and there is no way for the "low" network to ensure a successful data transfer occurred. Also, this does not prevent viruses or other malicious programs from travelling to the "high" network through the connection.

These products tend to focus on the defense and infrastructure environments where security is critical.

http://www.securitywizardry.com/index.php/products/boundary-guard/data-diodes.html

2.419 DISPONIBILIDAD

2.419.1 DISPONIBLE

Dicho de una cosa: Que se puede disponer libremente de ella o que está lista para usarse o utilizarse.

DRAE. Diccionario de la Lengua Española.

2.419.2 DISPONIBILIDAD

Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE-71504:2008]

2.419.3 DISPONIBILIDAD

Capacidad de ser accesble y estar listo para su uso a demanda de una entidad aturorizada. [UNE-ISO/IEC 27000:2014]

2.419.4 DISPONIBILIDAD

(Diseño del Servicio) Habilidad de un Elemento de Configuración o de un Servicio TI para realizar las Funciones acordadas cuando se requiere. La Disponibilidad la determinan la Certeza, Mantenibilidad, Servicio, Rendimiento, y Seguridad. Normalmente la Disponibilidad se calcula en porcentajes. Éste cálculo se basa normalmente en el Tiempo Acordado para el Servicio y el Tiempo de Parada. Es una Buena Práctica calcular la Disponibilidad usando métricas de las salidas del Negocio respecto del Servicio TI. [ITIL:2007]

2.419.5 DISPONIBILIDAD

Propiedad de los elementos esenciales de ser accesibles sólo para los usuarios autorizados cuando éstos lo requieran. [EBIOS:2005]

2.419.6 DISPONIBILIDAD

1. Propiedad que requiere que los recursos de un sistema abierto sean accesibles y utilizables a petición de una entidad autorizada (ISO-7498-2). Según esta norma la disponibilidad es un servicio de seguridad.

2. Prevención de una negación ilícita de acceso a la información o los recursos (ITSEC).

3, Propiedad de los datos y sistemas de información que son accesibles y utilizables en el tiempo y la forma autorizada (OCDE).

El mantenimiento de la disponibilidad, junto con el de la confidencialidad e integridad, constituye el objetivo de la seguridad de la información.

[Ribagorda:1997]

2.419.7 DISPONIBILIDAD

1. Grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado.

2. Situación que se produce cuando se puede acceder a los servicios de un sistema en un periodo de tiempo considerado aceptable.

[CESID:1997]

2.419.8 DISPONIBILIDAD

Propiedad de ser accesible y utilizable a petición por una entidad autorizada. [ISO-7498-2:1989]

2.419.9 (EN) AVAILABILITY

property of being accessible and usable upon demand by an authorized entity [ISO/IEC 27000:2014]

2.419.10 (EN) AVAILABILITY

The term `availability' means ensuring timely and reliable access to and use of information.

Cyber Intelligence Sharing and Protection Act. H.R. 624. 2013.

2.419.1 (EN) AVAILABILITY

The property of being accessible and useable upon demand by an authorized entity.

NIST 800-53: Ensuring timely and reliable access to and use of information.

[CNSSI_4009:2010]

2.419.2 (EN) AVAILABILITY

1. (I) The property of a system or a system resource being accessible, or usable or operational upon demand, by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them. (See: critical, denial of service. Compare: precedence, reliability, survivability.)

2. (O) "The property of being accessible and usable upon demand by an authorized entity." [ISO-7498-2]

[RFC4949:2007]

2.419.3 (EN) AVAILABILITY

Timely, reliable access to information by authorized entities. [NIST-SP800-57:2007]

2.419.4 (EN) AVAILABILITY

(Service Design) Ability of a Configuration Item or IT Service to perform its agreed Function when required. Availability is determined by Reliability, Maintainability, Serviceability, Performance, and Security. Availability is usually calculated as a percentage. This calculation is often based on Agreed Service Time and Downtime. It is Best Practice to calculate Availability using measurements of the Business output of the IT Service. [ITIL:2007]

2.419.5 (EN) AVAILABILITY

Property of essential elements that allows authorised users to access them at the required time. [EBIOS:2005]

2.419.6 (EN) AVAILABILITY

The security goal that generates the requirement for protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data. [NIST-SP800-27:2004]

2.419.7 (EN) AVAILABILITY

Ensuring timely and reliable access to and use of information.

U.S. Code 44, Sec. 3542. Definitions, 2007

2.419.8 (EN) AVAILABILITY

The property of being accessible and useable upon demand by an authorized entity. [ISO-18028-2:2006]

2.419.9 (EN) AVAILABILITY

The Availability Security Dimension ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to events impacting the network. Disaster recovery solutions are included in this category. [X.805:2003]

2.419.10 (EN) AVAILABILITY

The extend to which, or frequency with which, an asset must be present or ready for use. [Octave:2003]

2.419.11 (EN) AVAILABILITY

The security objective that generates the requirement for protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data. [NIST-SP800-33:2001]

2.419.12 (EN) AVAILABILITY

The assurance that data transmissions, computer processing systems, and/or communications are not denied to those who are authorized to use them (JCS 1997)

http://www.ioss.gov/docs/definitions.html

2.419.13 (EN) AVAILABILITY

the prevention of the unauthorised withholding of information or resources. [ITSEC:1991]

2.419.14 (EN) AVAILABILITY

The property of being accessible and useable upon demand by an authorized entity. [ISO-7498-2:1989]

2.419.15 (EN) AVAILABILITY

Availability is the need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it.

http://www.sans.org/security-resources/glossary-of-terms/

2.419.16 (FR) DISPONIBILITÉ

(Conception de services) Capacité d'un élément de configuration ou d'un service des TI à réaliser sa fonction convenue lorsque c'est nécessaire. La disponibilité est déterminée par la fiabilité, la facilité de maintenance, la facilité de service, la performance et la sécurité. La disponibilité est habituellement calculée sous la forme d'un pourcentage. Ce calcul est basé le plus souvent sur le temps de service convenu et le Temps d'indisponibilité. La meilleure pratique consiste à calculer la disponibilité en se basant sur les mesures du service des TI effectuées côté Business. [ITIL:2007]

2.419.17 (FR) DISPONIBILITÉ

Propriété d'accessibilité au moment voulu des éléments essentiels par les utilisateurs autorisés. [EBIOS:2005]

2.419.18 (FR) DISPONIBILITÉ

La propriété de ce qui peut être accessible et utilisable à la demande par une entité autorisée. [ISO-7498-2:1989]

2.419.19 (FR) DISPONIBILITÉ

Condition d'être accessible et utilisable de manière fiable et en temps opportun.

http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578

2.420 DISPOSITIVO CRIPTOGRÁFICO

Ver:

- *Módulo criptográfico*
- *Equipo criptográfico*
- *Token criptográfico*

2.420.1 DISPOSITIVO SEGURO CRIPTOGRÁFICO

Un conjunto de hardware, software y firmware que implementa procesos criptográficos (incluidos algoritmos criptográficos y generación de claves) y que está contenido dentro de un límite criptográfico definido. Entre los ejemplos de dispositivos criptográficos seguros se incluyen los módulos de seguridad de hardware o de host (HSM) y dispositivos de punto de interacción (POI) que se han validad mediante los PCI PTS.

http://es.pcisecuritystandards.org

2.420.2 HSM

Acrónimo de “hardware security module” (módulo de seguridad de hardware) o “host security module” (módulo de seguridad de host). Un dispositivo de hardware protegido en forma lógica y física que proporciona un conjunto seguro de servicios cartográficos, empleados en funciones de administración de claves criptográficas o el descifrado de los datos de cuentas.

http://es.pcisecuritystandards.org

2.420.3 HSM

Acrónimo de las siglas en inglés de Hardware Security Module, Módulo de Seguridad de Hardware. Es un dispositivo seguro de creación de firma electrónica el cual consiste en un hardware criptográfico diseñado especialmente para generar, almacenar y utilizar claves tanto simétricas como asimétricas.

Suele ser utilizado para aportar una mayor velocidad a las operaciones criptográficas. Su funcionamiento implica que las aplicaciones no operen directamente con las claves, sino que se comuni-

quen con el hardware criptográfico solicitando la realización de una operación, tratando de conseguir que una clave nunca esté en una máquina donde está la aplicación, sino en la memoria del HSM.

http://www.inteco.es/glossary/Formacion/Glosario/

2.420.4 DISPOSITIVO CRIPTOGRÁFICO

Componente electrónico de un equipo físico, o submontaje de éste, que implementa un cifrado (ISO-8732). [Ribagorda:1997]

2.420.5 EQUIPO CRIPTOGRÁFICO

Equipo en el que se ejecutan las funciones criptográficas (por ejemplo: cifrado, autenticación, generación de claves) (ISO-8732). [Ribagorda:1997]

2.420.6 (EN) SECURE CRYPTOGRAPHIC DEVICE:

A set of hardware, software and firmware that implements cryptographic processes (including cryptographic algorithms and key generation) and is contained within a defined cryptographic boundary. Examples of secure cryptographic devices include host/hardware security modules (HSMs) and point-of-interaction devices (POIs) that have been validated to PCI PTS.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.420.7 (EN) HSM

Acronym for “hardware security module” or “host security module.” A physically and logically protected hardware device that provides a secure set of cryptographic services, used for cryptographic key-management functions and/or the decryption of account data.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.420.8 (EN) CRYPTOGRAPHIC COMPONENT

(I) A generic term for any system component that involves cryptography. (See: cryptographic module.) [RFC4949:2007]

2.420.9 (FR) PÉRIPHÉRIQUES CRYPTOGRAPHIQUES SÉCURISÉS

Un ensemble de matériel, logiciel et firmware qui implémente les processus cryptographiques (y compris les algorithmes et la production de clés cryptographiques) et qui est contenu dans une frontière cryptographique définie. Les exemples de périphériques cryptographiques comprennent les modules de sécurité hôte/matériel (HSM) et les appareils de point d’interaction (POI) qui ont été validés selon PCI PTS.

http://fr.pcisecuritystandards.org/

2.420.10 (FR) HSM

Acronyme de «hardware security module», module de sécurité matérielle ou «host security module», module de sécurité hôte. Un dispositif matériel protégé physiquement et logiquement qui

offre un ensemble sécurisé de services cryptographiques utilisé pour les fonctions de gestion de clé cryptographique et/ou le décryptage des données de compte.

http://fr.pcisecuritystandards.org/

2.421 DISPOSITIVO DE CREACIÓN DE FIRMA

Ver:

- *Firma electrónica*
- *Datos de creación de firma*

2.421.1 DISPOSITIVO DE CREACIÓN DE FIRMA ELECTRÓNICA

«dispositivo de creación de firma electrónica», un equipo o programa informático configurado que se utiliza para crear una firma electrónica; [PE-CONS 60/14]

2.421.2 DISPOSITIVO CUALIFICADO DE CREACIÓN DE FIRMA ELECTRÓNICA

«dispositivo cualificado de creación de firma electrónica», un dispositivo de creación de firmas electrónicas que cumple los requisitos enumerados en el anexo II; [PE-CONS 60/14]

2.421.3 DISPOSITIVO DE CREACIÓN DE FIRMA

es un programa o sistema informático que sirve para aplicar los datos de creación de firma. [Ley-59:2003]

2.421.4 DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA

es un dispositivo de creación de firma que ofrece, al menos, las siguientes garantías:

- Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.
- Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.
- Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.
- Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.

[Ley-59:2003]

2.421.5 (EN) ELECTRONIC SIGNATURE CREATION DEVICE

'electronic signature creation device' means configured software or hardware used to create an electronic signature; [PE-CONS 60/14]

2.421.6 (EN) QUALIFIED ELECTRONIC SIGNATURE CREATION DEVICE

'qualified electronic signature creation device' means an electronic signature creation device that meets the requirements laid down in Annex II; [PE-CONS 60/14]

2.421.7 (EN) SIGNATURE-CREATION DEVICE

means configured software or hardware used to implement the signature-creation data [Directive-1999/93/EC:1999]

2.421.8 (EN) SECURE-SIGNATURE-CREATION DEVICE

means a signature-creation device which meets the requirements laid down in Annex III.

1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:

- the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
- the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
- the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.

2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

[Directive-1999/93/EC:1999]

2.421.9 (FR) DISPOSITIF DE CREATION DE SIGNATURE ELECTRONIQUE

"dispositif de création de signature électronique", un dispositif logiciel ou matériel configuré servant à créer une signature électronique; [PE-CONS 60/14]

2.421.10 (FR) DISPOSITIF DE CREATION DE SIGNATURE ELECTRONIQUE QUALIFIE

"dispositif de création de signature électronique qualifié", un dispositif de création de signature électronique qui satisfait aux exigences énoncées à l'annexe II; [PE-CONS 60/14]

2.422 DISPOSITIVO DE PROTECCIÓN PERIMETRAL

Acrónimos: BPD

Ver:

- *Protección del perímetro*

2.422.1 DISPOSITIVO DE PROTECCIÓN DE PERÍMETRO

Hardware y/o software, cuya finalidad es mediar en el tráfico de entrada y salida en los puntos de interconexión de los sistemas. [CCN-STIC-302:2012]

2.422.2 (EN) BOUNDARY PROTECTION DEVICE

A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) monitors and controls communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications. Boundary protection devices include such components as proxies, gateways, routers, firewalls, guards, and encrypted tunnels. [NIST-SP800-53:2013]

2.423 DISPOSITIVO DE VERIFICACIÓN DE FIRMA

Ver:

- *Firma electrónica*
- *Datos de verificación de firma*

2.423.1 DISPOSITIVO DE VERIFICACIÓN DE FIRMA

es un programa o sistema informático que sirve para aplicar los datos de verificación de firma.

Los dispositivos de verificación de firma electrónica garantizarán, siempre que sea técnicamente posible, que el proceso de verificación de una firma electrónica satisfaga, al menos, los siguientes requisitos:

- Que los datos utilizados para verificar la firma correspondan a los datos mostrados a la persona que verifica la firma.
- Que la firma se verifique de forma fiable y el resultado de esa verificación se presente correctamente.
- Que la persona que verifica la firma electrónica pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.
- Que se muestren correctamente tanto la identidad del firmante o, en su caso, conste claramente la utilización de un seudónimo, como el resultado de la verificación.
- Que se verifiquen de forma fiable la autenticidad y la validez del certificado electrónico correspondiente.
- Que pueda detectarse cualquier cambio relativo a su seguridad.

[Ley-59:2003]

2.423.2 (EN) SIGNATURE-VERIFICATION DEVICE

means configured software or hardware used to implement the signature-verification-data.

[Directive-1999/93/EC:1999]

2.424 DISTRIBUCIÓN DE CLAVES

Ver:

- *Clave*
- *Clave criptográfica*
- *Centro de distribución de claves*

2.424.1 DISTRIBUCIÓN ELECTRÓNICA DE CLAVES

Transmisión segura por medio de un sistema de comunicación eléctrica y a través del canal de transmisión de una clave a utilizar en cifrados posteriores. [CESID:1997]

2.424.2 DISTRIBUCIÓN FÍSICA DE CLAVES

Transmisión de una clave en un determinado soporte (papel, cinta perforada, disquete, inyector de claves...) hasta el equipo remoto por medios ajenos al canal de transmisión, en general un mensajero. [CESID:1997]

2.424.3 (EN) KEY DISTRIBUTION

(I) A process that delivers a cryptographic key from the location where it is generated to the locations where it is used in a cryptographic algorithm. (See: key establishment, key management.) [RFC4949:2007]

2.424.4 (EN) KEY DISTRIBUTION

The transport of a key and other keying material from an entity that either owns the key or generates the key to another entity that is intended to use the key. [NIST-SP800-57:2007]

2.425 DISUASIÓN

2.425.1 DISUASIÓN

Medida de seguridad que previene la ocurrencia de incidentes en base a causar miedo, dudas o ansiedad en el atacante. Las técnicas de disuasión reducen la probabilidad de que el ataque se lleve a cabo.

2.425.2 (EN) DETERRENT

measure that discourages an action or prevents an occurrence by instilling fear, doubt, or anxiety

Annotation: A deterrent reduces threat by decreasing the likelihood of an attempted attack.

DHS Risk Lexicon, September 2008

2.426 DOMINIO DE INFORMACIÓN

2.426.1 DOMINIO DE INFORMACIÓN

Concepto relativo a la compartición de información independiente del sistema de información y del dominio de seguridad.

1. Se identifica individualmente a las personas que forman parte del dominio.

2. Se identifican objetos o elementos de información a compartir.

3. Se establece una política de seguridad que dentifica los roles y privilegios de los miembros y las protecciones que requieren los elementos de información.

2.426.2 (EN) INFORMATION DOMAIN

A three-part concept for information sharing, independent of, and across information systems and security domains that 1) identifies information sharing participants as individual members, 2) contains shared information objects, and 3) provides a security policy that identifies the roles and privileges of the members and the protections required for the information objects. [CNSSI_4009:2010]

2.427 DOMINIO DE SEGURIDAD

Ver:

- *Autoridad de dominio de seguridad*
- *Política de seguridad*

2.427.1 DOMINIO DE SEGURIDAD

Un conjunto de elementos, una política de seguridad, una autoridad de seguridad y un conjunto de actividades pertinentes a la seguridad, donde el conjunto de elementos está sujeto a la política de seguridad, para las actividades especificadas y la política de seguridad es administrada por la autoridad de seguridad para el dominio de seguridad. [X.810:1995]

2.427.2 (EN) DOMAIN

An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See also security domain. [CNSSI_4009:2010]

2.427.3 (EN) DOMAIN

1a. (I) /general security/ An environment or context that (a) includes a set of system resources and a set of system entities that have the right to access the resources and (b) usually is defined by a security policy, security model, or security architecture. (See: CA domain, domain of interpretation, security perimeter. Compare: COI, enclave.)

1b. (O) /security policy/ A set of users, their information objects, and a common security policy. [DoD6, SP33]

1c. (O) /security policy/ A system or collection of systems that (a) belongs to a community of interest that implements a consistent security policy and (b) is administered by a single authority.

[RFC4949:2007]

2.427.4 (EN) SECURITY DOMAIN

A system or subsystem that is under the authority of a single trusted authority. Security domains may be organized (e.g., hierarchically) to form larger domains. [NIST-SP800-57:2007]

2.427.5 (EN) SECURITY DOMAIN

the collection of resources to which an active entity has access. [CC:2006]

2.427.6 (EN) DOMAIN

An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. [NIST-SP800-53:2013]

2.427.1 (EN) DOMAIN

An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See also security domain. [CNSSI_4009:2010]

2.427.2 (EN) SECURITY DOMAIN

A domain that implements a security policy and is administered by a single authority. [NIST-SP800-53:2009]

2.427.3 (EN) SECURITY DOMAIN

a set of assets and resources subject to a common security policy. [ISO-18028-1:2006]

2.427.4 (EN) SECURITY DOMAIN

A security domain is a collection of users and systems subject to a common security policy. [ISO-18028-3:2005]

2.427.5 (EN) DOMAIN

Collection of entities operating under a single security policy, e.g., public key certificates created by a single certification authority, or by a collection of certification authorities using the same security policy. [ISO-9798-5:2004]

2.427.6 (EN) SECURITY DOMAIN

A set of subjects, their information objects, and a common security policy. [NIST-SP800-27:2004]

2.427.7 (EN) SECURITY DOMAIN

A collection of users and systems subject to a common security policy. [ISO-15816:2002]

2.427.8 (EN) SECURITY DOMAIN

A set of subjects, their information objects, and a common security policy. [NIST-SP800-33:2001]

2.427.9 (EN) SECURITY DOMAIN

A set of elements, a security policy, a security authority and a set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain. [X.810:1995]

2.427.10 (EN) DOMAIN SEPARATION

the security architecture property whereby the TSF defines separate security domains for each user and for the TSF and ensures that no user process can affect the contents of a security domain of another user or of the TSF.

TSF - TOE Security Functionality

[CC:2006]

2.427.11 (FR) DOMAINE DE SÉCURITÉ

ensemble d'éléments, politique de sécurité, autorité de sécurité et ensemble d'activités liées à la sécurité dans lesquels l'ensemble des éléments est sujet à la politique de sécurité, pour les activités spécifiées et la politique de sécurité est administrée par l'autorité de sécurité, pour le domaine de sécurité. [X.810:1995]

2.428 DRIVE-BY EXPLOITS

2.428.1 DRIVE-BY

Drive-by download, también conocido como *Drive-by Exploit*, se refiere a un malware que se instala en tu computadora con el sólo hecho de visitar páginas en Internet que están infectadas por este tipo de amenaza. No se requiere una interacción alguna, este malware se encuentra en el mismo código HTML de las páginas infectadas y el sólo hecho de cargarlas en tu navegador de Internet hace que se contamine tu computadora.

http://aprenderinternet.about.com/od/Glosario/

2.428.2 (EN) DRIVE-BY EXPLOITS

This threat refers to the injection of malicious code in HTML code of websites that exploits vulnerabilities in user web browsers. Also known as drive-by download attacks, these attacks target software residing in Internet user computers (web browser, browser plug-ins and operating system) and infects them automatically when visiting a drive-by download website, without any user interaction.

ENISA Threat Landscape [Deliverable – 2012-09-28]

2.428.3 (EN) DRIVE-BY-DOWNLOADS

In a Drive-by-Download attack, the web application is tampered (i.e. injected with HTML code) that instructs a visitor’s browser to download malware located in an attacker’s controlled server. Most often, tampering is not visually apparent to visitors, thus innocent victims are unaware of the background download operation. If any warning appears it is usually dismissed since victims believe it to be part of the original application. The malware is usually Trojan horse software that takes control of the victim’s machine, making it part of a larger botnet.

http://www.imperva.com/resources/glossary/glossary.html

2.428.4 (EN) DRIVE-BY DOWNLOAD

Description of a series of events culminating in the delivery of malware without the end user being aware. A "Drive-by-Download" begins with a user visiting a website that hosts an Exploit which then compromises the user's web browser. Once the end user's system has been "owned", the exploit makes a call to download the malware. One commonly overlooked aspect of "Drive-by downloads" is that they require a vulnerable web browser to be compromised by an exploit. Any security solution that stops the exploit will prevent the malware from being downloaded.

https://www.nsslabs.com/reports/threat-definitions

2.428.5 (EN) DRIVE-BY-DOWNLOAD:

Software, often malware, downloaded onto a computer from the Internet without the user's knowledge or permission.

Cybersecurity for Dummies, Palo Alto Networks Edition, 2014

2.429 DSA - DIGITAL SIGNATURE ALGORITHM

Acrónimos: DSA, DSS

Ver:

- *Firma digital*
- [FIPS-186-2:2000]
- *El Gamal*
- *ECDSA - Elliptic Curve Digital Signature Algorithm*

2.429.1 ESTÁNDAR ESTADOUNIDENSE DE FIRMA DIGITAL

Procedimiento de firma digital elevado a la categoría de estándar federal con el nombre de Digital Signature Standard y más conocido por sus siglas DSS.

Está basado en el algoritmo de El Gamal, pero el hecho de no poder ser utilizado para cifrar información (a diferencia del algoritmo RSA que puede ser usado para firmar y cifrar) y cierta precipitación en su adopción como norma federal, ha provocado una generalizada prevención hacia el mismo entre la comunidad criptológica.

[Ribagorda:1997]

2.429.2 DSA

Algoritmo estándar estadounidense de firma digital para aplicaciones gubernamentales diseñado por el National Institute for Standards and Technology (NIST). Es una variante con apéndice del esquema de firma digital de El Gamal. [CESID:1997]

2.429.3 (EN) DIGITAL SIGNATURE ALGORITHM (DSA)

(N) An asymmetric cryptographic algorithm for a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified. (See: DSS.) [RFC4949:2007]

2.429.4 (EN) DIGITAL SIGNATURE STANDARD (DSS)

(N) The U.S. Government standard [FP186] that specifies the DSA. [RFC4949:2007]

2.429.5 (EN) DSA

An asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified.

2.430 DSNIFF

Ver:

- *Pruebas de penetración*
- http://monkey.org/~dugsong/dsniff/

2.430.1 DSNIFF

Conjunto de herramientas para análisis de redes: auditoría y pruebas de penetración.

2.430.2 (EN) DSNIFF

dsniff is a collection of tools for network auditing and penetration testing. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy passively monitor a network for interesting data (passwords, e-mail, files, etc.). arpspoof, dnsspoof, and macof facilitate the interception of network traffic normally unavailable to an attacker (e.g, due to layer-2 switching). sshmitm and webmitm implement active monkey-in-the-middle attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI.

2.431 ECB - ELECTRONIC CODEBOOK MODE

Acrónimos: ECB

Ver:

- *Modo de operación (1)*
- [NIST-SP800-38A:2001]
- [FIPS-81:1980]
- *Criptografía de clave secreta*
- http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

2.431.1 LIBRO ELECTRÓNICO DE CÓDIGOS

Modalidad de cifrado de bloques en la cual cada bloque se cifra independientemente de los demás, sin realimentación del texto cifrado sobre el propio dispositivo criptográfico (ISO-7498-2). [Ribagorda:1997]

2.431.2 (EN) ELECTRONIC CODEBOOK (ECB)

(N) A block cipher mode in which a plaintext block is used directly as input to the encryption algorithm and the resultant output block is used directly as cipher text [FP081]. (See: block cipher, [SP38A].) [RFC4949:2007]

2.431.3 (EN) ECB - ELECTRONIC CODEBOOK MODE

The simplest of the encryption modes is the electronic codebook (ECB) mode. The message is divided into blocks and each encrypted separately. The disadvantage of this method is that identical plaintext blocks are encrypted into identical ciphertext blocks; thus, it does not hide data patterns well. In some senses, it doesn't provide serious message confidentiality, and it is not recommended for use in cryptographic protocols at all.

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

2.432 ECDSA - ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

Acrónimos: ECDSA

Ver:

- *DSA - Digital Signature Algorithm*

2.432.1 ECDSA - ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

Es una modificación del algoritmo DSA que emplea operaciones sobre puntos de curvas elípticas en lugar de las exponenciaciones que usa DSA (problema del logaritmo discreto). La principal ventaja de este esquema es que requiere números de tamaños menores para brindar la misma seguridad que DSA o RSA.

http://es.wikipedia.org/wiki/ECDSA

2.432.2 (EN) ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

(I) A type of asymmetric cryptography based on mathematics of groups that are defined by the points on a curve, where the curve is defined by a quadratic equation in a finite field. [Schn] [RFC4949:2007]

2.432.3 (EN) ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA)

(N) A standard [A9062] that is the analog, in elliptic curve cryptography, of the Digital Signature Algorithm. [RFC4949:2007]

2.433 EFECTIVIDAD

Ver:

- *Eficiencia*

2.433.1 EFECTIVIDAD

Capacidad de lograr el efecto que se desea o se espera.

DRAE. Diccionario de la Lengua Española.

2.433.2 EFICACIA

Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados. [UNE-ISO/IEC 27000:2014]

2.433.3 EFECTIVIDAD

(Mejora Continua del Servicio) Una medida de si los Objetivos de un Proceso, Servicio o Actividad han sido alcanzados. Un Efectivo Proceso o Actividad es uno que alcanza sus Objetivos acordados. Ver KPI. [ITIL:2007]

2.433.4 EFICACIA

extensión en la que se realizan las actividades planificadas y se alcanzan los resultados planificados [ISO-9000_es:2000]

2.433.5 EFECTIVIDAD

Propiedad de un Objeto de Evaluación, que representa lo adecuadamente que éste proporciona seguridad en el contexto de su uso operativo real o propuesto (ITSEC) [Ribagorda:1997]

2.433.6 EFECTIVIDAD

Medida del grado en que un sistema de información proporciona seguridad en un contexto concreto o en el desempeño de una función determinada. [CESID:1997]

2.433.7 (EN) EFFECTIVINESS

extent to which planned activities are realized and planned results achieved [ISO/IEC 27000:2014]

2.433.8 (EN) EFFECTIVITY

producing the result that is wanted or intended; producing a successful result.

Oxford Advanced Learner's Dictionary.

2.433.9 (EN) EFFECTIVENESS

(O) /ITSEC/ A property of a TOE representing how well it provides security in the context of its actual or proposed operational use. [RFC4949:2007]

2.433.10 (EN) EFFECTIVENESS

a property of a system or product representing how well it provides security in the context of its proposed or actual operational use. [ISO-21827:2007]

2.433.11 (EN) EFFECTIVENESS

(Continual Service Improvement) A measure of whether the Objectives of a Process, Service or Activity have been achieved. An Effective Process or Activity is one that achieves its agreed Objectives. See KPI. [ITIL:2007]

2.433.12 (EN) EFFECTIVENESS

a property of a Target of Evaluation representing how well it provides security in the context of its actual or proposed operational use. [ITSEC:1991]

2.433.13 (FR) EFFICACITÉ

(Amélioration continuelle du service) Mesure permettant de savoir si les objectifs d'un processus, d'un service ou d'une activité ont été atteints. Un processus ou une activité efficace est celui ou celle qui atteint les objectifs convenus. Voir KPI. [ITIL:2007]

2.434 EFECTO AVALANCHA

Ver:

- *Confusión*
- *Difusión*

2.434.1 EFECTO AVALANCHA

Propiedad de los algoritmos de cifra en virtud de la cual pequeños cambios en el texto en claro producen cambios radicales en el texto cifrado.

Rigurosamente, se dice que un algoritmo cumple el criterio de avalancha cuando, en promedio, complementa la mitad de los bits del texto cifrado al complementar un solo bit del texto en claro. Si cada bit del texto cifrado se complementa con probabilidad de un medio, siempre que un bit cualquiera del texto en se complemente, se afirma que satisface el criterio de avalancha estricto.

[Ribagorda:1997]

2.434.2 EFECTO AVALANCHA

Propiedad de diseño de los algoritmos criptográficos por la cual el cambio de un bit de la clave o un bit del texto claro produce un cambio radical en el texto cifrado obtenido. [CESID:1997]

2.434.3 (EN) AVALANCHE EFFECT

An effect in DES and other secret key ciphers where each small change in plaintext implies that somewhere around half the ciphertext changes. The avalanche effect makes it harder to successfully cryptanalyze the ciphertext.

http://www.crypto.ch/

2.435 EFICIENCIA

Ver:

- *Efectividad*

2.435.1 EFICIENCIA

(Mejora Continua del Servicio) Una medida de si el correcto monto de recursos ha sido utilizado para la provisión de un Proceso, Servicio o Actividad. Un Eficiente Proceso alcanza sus Objetivos con el mínimo de cantidad de tiempo, dinero, gente u otros recursos. Ver KPI. [ITIL:2007]

2.435.2 EFICIENCIA

relación entre el resultado alcanzado y los recursos utilizados. [ISO-9000_es:2000]

2.435.3 (EN) EFFICIENCY

(Continual Service Improvement) A measure of whether the right amount of resources have been used to deliver a Process, Service or Activity. An Efficient Process achieves its Objectives with the minimum amount of time, money, people or other resources. See KPI. [ITIL:2007]

2.435.4 (FR) EFFICIENCE

(Amélioration continuelle du service) Mesure permettant de savoir si la bonne quantité de ressources a été utilisée pour un processus, un service ou une activité. Un processus efficient atteint ses objectifs avec un minimum de temps, d'argent, de personnel ou autres ressources. Voir KPI. [ITIL:2007]

2.436 EL GAMAL

Ver:

- *DSA - Digital Signature Algorithm*
- *Firma digital*

2.436.1 FIRMA DIGITAL DE EL GAMAL

Es de recalcar que aunque el algoritmo citado puede emplearse también para cifrar información, su complejidad y el hecho de duplicar el texto cifrado la longitud del texto en claro lo hacen poco recomendable para tal fin. [Ribagorda:1997]

2.436.2 ESQUEMA DE EL GAMAL

Algoritmo criptográfico de clave pública que puede emplearse tanto para cifrar como para obtener firmas digitales y que basa su seguridad en la dificultad de calcular logaritmos discretos en un campo finito. [CESID:1997]

2.436.3 (EN) EL GAMAL ALGORITHM

(N) An algorithm for asymmetric cryptography, invented in 1985 by Taher El Gamal, that is based on the difficulty of calculating discrete logarithms and can be used for both encryption and digital signatures. [ElGa] [RFC4949:2007]

2.436.4 (EN) ELGAMAL SIGNATURE SCHEME

The ElGamal signature scheme is a digital signature scheme which is based on the difficulty of computing discrete logarithms. It was described by Taher ElGamal in 1984 (see T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans inf Theo, 31:469-472, 1985).

The ElGamal signature algorithm described in this article is rarely used in practice. A variant developed at NSA and known as the Digital Signature Algorithm is much more widely used. There are several other variants (see K. Nyberg and R. A. Rueppel, Message recovery for signature schemes based on the discrete logarithm problem, J Crypt, 8:27-37, 1995). The ElGamal signature scheme must not be confused with ElGamal encryption which was also invented by Taher ElGamal.

The ElGamal signature scheme allows that a verifier can confirm the authenticity of a message m sent by the signer sent to him over an insecure channel.

http://en.wikipedia.org/wiki/ElGamal_signature_scheme

2.437 EMANACIONES

Ver:

- *Emanaciones comprometedoras*
- *Seguridad de las emanaciones*
- *TEMPEST*

2.437.1 EMANACIONES

Radiación electromagnética emitida por los equipos o líneas de comunicaciones. Pudiera ser objeto de análisis por parte de un atacante con él ánimo de acceder a la información procesada o transmitida.

2.437.2 (EN) EMANATION

(I) A signal (e.g., electromagnetic or acoustic) that is emitted by a system (e.g., through radiation or conductance) as a consequence (i.e., byproduct) of the system's operation, and that may contain information. (See: emanations security.) [RFC4949:2007]

2.437.3 (EN) EMANATIONS ANALYSIS

Gaining direct knowledge of communicated data by monitoring and resolving a signal that is emitted by a system and that contains the data but is not intended to communicate the data.

http://www.sans.org/security-resources/glossary-of-terms/

2.437.4 (EN) RADIATION MONITORING

Radiation monitoring is the process of receiving images, data, or audio from an unprotected source by listening to radiation signals.

http://www.sans.org/security-resources/glossary-of-terms/

2.438 EMANACIONES COMPROMETEDORAS

Ver:

- *Emanaciones*
- *TEMPEST*

2.438.1 EMANACIONES COMPROMETEDORAS

Señales emitidas accidentalmente que, si son interceptadas y analizadas, podrían llevar a la revelación de la información almacenada, transmitida o presentada en un sistema de información.

2.438.2 (EN) COMPROMISING EMANATIONS

Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by information systems equipment. See TEMPEST [CNSSI_4009:2010]

2.439 EMERGENCIA

Ver:

- *Continuidad*
- *CERT - Equipo de reacción rápida ante incidentes informáticos*

2.439.1 EMERGENCIA

Situación de peligro o desastre que requiere una acción inmediata.

DRAE. Diccionario de la Lengua Española.

2.439.2 (EN) EMERGENCY RESPONSE

(O) An urgent response to a fire, flood, civil commotion, natural disaster, bomb threat, or other serious situation, with the intent of protecting lives, limiting damage to property, and minimizing disruption of system operations. [FP087] (See: availability, CERT, emergency plan.) [RFC4949:2007]

2.440 EMPLAZAMIENTO MÓVIL

Ver:

- *Sede alternativa*

2.440.1 EMPLAZAMIENTO MÓVIL

Sistema autocontenido ubicado en una plataforma móvil.

2.440.2 (EN) MOBILE SITE

A self-contained, transportable shell custom-fitted with the specific IT equipment and telecommunications necessary to provide full recovery capabilities upon notice of a significant disruption. [NIST-SP800-34:2002]

2.440.3 (EN) MOBILE SITE

A Hot Site or a Cold Site on wheels.

Mobile sites are typically trailers which contain the necessary heating, cooling, electrical installations and equipment to form temporary offices or computer rooms.

2.441 ENCADENAMIENTO CRIPTOGRÁFICO

2.441.1 ENCADENAMIENTO CRIPTOGRÁFICO

Modo de utilización de un algoritmo criptográfico en el cual la transformación realizada por el algoritmo depende de los valores de las entradas o salidas previas. [X.810:1995]

2.441.2 (EN) CRYPTOGRAPHIC CHAINING

A mode of use of a cryptographic algorithm in which the transformation performed by the algorithm depends on the values of previous inputs or outputs. [X.810:1995]

2.441.3 (FR) CHAÎNAGE CRYPTOGRAPHIQUE

mode d'utilisation d'un algorithme cryptographique dans lequel la transformation effectuée par l'algorithme dépend des valeurs des entrées ou sorties précédentes. [X.810:1995]

2.442 ENCRIPCIÓN

Ver:

- *Cifrado*
- *Algoritmo de cifra*

2.442.1 ENCRIPCIÓN

Véase cifrado. [ISO-7498-2:1989]

2.442.2 (EN) ENCRYPTION

1. (I) Cryptographic transformation of data (called "plain text") into a different form (called "cipher text") that conceals the data's original meaning and prevents the original form from being used. The corresponding reverse process is "decryption", a transformation that restores encrypted data to its original form. (See: cryptography.)

2. (O) "The cryptographic transformation of data to produce ciphertext." [ISO-7498-2]

Usage: For this concept, IDOCs SHOULD use the verb "to encrypt" (and related variations: encryption, decrypt, and decryption). However, because of cultural biases involving human burial, some international documents (particularly ISO and CCITT standards) avoid "to encrypt" and instead use the verb "to encipher" (and related variations: encipherment, decipher, decipherment).

[RFC4949:2007]

2.442.3 (EN) ENCRYPTION

The process of changing plaintext into ciphertext using a cryptographic algorithm and key. [NIST-SP800-57:2007]

2.442.4 (EN) ENCRYPTION

(reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data [ISO/IEC ISO-9797-1]. [ISO-18033-1:2005]

2.442.5 (EN) ENCRYPTION

Encryption is a cryptographic operation that is used to provide confidentiality for sensitive information; decryption is the inverse operation.

Encrypted data is inaccessible until decrypted, and the ability to decrypt can be limited only to authorized receivers of the data.

Encryption is used to protect data confidentiality; with additional features, it can also protect data integrity (through validating that the encrypted data has not been altered). Encryption can be used to protect data at rest and data in motion.

Mobile Security Reference Architecture, May 23, 2013

2.443 ENCRYPT

Ver:

- *Cifrar*
- *Codificar*
- *Encripción*

2.443.1 ENCRIPTAR

Anglicismo que parece referirse al término "cifrar".

2.443.1 (EN) ENCRYPT

Generic term encompassing encipher and encode. [CNSSI_4009:2010]

2.443.2 (EN) ENCRYPT

(I) Cryptographically transform data to produce cipher text. (See: encryption. Compare: seal.) [RFC4949:2007]

2.444 ENGAÑO

Ver:

- *Engaño en comunicaciones*

2.444.1 ENGAÑO

Conjunto de circunstancias como consecuencia del cual una entidad puede acabar dando por ciertos datos que son falsos.

2.444.2 (EN) DECEPTION

(I) A circumstance or event that may result in an authorized entity receiving false data and believing it to be true. (See: authentication.) [RFC4949:2007]

2.445 ENGAÑO EN COMUNICACIONES

Ver:

- *Engaño*

2.445.1 ENGAÑO EN COMUNICACIONES

Transmisión, retransmisión o alteración de unas comunicaciones de forma deliberada para hacer confundir o engañar al receptor.

2.445.2 (EN) COMMUNICATIONS DECEPTION

Deliberate transmission, retransmission, or alteration of communications to mislead an adversary's interpretation of the communications. [CNSSI_4009:2010]

2.445.3 (EN) IMITATIVE COMMUNICATIONS DECEPTION

Introduction of deceptive messages or signals into an adversary's telecommunications signals. See communications deception and manipulative communications deception. [CNSSI_4009:2010]

2.445.4 (EN) MANIPULATIVE COMMUNICATIONS DECEPTION

Alteration or simulation of friendly telecommunications for the purpose of deception. See communications deception and imitative communications deception. [CNSSI_4009:2010]

2.446 ENIGMA

Ver:

- *JADE*
- *PURPLE*

2.446.1 ENIGMA (MÁQUINA)

La máquina Enigma era un mecanismo de cifrado rotativo utilizado tanto para cifrado como para descifrado, ampliamente utilizada de varios modos en Europa desde los tempranos años 1920 en adelante. Su fama se la debe a haber sido adoptada por muchas fuerzas militares de Alemania desde 1930 en adelante. Su facilidad de manejo y su supuesta inviolabilidad fueron las principales razones para su amplio uso. Su cifrado, fue roto, y la lectura de la información que ofrecía en los mensajes que no protegió es a veces reconocida como la causa para acabar al menos un año antes la Segunda Guerra Mundial de lo que hubiera podido ser de otro modo.

http://es.wikipedia.org/wiki/Enigma_%28m%C3%A1quina%29

2.446.2 (EN) ENIGMA

Name for a machine used by the Germans to encrypt and decrypt secret messages in World War II.

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.446.3 (EN) ENIGMA MACHINE

In the history of cryptography, the Enigma was a portable cipher machine used to encrypt and decrypt secret messages. More precisely, Enigma was a family of related electro-mechanical rotor machines comprising a variety of different models.

The Enigma was used commercially from the early 1920s on, and was also adopted by the military and governmental services of a number of nations most famously by Nazi Germany before and during World War II.

The German military model, the Wehrmacht Enigma, is the version most commonly discussed. The machine has gained notoriety because Allied cryptologists were able to decrypt a large number of messages that had been enciphered on the machine. The intelligence gained through this source codenamed ULTRA was a significant aid to the Allied war effort. The exact influence of ULTRA is debated, but a typical assessment is that the end of the European war was hastened by two years because of the decryption of German ciphers.

Although the Enigma cipher has cryptographic weaknesses, it was, in practice, only their combination with other significant factors which allowed codebreakers to read messages: mistakes by operators, procedural flaws, and the occasional captured machine or codebook.

http://en.wikipedia.org/wiki/Enigma_machine

2.447 ENTIDAD

2.447.1 ENTIDAD

Una persona, un grupo, un dispositivo o un proceso. [UNE-71504:2008]

2.447.2 (EN) ENTITY

An individual (person), organization, device or process. [NIST-SP800-57:2007]

2.447.3 (EN) ENTITY

a person, a group, a device or a process. [ISO-19790:2006]

2.447.4 (EN) ENTITY

Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information). [NIST-SP800-27:2004]

2.447.5 (EN) ENTITY

Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information). [NIST-SP800-33:2001]

2.448 ENTIDAD DE CONFIANZA

Ver:

- *Tercera parte de confianza*

2.448.1 ENTIDAD CONFIABLE

Entidad que puede infringir una política de seguridad, ya sea porque ejecuta acciones indebidas o porque no ejecuta las acciones debidas. [X.810:1995]

2.448.2 ENTIDAD CONDICIONALMENTE CONFIABLE

Una entidad que es confiable en el contexto de una política de seguridad, pero que no puede infringir la política de seguridad sin ser detectada. [X.810:1995]

2.448.3 ENTIDAD INCONDICIONALMENTE CONFIABLE

Entidad confiable que puede infringir una política de seguridad sin ser detectada. [X.810:1995]

2.448.4 (EN) TRUSTED ENTITY

An entity that can violate a security policy, either by performing actions which it is not supposed to do, or by failing to perform actions which it is supposed to do. [X.810:1995]

2.448.5 (EN) CONDITIONALLY TRUSTED ENTITY

An entity that is trusted in the context of a security policy, but which cannot violate the security policy without being detected. [X.810:1995]

2.448.6 (EN) UNCONDITIONALLY TRUSTED ENTITY

A trusted entity that can violate a security policy without being detected. [X.810:1995]

2.448.7 (FR) ENTITÉ DE CONFIANCE

entité qui peut violer une politique de sécurité, soit en réalisant des actions qu'elle n'est pas censée accomplir, soit en ne réussissant pas à réaliser des actions qu'elle est censée accomplir. [X.810:1995]

2.448.8 (FR) ENTITÉ DE CONFIANCE CONDITIONNELLE

entité à laquelle il est fait confiance dans le contexte d'une politique de sécurité, mais qui ne peut pas violer la politique de sécurité sans être détectée. [X.810:1995]

2.448.9 (FR) ENTITÉ DE CONFIANCE INCONDITIONNELLE

entité de confiance qui peut violer une politique de sécurité sans être détectée. [X.810:1995]

2.449 ENTIDAD FINAL

Ver:

- *Entidad*

2.449.1 ENTIDAD FINAL

Sujeto del certificado de clave pública que utiliza su clave privada para otros fines distintos que firmar certificados, o titular de certificado de atributo que utiliza sus atributos para obtener acceso a un recurso, o entidad que es una parte confiante. [X.509:2005]

2.449.2 (EN) END ENTITY

Either a public key certificate subject that uses its private key for purposes other than signing certificates, or an attribute certificate holder that uses its attributes to gain access to a resource, or an entity that is a relying party. [X.509:2005]

2.449.3 (FR) ENTITÉ FINALE

il s'agit soit d'un sujet d'un certificat de clé publique qui utilise sa clé privée à d'autres fins que la signature de certificats, soit d'un détenteur de certificat d'attribut qui utilise ses attributs pour accéder à une ressource ou à une entité qui est un participant faisant confiance. [X.509:2005]

2.450 ENTORNO

2.450.1 ENTORNO

Contexto de un desarrollo, operación y mantenimiento de un sistema de información. Incluye procedimientos, condiciones y objetos.

2.450.2 (EN) ENVIRONMENT

Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system. [CNSSI_4009:2010]

2.451 ENTRENAMIENTO (EN SEGURIDAD)

Ver:

- *Concienciación (en seguridad)*

2.451.1 ENTRENAMIENTO (EN SEGURIDAD)

Entrenamiento específico para los responsables de llevar a cabo las funciones de seguridad del sistema. Cada persona se entrena en su misión propia.

2.451.2 (EN) WHAT IS SECURITY TRAINING?

A. Security training strives to produce relevant and needed security knowledge and skills within the workforce. Training supports competency development and helps personnel understand and learn how to perform their security role. Security training provides general security courses that are appropriate and applicable to the entire workforce and offers role-based training that is tailored to the specific needs of each security role. [NIST-SP800-100:2006]

2.452 ENTROPÍA

2.452.1 ENTROPÍA

Valor medio ponderado de la cantidad de información transmitida por un mensaje, no conocido a priori, de una fuente (conjunto) de ellos.

En otras palabras, la entropía de una fuente mide la incertidumbre que, a priori, tiene un observador acerca de la aparición de un mensaje (no conocido previamente) de dicha fuente.

Se mide en bitios y, raramente, en Hartleys (en honor del matemético estadounidense R.V. Hartley, uno de los primeros estudiosos de la teoría de la información).

[Ribagorda:1997]

2.452.2 ENTROPIA

Medida de la impredictibilidad. Se dice que una contraseña tiene mayor entropía cuanto más impredecible sea. Y viceverse, una contraseña fácilmente predecible tiene poca entropía.

2.452.3 (EN) ENTROPY

A measure of the amount of uncertainty that an Attacker faces to determine the value of a secret. Entropy is usually stated in bits. [NIST-SP800-63:2013]

2.452.4 (EN) GUESSING ENTROPY

A measure of the difficulty that an Attacker has to guess the average password used in a system. In this document, entropy is stated in bits. When a password has n-bits of guessing entropy then an Attacker has as much difficulty guessing the average password as in guessing an n-bit random quantity. The Attacker is assumed to know the actual password frequency distribution. [NIST-SP800-63:2013]

2.452.5 (EN) MIN-ENTROPY

A measure of the difficulty that an Attacker has to guess the most commonly chosen password used in a system. In this document, entropy is stated in bits. When a password has n-bits of min-entropy then an Attacker requires as many trials to find a user with that password as is needed to guess an n-bit random quantity. The Attacker is assumed to know the most commonly used password(s). [NIST-SP800:63:2013]

2.453 ENVENENAMIENTO DEL DNS

Ver:

- *Pharming*
- *Secuestro de DNS*
- *Suplantación de DNS*
- *Extensiones de seguridad para el DNS*

2.453.1 ENVENENAMIENTO DEL DNS

Técnica de ataque contra el servicio DNS. Consiste en enviarle información falsa haciéndole creer que procede de una fuente fiable. Si el DNS cae en el engaño, contribuirá a difundir la falsa información.

2.453.2 (EN) CACHE POISONING

Cache poisoning, also called domain name system (DNS) poisoning or DNS cache poisoning, is the corruption of an Internet server's domain name system table by replacing an Internet address with that of another, rogue address. When a Web user seeks the page with that address, the request is redirected by the rogue entry in the table to a different address. At that point, a worm, spyware, Web browser hijacking program, or other malware can be downloaded to the user's computer from the rogue location.

http://whatis.techtarget.com/

2.453.3 (EN) DNS CACHE POISONING

A clever technique that tricks your DNS server into believing it has received authentic information when, in reality, it has been lied to. Why would an attacker corrupt your DNS server's cache? So that your DNS server will give out incorrect answers that provide IP addresses of the attacker's choice, instead of the real addresses. Imagine that someone decides to use the Microsoft Update Web site to get the latest Internet Explorer patch. But, the attacker has inserted phony addresses for update.microsoft.com in your DNS server, so instead of being taken to Microsoft's download site, the victim's browser arrives at the attacker's site and downloads the latest worm.

http://www.watchguard.com/glossary/

2.453.4 (EN) CACHE POISONING

Malicious or misleading data from a remote name server is saved [cached] by another name server. Typically used with DNS cache poisoning attacks.

http://www.sans.org/security-resources/glossary-of-terms/

2.453.5 (EN) DNS CACHE POISONING

An attacker modifies a public DNS cache to cause certain names to resolve to incorrect addresses that the attacker specifies. The result is that client applications that rely upon the targeted cache for domain name resolution will be directed not to the actual address of the specified domain name but to some other address. Attackers can use this to herd clients to sites that install malware on the victim's computer or to masquerade as part of a Pharming attack.

Attack Pattern 142

http://capec.mitre.org/data/index.html

2.454 ENVENENAMIENTO DEL MOTOR DE BÚSQUEDA

Acrónimo: SEP

2.454.1 ENVENENAMIENTO DEL MOTOR DE BÚSQUEDA

Ataque que consiste en manipular los resultados devueltos por un motos de búsqueda de contenidos en la red, redirigiendo al usuario a sitios que contienen software dañino.

2.454.2 (EN) SEARCH ENGINE POISONING

Search Engine Poisoning (SEP) attacks exploit the trust between Internet users and search engines. Attackers deliver bait content for searches to various topics. In this way, users searching for such items are being diverted to malicious content.

ENISA Threat Landscape [Deliverable – 2012-09-28]

2.454.3 (EN) SEARCH ENGINE POISONING (SEP)

Search Engine Poisoning (SEP) attacks manipulate search engines to display search results that contain references to malware-delivering websites. There are a multitude of methods to perform SEP, including taking control of popular websites, using the search engines' "sponsored" links to reference malicious sites to inject HTML code.

http://www.imperva.com/resources/glossary/glossary.html

2.455 EQUIPO AZUL

Ver:

- *Equipo rojo*
- *Equipo blanco*

2.455.1 EQUIPO AZUL

Equipo de personas que se encarga de defender el sistema de información frente a los atacantes (equipo rojo).

2.455.2 (EN) BLUE TEAM

1. The group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team). Typically the Blue Team and its supporters must defend against real or simulated attacks 1) over a significant period of time, 2) in a representative operational context (e.g., as part of an operational exercise), and 3) according to rules established and monitored with the help of a neutral group refereeing the simulation or exercise (i.e., the White Team).

2. The term Blue Team is also used for defining a group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on the Blue Team

findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the customer's cyber security readiness posture. Often times a Blue Team is employed by itself or prior to a Red Team employment to ensure that the customer's networks are as secure as possible before having the Red Team test the systems. [CNSSI_4009:2010]

2.456 EQUIPO BLANCO

Ver:

- *Equipo azul*
- *Equipo rojo*

2.456.1 EQUIPO BLANCO

Equipo de persona que actúan como árbitros en un ejercicio de seguridad entre el equipo rojo (atacante) y el equipo azul (defensa).

2.456.2 (EN) WHITE TEAM

1. The group responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of their enterprise's use of information systems. In an exercise, the White Team acts as the judges, enforces the rules of the exercise, observes the exercise, scores teams, resolves any problems that may arise, handles all requests for information or questions, and ensures that the competition runs fairly and does not cause operational problems for the defender's mission. The White Team helps to establish the rules of engagement, the metrics for assessing results and the procedures for providing operational security for the engagement. The White Team normally has responsibility for deriving lessons-learned, conducting the post engagement assessment, and promulgating results.

2. Can also refer to a small group of people who have prior knowledge of unannounced Red Team activities. The White Team acts as observers during the Red Team activity and ensures the scope of testing does not exceed a pre-defined threshold.

[CNSSI_4009:2010]

2.457 EQUIPO CRIPTOGRÁFICO

Ver:

- *Módulo criptográfico*
- *Dispositivo criptográfico*

2.457.1 EQUIPO CRIPTOGRÁFICO

Equipo en el que se ejecutan las funciones criptográficas (por ejemplo: cifrado, autenticación, generación de claves) (ISO-8732). [Ribagorda:1997]

2.458 EQUIPO DE CIFRA

Ver:

- *Equipo criptográfico*

2.458.1 EQUIPO DE CIFRA

Equipo que tiene implementado mecánica o electrónicamente un algoritmo de cifra que, junto a unas claves, sirve para el cifrado o descifrado de información. [CESID:1997]

2.458.2 (EN) ENCRYPTION EQUIPMENT

Equipment, mechanical or electronic, that implements an encryption or decryption algorithm.

2.459 EQUIPO ROJO

Ver:

- *Equipo azul*
- *Equipo blanco*

2.459.1 EQUIPO ROJO

Un elemento de la organización compuesta por miembros entrenados y educados que proporcionan una capacidad independiente para explorar a fondo las alternativas en los planes y actividades en el contexto del entorno operativo y desde la perspectiva de los adversarios.

2.459.2 (EN) RED TEAM

An organizational element comprised of trained and educated members that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of adversaries and others. [JP2-0:2013]

2.459.3 (EN) RED TEAM

A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. [CNSSI_4009:2010]

2.459.4 (EN) RED TEAM

A structured, iterative process executed by trained, educated and practiced team members that provides commanders an independent capability to continuously challenge plans, operations, concepts, organizations and capabilities in the context of the operational environment and from our partners' and adversaries' perspectives.

http://cyber.law.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas

2.460 ESCALADA DE PRIVILEGIOS

Ver:

- *Cross-zone scripting*

2.460.1 ELEVACIÓN DE PRIVILEGIOS

Proceso mediante el cual el usuario engaña al sistema para que le otorgue derechos no autorizados, usualmente con el propósito de comprometer o destruir el sistema.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.460.2 (EN) PRIVILEGE ESCALATION

A privilege escalation attack is a type of network intrusion that takes advantage of programming errors or design flaws to grant the attacker elevated access to the network and its associated data and applications.

http://searchsecurity.techtarget.com/

2.460.3 (EN) ELEVATION OF PRIVILEGE

When a user (particularly a malicious user) gains more access rights than they normally have.

http://www.getsafeonline.org/

2.460.4 (EN) ELEVATION OF PRIVILEGE

Almost every computer program has some notion of "privilege" built in, meaning, permission to do some set of actions on the system. This permission is granted to individuals based on their ability to present proper credentials (for example, a username and password). Privilege has levels -- for example, a guest account typically has fewer privileges than an administrator account. Many network attacks begin with an attacker obtaining limited privileges on a system, then attempting to leverage those privileges into greater privileges that might ultimately lead to controlling the system. Any attempt to gain greater permissions illicitly (typically, by impersonating a privileged user or otherwise bypassing normal authentication) is considered an elevation of privilege.

http://www.watchguard.com/glossary/

2.460.5 (EN) PRIVILEGE ESCALATION

is the act of exploiting a bug in an application to gain access to resources which normally would have been protected from an application or user. The result is that the application performs actions with a higher security context than intended by the application developer or system administrator.

http://en.wikipedia.org/wiki/Privilege_escalation

2.461 ESCÁNER DE VULNERABILIDADES

Ver:

- *Vulnerabilidad*
- *Evaluación de vulnerabilidad*
- *Análisis de vulnerabilidades*
- *Ataque controlado*
- *Pruebas de penetración*
- *SATAN - Security Administrator Tool for Analyzing Networks*

2.461.1 ESCÁNER DE VULNERABILIDADES

Programa que analiza un sistema buscando vulnerabilidades. Utiliza una base de datos de defectos conocidos y determina si el sistema bajo examen es vulnerable o no.

2.461.2 ANÁLISIS DE SEGURIDAD DE LA RED

Proceso mediante el cual se buscan vulnerabilidades en los sistemas de una entidad de manera remota a través del uso de herramientas manuales o automatizadas. Análisis de seguridad que incluyen la exploración de sistemas internos y externos, así como la generación de informes sobre los servicios expuestos a la red. Los análisis pueden identificar vulnerabilidades en sistemas operativos, servicios y dispositivos que pudieran utilizar personas malintencionadas.

http://es.pcisecuritystandards.org

2.461.3 (EN) NETWORK SECURITY SCAN

Process by which an entity's systems are remotely checked for vulnerabilities through use of manual or automated tools. Security scans that include probing internal and external systems and reporting on services exposed to the network. Scans may identify vulnerabilities in operating systems, services, and devices that could be used by malicious individuals.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.461.4 (EN) VULNERABILITY SCANNER

A vulnerability scanner is a program that performs the diagnostic phase of a vulnerability analysis, also known as vulnerability assessment. Vulnerability analysis defines, identifies, and classifies the security holes (vulnerabilities) in a computer, server, network, or communications infrastructure. In addition, vulnerability analysis can forecast the effectiveness of proposed countermeasures, and evaluate how well they work after they are put into use.

A vulnerability scanner relies on a database that contains all the information required to check a system for security holes in services and ports, anomalies in packet construction, and potential paths to exploitable programs or scripts. Then the scanner tries to exploit each vulnerability that is discovered. This process is sometimes called ethical hacking.

http://searchsoftwarequality.techtarget.com/glossary/

2.461.5 (EN) WEB APPLICATION VULNERABILITY SCANNER

An automated security program that searches for software vulnerabilities within web applications.

http://www.webappsec.org/projects/glossary/

2.461.6 (EN) VULNERABILITY SCANNING

The practice of scanning for and identifying known vulnerabilities of computing systems on a computer network. Since vulnerability scanning is an informationgathering process, when performed by unknown individuals it is considered a prelude to attack.

D. Schweitzer, 2003, Incident Response: Computer Forensics Toolkit

2.461.7 (FR) ANALYSE DE SECURITE DU RESEAU

Processus par lequel les systèmes d'une entité sont vérifiés à distance pour déceler d'éventuelles vulnérabilités à l'aide d'outils manuels ou automatisés. Les analyses de sécurité comprennent la vérification des systèmes internes et externes, ainsi que le rapport sur les services exposés au réseau. Les analyses permettent d'identifier les vulnérabilités des systèmes d'exploitation, des services et des dispositifs susceptibles d'être utilisés par des individus malveillants.

http://fr.pcisecuritystandards.org/

2.462 ESCOLTA

2.462.1 ESCOLTA

1. com. Persona que acompaña a alguien o algo para protegerlo:
   en el atentado murieron cuatro escoltas del general.
2. Conjunto de las personas y los medios utilizados para escoltar a alguien o algo:
   iban como escolta más de tres vehículos todoterreno y un helicóptero.

Diccionario de la lengua española.

2.462.2 (EN) ESCORT

A cleared person, designated by the contractor, who accompanies a shipment of classified material to its destination. The classified material does not remain in the personal possession of the escort but the conveyance in which the material is transported remains under the constant observation and control of the escort. [DoD 5220:2006]

2.463 ESPACIO DE CLAVES

Ver:

- *Clave*
- *Clave criptográfica*

2.463.1 ESPACIO DE CLAVES

Rango de valores que puede tomar loa clave criptográfica de un algoritmo de cifrado. El espacio de claves es propio de cada algoritmo de cifra.

Supuesto que no se conozca ninguna vulnerabilidad intrínseca de un algoritmo, la fortaleza de éste se mide por la cardinalidad de su espacio de claves, que indica su resistencia a un ataque exhaustivo.

[Ribagorda:1997]

2.463.2 ESPACIO DE CLAVES

Rango de todos los valores que puede tomar una clave. [CESID:1997]

2.463.3 (EN) KEY SPACE

(I) The range of possible values of a cryptographic key; or the number of distinct transformations supported by a particular cryptographic algorithm. (See: key length.) [RFC4949:2007]

2.464 ESPACIO INSPECCIONABLE

Ver:

- *TEMPEST*

2.464.1 ESPACIO INSPECCIONABLE

Espacio tridimensional que rodea los equipos que procesan información clasificada, en el que se considera impracticable por el oponente la interceptación de emisiones TEMPEST. Ver zona de control.

2.464.2 (EN) INSPECTABLE SPACE

Three dimensional space surrounding equipment that processes classified and/or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and remove a potential TEMPEST exploitation exists. Synonymous with zone of control. [CNSSI_4009:2010]

2.464.3 (EN) ZONE OF CONTROL

Three dimensional space surrounding equipment that processes classified and/or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and remove a potential TEMPEST exploitation exists. [CNSSI_4009:2010]

2.465 ESP - ENCAPSULATING SECURITY PAYLOAD

Acrónimos: ESP

Ver:

- *IPsec - IP security*
- *AH - Authentication Header*

2.465.1 ESP - ENCAPSULATING SECURITY PAYLOAD

ESP es una cabecera IP para proporcionar a los paquetes IP que viajan por la red servicios de confidencialidad, autenticación del origen, integridad de la conexión, anti-replay y, en cierta medida, inmunidad al análisis de tráfico.

2.465.2 (EN) ENCAPSULATING SECURITY PAYLOAD (ESP)

(I) An Internet protocol [R2406, R4303] designed to provide data confidentiality service and other security services for IP datagrams. (See: IPsec. Compare: AH.) [RFC4949:2007]

2.465.3 (EN) ENCAPSULATING SECURITY PAYLOAD - ESP

an IP-based protocol providing confidentiality services for data. Specifically, ESP provides encryption as a security service to protect the data content of the IP packet. ESP is an Internet standard (RFC 2406). [ISO-18028-4:2005]

2.465.4 (EN) ESP - ENCAPSULATING SECURITY PAYLOAD

The Encapsulating Security Payload (ESP) header is designed to provide a mix of security services in IPv4 and IPv6. ESP may be applied alone, in combination with the IP Authentication Header (AH).

ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality.

http://www.ietf.org/rfc/rfc4303

2.466 ESPECTRO ENSANCHADO

2.466.1 ESPECTRO ENSANCHADO POR SALTO DE FRECUENCIA

El espectro ensanchado por salto de frecuencia (del inglés Frequency Hopping Spread Spectrum o FHSS) es una técnica de modulación en espectro ensanchado en el que la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia sincrónicamente con el transmisor. Los receptores no autorizados escucharán una señal ininteligible. Si se intentara interceptar la señal, sólo se conseguiría para unos pocos bits. Una transmisión en espectro ensanchado ofrece 3 ventajas principales:

1. Las señales en espectro ensanchado son altamente resistentes al ruido y a la interferencia.

2. Las señales en espectro ensanchado son difíciles de interceptar. Una transmisión de este tipo suena como un ruido de corta duración, o como un incremento en el ruido en cualquier receptor, excepto para el que esté usando la secuencia que fue usada por el transmisor.

3. Transmisiones en espectro ensanchado pueden compartir una banda de frecuencia con muchos tipos de transmisiones convencionales con mínima interferencia.

Su principal desventaja es su elevado ancho de banda.

http://es.wikipedia.org/wiki/Espectro_ensanchado_por_salto_de_frecuencia

2.466.2 (EN) FREQUENCY HOPPING

Repeated switching of frequencies during radio transmission according to a specified algorithm, to minimize unauthorized interception or jamming of telecommunications [CNSSI_4009:2010]

2.466.3 (EN) SPREAD SPECTRUM

Telecommunications techniques in which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information. Frequency hopping, direct sequence spreading, time scrambling, and combinations of these techniques are forms of spread spectrum. [CNSSI_4009:2010]

2.467 ESQUEMA DE CLASIFICACIÓN

Ver:

- *Información clasificada*

2.467.1 ESQUEMA DE CLASIFICACIÓN DE DATOS

Un esquema empresarial para clasificar los datos por factores tales como criticidad, sensibilidad y propiedad. [COBIT:2006]

2.467.2 CLASIFICACIÓN DE LA INFORMACIÓN

La Organización dispone de una normativa adecuada para realizar la clasificación y tratamiento de la información atendiendo a la criticidad de la misma según los criterios más adecuados para su actividad. La normativa de seguridad contempla también los aspectos de parámetros, algoritmos, etc. de los elementos orientados a mantener los requisitos de seguridad. [CCN-STIC-404:2006]

2.467.3 PROCESO DE CLASIFICACIÓN / DESCLASIFICACIÓN

Mecanismo definido en la normativa de clasificación a través del cual se asigna / modifica un determinado nivel de clasificación a un documento. Este mecanismo conlleva una serie de acciones de registro indicadas en el procedimiento establecido por la Organización. [CCN-STIC-404:2006]

2.467.4 CLASIFICACIÓN

Asignación de un nivel de sensibilidad (sea de confidencialidad o de integridad) a una información, dispositivo o equipo de tratamiento de la misma.

Atendiendo a la confidencialidad, en ambientes militares es usual definir los niveles de alto secreto, secreto, confidencial y no clasificado.

En España, la Ley de Secretos Oficiales establece sólo dos niveles: confidencial y reservado, estando conferida la potestad para asignar tal clasificación al Gobierno de la Nación y a la Junta de Jefes de Estado Mayor.

[Ribagorda:1997]

2.467.5 GRADO DE CLASIFICACIÓN O NIVEL DE SEGURIDAD

Representación de la sensibilidad de una información mediante la combinación de una clasificación jerárquica y parámetros no jerárquicos. [CESID:1997]

2.467.6 (EN) DATA CLASSIFICATION SCHEME

An enterprisewide shema for classifying data on factors such as criticality, sensitivity and ownership. [COBIT:2006]

2.468 ESQUEMA DE EVALUACIÓN

Ver:

- *Criterios comunes*

- [ITSEM:1993]
- [ITSEC:1991]

2.468.1 ESQUEMA DE EVALUACIÓN

Marco administrativo y regulador bajo el que una autoridad de evaluación aplica los CC en una comunidad específica. [CC:2006]

2.468.2 (EN) EVALUATION SCHEME

the administrative and regulatory framework under which the Common Criteria is applied by an evaluation authority within a specific community. [CC:2006]

2.468.3 (EN) NATIONAL SCHEME

a set of national rules and regulations for evaluation and certification in accordance with the ITSEC and ITSEM. [ITSEM:1993]

2.469 ESTABLECIMIENTO DE CLAVES

Ver:

- *Clave*
- *Clave criptográfica*
- *Negociación de claves*
- *Transporte de claves*
- *Criptografía de clave secreta*

2.469.1 ESPECIFICACIÓN DE CLAVE

Proceso de acuerdo de una clave criptográfica entre dos o más entidades. La especificación incluye la negociación y el transporte (ISO/IEC ISO-11770-3). [Ribagorda:1997]

2.469.2 (EN) KEY ESTABLISHMENT

The process by which cryptographic keys are securely established among cryptographic modules using key transport and/or key agreement procedures. See key distribution. [CNSSI_4009:2010]

2.469.3 (EN) KEY ESTABLISHMENT (ALGORITHM OR PROTOCOL)

1. (I) A procedure that combines the key-generation and key- distribution steps needed to set up or install a secure communication association.

2. (I) A procedure that results in keying material being shared among two or more system entities. [A9042, SP56]

[RFC4949:2007]

2.469.4 (EN) KEY ESTABLISHMENT

A function in the lifecycle of keying material; the process by which cryptographic keys are securely established among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement). [NIST-SP800-57:2007]

2.469.5 (EN) KEY ESTABLISHMENT

the process of making available a shared secret key to one or more entities

NOTE. Key establishment includes key agreement and key transport.

[ISO-19790:2006]

2.469.6 (EN) KEY ESTABLISHMENT

the process of making available a shared secret to one or more entities. Key establishment includes key agreement and key transport. [ISO-15946-3:2002]

2.469.7 (EN) KEY ESTABLISHMENT

the process by which cryptographic keys are securely distributed among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement). [FIPS-140-2:2001]

2.469.8 (EN) KEY ESTABLISHMENT

The process of making available a shared secret key to one or more entities. Key establishment includes key agreement and key transport. [ISO-11770-3:2008]

2.470 ESTEGANÁLISIS

Ver:

- *Esteganografía*

2.470.1 ESTEGANÁLISIS

Detección y revelación de información oculta por medio de técnicas esteganográficas.

2.470.2 (EN) STEGANALYSIS

Steganalysis is the process of detecting and defeating the use of steganography.

http://www.sans.org/security-resources/glossary-of-terms/

2.471 ESTEGANOGRAFÍA

Ver:

- *esteganálisis*

2.471.1 ESTEGANOGRAFÍA

Técnica que consiste en ocultar un mensaje u objeto, dentro de otro, llamado portador, de modo que no se perciba la existencia del mensaje que se quiere ocultar.

A diferencia de la criptografía que se utiliza para cifrar o codificar información de manera que sea ininteligible para un probable intruso, a pesar del conocimiento de su existencia; la esteganografía oculta la información en un portador de modo que no sea advertida el hecho mismo de su existencia y envío.

http://www.inteco.es/glossary/Formacion/Glosario/

2.471.2 ESTEGANOGRAFÍA

Disciplina que estudia los métodos de encubrir mensajes. A diferencia de la criptografía, que trata de ocultar la información contenida en un mensaje, la esteganografía pretende encubrir el propio mensaje.

Ejemplos de métodos esteganográficos lo constituyen la escritura con tintas simpáticas (es decir, invisibles salvo tratamiento adecuado), con micropuntos, con dos fuentes de letras muy similares, etc.

[Ribagorda:1997]

2.471.1 CIFRA ENCUBIERTA O MENSAJE DISIMULADO O ESTEGANOGRAFÍA

Procedimientos encaminados a ocultar la existencia de un mensaje (tintas invisibles, micropunto, disimulación de archivos...). [CESID:1997]

2.471.2 (EN) STEGANOGRAPHY:

The use of encoding techniques for hiding content within other content. For example, there are computer-based steganographic techniques and tools for embedding the contents of a computer file containing engineering diagrams and text into an image file (e.g., a JPG document) such that the existence of the engineering data in the image file is difficult for the observer to detect.

The Tallinn Manual, 2013

2.471.3 (EN) STEGANOGRAPHY

The art, science, and practice of communicating in a way that hides the existence of the communication. [CNSSI_4009:2010]

2.471.4 (EN) STEGANOGRAPHY

(I) Methods of hiding the existence of a message or other data. This is different than cryptography, which hides the meaning of a message but does not hide the message itself. Examples: For classic, physical methods, see [Kahn]; for modern, digital methods, see [John]. (See: cryptology. Compare: concealment system, digital watermarking.) [RFC4949:2007]

2.471.5 (EN) STEGANOGRAPHY

Methods of hiding the existence of a message or other data. This is different than cryptography, which hides the meaning of a message but does not hide the message itself. An example of a steganographic method is "invisible" ink.

http://www.sans.org/security-resources/glossary-of-terms/

2.472 ESTIMAR

Ver:

- *Valoración*
- *Evaluación*

2.472.1 ESTIMAR

Apreciar, poner precio, evaluar algo.

DRAE. Diccionario de la Lengua Española.

2.472.2 (EN) ESTIMATE

To judge tentatively or approximately the value, worth, or significance of ...

To determine roughly the size, extent, or nature of ...

To produce a statement of the approximate cost of ...

Synonyms ESTIMATE, APPRAISE, EVALUATE, VALUE, RATE.

ASSESS mean to judge something with respect to its worth or significance.

ESTIMATE implies a judgment, considered or casual, that precedes or takes the place of actual measuring or counting or testing out <estimated the crowd at two hundred>.

APPRAISE commonly implies the fixing by an expert of the monetary worth of a thing, but it may be used of any critical judgment <having their house appraised>.

EVALUATE suggests an attempt to determine relative or intrinsic worth in terms other than monetary <evaluate a student's work>.

VALUE equals APPRAISE but without implying expertness of judgment <a watercolor valued by the donor at $500>.

RATE adds to ESTIMATE the notion of placing a thing according to a scale of values <a highly rated restaurant>.

ASSESS implies a critical appraisal for the purpose of understanding or interpreting, or as a guide in taking action <officials are trying to assess the damage>.

2.472.3 (EN) ESTIMATE

1. a judgement that you make without having the exact details or figures about the size, amount, cost, etc. of sth

2. a statement of how much a piece of work will probably cost: verb /'est{I}me{I}t/ [often passive] ~ sth (at sth) to form an idea of the cost, size, value etc. of sth, but without calculating it exactly

Oxford Advanced Learner's Dictionary.

2.473 ETIQUETA DE CLASIFICACIÓN

Ver:

- *Información clasificada*
- *Etiqueta de sensibilidad*

2.473.1 ETIQUETA DE CLASIFICACIÓN

Marca asociada a una pieza de información que califica el grado de daño que causaría su revelación a sujetos no autorizados. Puede indicar asimismo las salvaguardas de que debe ser objeto a fin de evitar su revelación no autorizada.

2.473.2 (EN) CLASSIFICATION LABEL

(I) A security label that tells the degree of harm that will result from unauthorized disclosure of the labeled data, and may also tell what countermeasures are required to be applied to protect the data from unauthorized disclosure. Example: IPSO. (See: classified, data confidentiality service. Compare: integrity label.) [RFC4949:2007]

2.474 ETIQUETA DE SEGURIDAD

Ver:

- *Etiqueta de clasificación*
- *Etiqueta de sensibilidad*

2.474.1 ETIQUETA DE SEGURIDAD

1. Marca permanentemente asociada con datos, procesos y/u otros recursos OSI protegidos, que puede ser usada para poner en práctica una política de seguridad (ISO-7498-2).

2. Marca asociada a un objeto que especifica los atributos de seguridad del mismo y la sensibilidad (clasificación) de las informaciones que contiene o trata.

[Ribagorda:1997]

2.474.2 ETIQUETA DE SEGURIDAD

Marca realizada implícita o explícitamente sobre cualquier tipo de recurso o sistema que nombra o designa los atributos de seguridad del mismo. [CESID:1997]

2.474.3 ETIQUETA DE SEGURIDAD

Marca vinculada a un recurso (que puede ser una unidad de datos) que denomina o designa los atributos de seguridad de dicho recurso. [ISO-7498-2:1989]

2.474.4 (EN) SECURITY LABEL

Hardware, firmware, and software elements of a trusted computing base implementing the reference monitor concept. Security kernel must mediate all accesses, be protected from modification, and be verifiable as correct. [CNSSI_4009:2010]

(en) Security Label

Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein [NIST-SP800-18:2006]

2.474.5 (EN) SECURITY LABEL

The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource. [ISO-7498-2:1989]

2.474.6 (FR) ÉTIQUETTE DE SÉCURITÉ

Marque liée à une ressource dénommant ou désignant les attributs de sécurité de cette ressource (cette ressource peut être une unité de données). [ISO-7498-2:1989]

2.475 ETIQUETA DE SENSIBILIDAD

Ver:

- *Sensibilidad*
- *Etiqueta de clasificación*

2.475.1 ETIQUETA DE SENSIBILIDAD

Sinónimo de "etiqueta de clasificación".

2.475.2 (EN) SENSITIVITY LABEL

Information representing elements of the security label(s) of a subject and an object. Sensitivity labels are used by the trusted computing base (TCB) as the basis for mandatory access control decisions. See security label. [CNSSI_4009:2010]

2.475.3 (EN) SENSITIVITY LABEL

(D) Synonym for "classification label". [RFC4949:2007]

2.475.4 (EN) SENSITIVITY LABEL

A piece of information that represents the security level of an object and that describes the sensitivity (e.g., classification) of the data in the object. Sensitivity labels are used by the TCB as the basis for mandatory access control decisions. [TCSEC:1985]

2.476 EVALUACIÓN

2.476.1 EVALUACIÓN

Proceso para determinar hasta qué punto una entidad, procedimiento o actuación satisface los objetivos previstos. En gestión de riesgos, es la parte en la que se evalúa la efectividad de las medidas de tratamiento del riesgo.

2.476.2 (EN) EVALUATION

process of examining, measuring and/or judging how well an entity, procedure, or action has met or is meeting stated objectives

Annotation: Evaluation is the step in the risk management cycle that measures the effectiveness of an implemented risk management option.

DHS Risk Lexicon, September 2008

2.477 EVALUACIÓN DE LA SEGURIDAD

2.477.1 EVALUACIÓN DE LA SEGURIDAD

Verificación de que un elemento de seguridad se ajusta a lo especificado.

2.477.2 (EN) SECURITY ASSESSMENT

Verification of a security deliverable against a security standard using the corresponding security method to establish compliance and determine the security assurance. a) The last stage of the product evaluation process [ISO/IEC 14598-1]. [ISO-15443-1:2005]

2.478 EVALUACIÓN DE RESPETO A LA PRIVACIDAD

Ver:

- *Privacidad*

2.478.1 (EN) PRIVACY IMPACT ASSESSMENT

An analysis of how information is handled:

(i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;

(ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and

(iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. [OMB Memorandum 03-22]

[NIST-SP800-53:2013]

2.478.2 (EN) PRIVACY IMPACT ASSESSMENT (PIA)

An analysis of how information is handled 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. [CNSSI_4009:2010]

2.479 EVALUACIÓN DE RIESGOS

Ver:

- *Riesgo*
- *Apreciación de los riesgos*
- *Criterios de evaluación de riesgos*

2.479.1 EVALUACIÓN DEL RIESGO

Proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables.

[UNE-ISO GUÍA 73:2010]

NOTA La evaluación del riesgo ayuda a la toma de decisiones sobre el tratamiento del riesgo.

[UNE-ISO/IEC 27000:2014]

2.479.1 EVALUACIÓN DEL RIESGO

Proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables.[UNE Guía 73:2010]

2.479.2 EVALUACIÓN DE RIESGOS

Proceso de comparación de los riesgos analizados frente a los criterios de evaluación de riesgos, para así determinar la importancia de los riesgos para la organización. [UNE-71504:2008]

2.479.3 (EN) RISK EVALUATION

process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable [ISO Guide 73:2009]

[ISO/IEC 27000:2014]

2.479.4 (EN) RISK EVALUATION

process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable [ISO Guide 73:2009]

2.479.5 (FR) ÉVALUATION DU RISQUE

processus de comparaison des résultats de l'analyse du risque avec les critères de risque afin de déterminer si le risque et/ou son importance sont acceptables ou tolérables [ISO Guide 73:2009]

2.479.1 (FR) ÉVALUATION DES RISQUES

Les étapes initiales de la gestion des risques. Analyser la valeur des actifs par rapport aux métiers, identifier les menaces envers ces actifs et évaluer comment chaque actif est vulnérable à ces menaces. L'évaluation du risque peut être quantitative (basée sur des données chiffrées) ou qualitative. [ITIL:2007]

2.480 EVALUACIÓN DE SEGURIDAD

Ver:

- *Estimar*
- *Evaluación*
- *Criterios comunes*
- *Esquema de evaluación*
- *Certificación*
- *Acreditación*

2.480.1 EVALUAR

1. Señalar el valor de algo.

2. Estimar, apreciar, calcular el valor de algo.

DRAE. Diccionario de la Lengua Española.

2.480.2 EVALUACIÓN DE LA SEGURIDAD

Proceso de comprobación de que un producto o Sistema satisface las características de seguridad que proclama tener. Dicho proceso consiste en el examen detallado con el fin de encontrar una posible vulnerabilidad y confirmar el nivel de seguridad establecido. El examen se realiza de acuerdo a un procedimiento o metodología determinado y siguiendo unos criterios de evaluación perfectamente definidos y establecidos. [CCN-STIC-101:2005]

2.480.3 EVALUACIÓN

1. Valoración de un sistema o producto de tecnologías de la información respecto de un criterio de evaluación definido (ITSEC).

2. Medida de la confianza que puede depositarse en un Objeto de Evaluación, consistente en una referencia a su Objetivo de Seguridad, un nivel de evaluación establecido por la valoración de la corrección de su implementación y la consideración de su efectividad en el contexto de su uso operativo real o propuesto, y un valor confirmado de la mínima solidez de sus mecanismos de seguridad en el contexto de su uso.

[Ribagorda:1997]

2.480.4 EVALUACIÓN

Estudio técnico detallado, efectuado por un organismo acreditado, de los aspectos de seguridad de un criptosistema, a fin de comprobar qué requisitos de seguridad cumple y hasta qué nivel, asegurando la inexistencia de aspectos ocultos de su funcionamiento y de que éste no es corruptible. (v. Validación, Verificación).

Como consecuencia de una evaluación el órgano de certificación asigna una acreditación y extiende un certificado. (v. Información sensible).

[CESID:1997]

2.480.5 (EN) EVALUATION

(I) Assessment of an information system against defined security criteria (for example, against the TCSEC or against a profile based on the Common Criteria). (Compare: certification.) [RFC4949:2007]

2.480.6 (EN) EVALUATION

assessment of a PP, an ST or a TOE, against defined criteria.

PP - Protection Profile

ST - Security Target

TOE - Target of Evaluation

[CC:2006]

2.480.7 (EN) SECURITY EVALUATION

An evaluation done to assess the degree of trust that can be placed in systems for the secure handling of sensitive information. [IRM-5239-8:1995]

2.480.8 (EN) EVALUATION OF SECURITY

the assessment of an IT system or product against defined evaluation criteria. [ITSEC:1991]

2.480.9 (EN) PP EVALUATION

assessment of a PP against defined criteria.

PP - Protection Profile

[CC:2006]

2.480.10 (EN) ST EVALUATION

assessment of an ST against defined criteria.

ST - Security Target

[CC:2006]

2.480.11 (EN) TOE EVALUATION

assessment of a TOE against defined criteria.

TOE - Target of Evaluation

[CC:2006]

2.481 EVALUACIÓN DE VULNERABILIDAD

Ver:

- *Vulnerabilidad*
- *Escáner de vulnerabilidades*
- *Análisis de vulnerabilidades*

2.481.1 EVALUACIÓN DE VULNERABILIDAD

1. Aspecto de la valoración de la efectividad de un Objeto de Evaluación; es decir, si las vulnerabilidades conocidas en el mismo pueden comprometer un la práctica su seguridad, tal como está especificada en el Objetivo de Seguridad (ITSEC).

2. Valoración de un programa o sistema para determinar su susceptibilidad a pérdidas o uso indebido.

[Ribagorda:1997]

2.481.2 (EN) VULNERABILITY ASSESSMENT

an aspect of the assessment of the effectiveness of a Target of Evaluation, namely whether known vulnerabilities in that Target of Evaluation could in practice compromise its security as specified in the security target. [ITSEC:1991]

2.482 EVALUADOR

Ver:

- *Evaluación*

2.482.1 EVALUADOR

Entidad independiente que lleva a cabo una evaluación.

2.482.2 (EN) EVALUATOR

the independent person or organisation that performs an evaluation. [ITSEC:1991]

2.483 EVENTO

Ver:

- *Detección de incidentes*
- *Gestión de eventos de seguridad*
- *Incidente*

2.483.1 SUCESO

Ocurrencia o cambio de un conjunto particular de circunstancias. [UNE-ISO GUÍA 73:2010]

NOTA 1 Un suceso puede ser único o repetirse, y se puede deber a varias causas.

NOTA 2 Un suceso puede consistir en algo que no se llega a producir.

NOTA 3 Algunas veces, un suceso se puede calificar como un "incidente" o un "accidente".

[UNE-ISO/IEC 27000:2014]

2.483.1 SUCESO

Ocurrencia o cambio de un conjunto particular de circunstancias. [UNE Guía 73:2010]

2.483.2 SUCESO DE SEGURIDAD DE LA INFORMACIÓN

Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de los controles o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.

[UNE-ISO/IEC 27000:2014]

2.483.3 EVENTO

(Operación del Servicio) Un cambio de estado significativo para la cuestión de un Elemento de Configuración o un Servicio de TI.

El término Evento también se usa como Alerta o notificación creada por un Servicio de TI, Elemento de Configuración o herramienta de Monitorización. Los Eventos requieren normalmente que el personal de Operaciones de TI tome acciones, y a menudo conllevan el registro de Incidentes.

[ITIL:2007]

2.483.4 (EN) EVENT

a thing that happens, especially sth important.

Oxford Advanced Learner's Dictionary.

2.483.1 (EN) EVENT

occurrence or change of a particular set of circumstances [ISO Guide 73:2009]

NOTE 1: An event can be one or more occurrences, and can have several causes.

NOTE 2: An event can consist of something not happening.

NOTE 3: An event can sometimes be referred to as an “incident” or “accident”.

[ISO/IEC 27000:2014]

2.483.2 (EN) INFORMATION SECURITY EVENT

identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant [ISO-27000:2014]

2.483.1 (EN) EVENT

Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring. [CNSSI_4009:2010]

2.483.2 (EN) EVENT

occurrence or change of a particular set of circumstances. [ISO Guide 73:2009]

2.483.3 (EN) EVENT

Something that happens at a specific place and/or time. [RiskIT-PG:2009]

2.483.4 (EN) EVENT TYPE

For the purpose of IT risk management, one of three possible sorts of events:

- threat event
- loss event
- vulnerability event

[RiskIT-PG:2009]

2.483.5 (EN) SECURITY EVENT

(I) An occurrence in a system that is relevant to the security of the system. (See: security incident.) [RFC4949:2007]

2.483.6 (EN) EVENT

(Service Operation) A change of state which has significance for the management of a Configuration Item or IT Service.

The term Event is also used to mean an Alert or notification created by any IT Service, Configuration Item or Monitoring tool. Events typically require IT Operations personnel to take actions, and often lead to Incidents being logged.

[ITIL:2007]

2.483.7 (EN) INFORMATION SECURITY EVENT

An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant. [ISO/IEC TR ISO-18044:2004] [ISO-18028-1:2006] [ISO-18044:2004]

2.483.8 (EN) EVENT

An instantaneous occurrence that changes the global status of an object. This status change may be persistent or temporary, thus allowing for surveillance, monitoring, and performance measurement functionality, etc. Events may or may not generate reports; they may be spontaneous or planned; they may trigger other events or may be triggered by one or more other events. [X.790:1995]

2.483.9 (EN) SECURITY RELEVANT EVENT

Any event that attempts to change the security state of the system, (e.g., change discretionary access controls, change the security level of the subject, change user password, etc.). Also, any event that attempts to violate the security policy of the system, (e.g., too many attempts to login, attempts to violate the mandatory access control limits of a defice, attempts to downgrade a file, etc.). [TCSEC:1985]

2.483.10 (EN) BLACK SWAN EVENT

An event that is highly improbable and therefore likely to end up at the bottom of the list of priorities to address.

“The Black Swan: The Impact of the Highly Improbable” Nassim Taleb, 2007.

2.483.11 (FR) ÉVÉNEMENT

occurrence ou changement d'un ensemble particulier de circonstances. [ISO Guide 73:2009]

2.483.12 (FR) ÉVÉNEMENT

(Exploitation de Services) Un changement d'état ayant de l'importance pour la gestion d'un élément de configuration ou un service des TI.

Le terme "événement" est aussi employé pour désigner une alerte ou une notification créée par un service des TI, un élément de configuration ou un outil de surveillance. Les événements requièrent habituellement du personnel d'exploitation des TI qu'il initie une action ce qui conduit le plus souvent à la journalisation d'incidents.

[ITIL:2007]

2.483.13 (FR) EVENEMENT LIE A LA SECURITE DE L´INFORMATION

un incident lié à la sécurité de l'information est indiqué par un ou plusieurs événement(s) de sécurité de l'information indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information. [ISO-18044:2004]

2.484 EVIDENCIA

Ver:

- *Prueba*
- *Criterios comunes*

2.484.1 EVIDENCIA

Certeza clara y manifiesta de la que no se puede dudar.

DRAE. Diccionario de la Lengua Española.

2.484.2 EVIDENCIA

Información que, por sí misma, o en combinación con otra información, se utiliza para probar algo.

Nota: una evidencia por sí misma no necesariamente prueba la certeza o existencia de algo; pero ayuda a establecer la prueba.

2.484.3 (EN) EVIDENCE

the facts, signs or objects that make you believe that sth is true.

Oxford Advanced Learner's Dictionary.

2.484.4 (EN) EVIDENCE

directly measurable characteristics of a process and/or product that represent objective, demonstrable proof that a specific activity satisfies a specified requirement. [ISO-21827:2007]

2.484.5 (EN) CM EVIDENCE

everything that may be used to establish confidence in the correct operation of the CM system, e.g., CM output, rationales provided by the developer, observations, experiments or interviews made by the evaluator during a site visit.

CM - Configuration Management

[CC:2006]

2.484.6 (EN) EVIDENCE

Information either by itself, or in conjuction with other information, is used to establish proof about an event or action.

NOTE. Evidence does not necessarily prove truth or existence of something (see proof) but contributes to establish proof.

[ISO-13888-1:2004]

2.485 EXPLOIT

Ver:

- *Vulnerabilidad*

2.485.1 EXPLOIT

Un tipo de software, un fragmento de datos, o una secuencia de comandos que aprovecha un fallo o una vulnerabilidad en el sistema de un usuario para provocar un comportamiento no deseado o

imprevisto. Las acciones que se suelen realizar la violenta toma de control de un sistema, una escalada de privilegios o un ataque de denegación de servicio.

http://www.inteco.es/glossary/Formacion/Glosario/

2.485.2 EXPLOIT

Código malicioso escrito con vistas a utilizar un error del sistema y poder así tomar control de la máquina. [CCN-STIC-435:2006]

2.485.3 (EN) EXPLOIT KITS

Exploit kits are ready-to-use software packages that "automate" cybercrime. They use mostly drive-by download attacks whose malicious code is injected in compromised websites. These attacks exploit multiple vulnerabilities in browsers and browser plug-ins26. Moreover, exploit kits use a plethora of channels to deliver malware and infect unsuspected web users. An important characteristic of exploit kits is their ease of use (usually through a web interface) allowing people without technical knowledge to purchase and easily use them.

ENISA Threat Landscape [Deliverable – 2012-09-28]

2.485.4 (EN) EXPLOIT

An exploit is a technique or software code (often in the form of scripts) that takes advantage of a vulnerability or security weakness in a piece of target software.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/attack/590-BSI.html

2.485.5 (EN) EXPLOIT

A program or technique that takes advantage of a vulnerability in software and that can be used for breaking security, or otherwise attacking a host over the network.

http://www.symantec.com/avcenter/refa.html

2.485.6 (EN) EXPLOIT

Code that takes advantage of a vulnerability to gain access to data and control over a system.

https://www.nsslabs.com/reports/threat-definitions

2.486 EXPOSICIÓN

Ver:

- *Vulnerabilidad*

2.486.1 EXPOSICIÓN

Se dice cuando información sensible queda expuesta al acceso de entidades no autorizadas. El hecho puede ser accidental o deliberado.

2.486.2 (EN) EXPOSURE

(I) A type of threat action whereby sensitive data is directly released to an unauthorized entity. (See: unauthorized disclosure.)

Usage: This type of threat action includes the following subtypes:

- "Deliberate Exposure": Intentional release of sensitive data to an unauthorized entity.
- "Scavenging": Searching through data residue in a system to gain unauthorized knowledge of sensitive data.
- "Human error": /exposure/ Human action or inaction that unintentionally results in an entity gaining unauthorized knowledge of sensitive data. (Compare: corruption, incapacitation.)
- "Hardware or software error": /exposure/ System failure that unintentionally results in an entity gaining unauthorized knowledge of sensitive data. (Compare: corruption, incapacitation.)

[RFC4949:2007]

2.486.3 (EN) EXPOSURE

An information security "exposure" is a system configuration issue or a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network.

CVE considers a configuration issue or a mistake an exposure if it does not directly allow compromise but could be an important component of a successful attack, and is a violation of a reasonable security policy.

http://www.cve.mitre.org/

2.487 EXPOSICIÓN ANUAL A UN RIESGO

Acrónimos: ALE

Ver:

- *Riesgo*

2.487.1 EXPOSICIÓN ANUAL A UN RIESGO

Producto del daño previsto, en unidades monetarias, producido por un ataque, multiplicado por el número previsto de ocurrencias al año del citado ataque. [Ribagorda:1997]

2.487.2 (EN) ANNUALISED LOSS EXPECTANCY

The Annualised Loss Expectancy (ALE) is the expected monetary loss that can be expected for an asset due to a risk over a one year period.

2.488 EXTENSIBLE AUTHENTICATION PROTOCOL

Acrónimos: EAP

Ver:

- http://www.ietf.org/rfc/rfc3748

2.488.1 EXTENSIBLE AUTHENTICATION PROTOCOL

Protocolo marco que soporta diversos modos de autenticación remota: contraseñas, sistemas reto-respuesta, etc.

2.488.2 (EN) EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

(I) An extension framework for PPP that supports multiple, optional authentication mechanisms, including cleartext passwords, challenge-response, and arbitrary dialog sequences. [R3748] (Compare: GSS-API, SASL.) [RFC4949:2007]

2.488.3 (EN) EXTENSIBLE AUTHENTICATION PROTOCOL

EAP an authentication protocol supported by RADIUS and standardised by the IETF in RFC 2284. [ISO-18028-4:2005]

2.488.4 (EN) EXTENSIBLE AUTHENTICATION PROTOCOL

A framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences.

2.489 EXTENSIONES DE SEGURIDAD PARA EL DNS (DNSSEC)

Ver:

- *Envenenamiento del DNS*
- *Pharming*
- *Secuestro de DNS*
- *Suplantación de DNS*
- *RFC 4033 - DNS Security Introduction and Requirements*
- *RFC 4034 - Resource Records for the DNS Security Extensions*
- *RFC 4035 - Protocol Modifications for the DNS Security Extensions*

2.489.1 EXTENSIONES DE SEGURIDAD PARA EL SISTEMA DE NOMBRES DE DOMINIO

Las Extensiones de seguridad para el Sistema de Nombres de Dominio (del inglés Domain Name System Security Extensions, o DNSSEC) es un conjunto de especificaciones de la Internet Engineering Task Force (IETF) para asegurar cierto tipo de información proporcionada por el sistema de nombre de dominio (DNS) que se usa en el protocolo de Internet (IP). Se trata de un conjunto de extensiones al DNS que proporcionan a los clientes DNS (o resolvers) la autenticación del origen de datos DNS, la negación autenticada de la existencia e integridad de datos, pero no disponibilidad o confidencialidad.

http://es.wikipedia.org/wiki/Domain_Name_System_Security_Extensions

2.489.2 (EN) DOMAIN NAME SYSTEM SECURITY EXTENSION (DNSEC)

DNSSEC was designed to protect internet resolvers (clients) from forged DNS data, such as that created by DNS. All answers in DNSSEC are digitally signed. By checking the digital signature, a DNS resolver is able to check if the information is identical (correct and complete) to the information on the authoritative DNS server. While protecting IP addresses is the immediate concernfor many users, DNSSEC can protect other information such as general-purpose cryptographic certificates stored in CERT records in the DNS.

DNSSEC is intended to protectthe end user from DNS protocol attacks. Unfortunately the current DNS is vulnerable to so-called spoofing or poisoning attacks, whichcan fool a cache into accepting false DNS data. Various man-in-the-middle attacks are also possible. The (DNSSEC) is not designed to end these attacks, but to make them detectable by the end user.

FY 2013 - Chief Information Officer - Federal Information Security Management Act - ReportingMetrics, November 30, 2012

2.489.3 DOMAIN NAME SYSTEM SECURITY EXTENSIONS (DNSSEC)

The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extensions to DNS which provide to DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality.

http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions

2.490 EXTERNALIZACIÓN

2.490.1 CONTRATAR EXTERNAMENTE

Establecer un acuerdo mediante el cual una organización externa realiza parte de una función o proceso de una organización.

[UNE-ISO/IEC 27000:2014]

2.490.2 (EN) OUTSOURCE

make an arrangement where an external organization performs part of an organization’s function or process [ISO/IEC 27000:2014]

2.490.3 (EN) EXTERNAL INFORMATION SYSTEM (OR COMPONENT)

An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. [CNSSI_4009:2010]

2.490.4 (EN) EXTERNAL INFORMATION SYSTEM SERVICE

An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. [CNSSI_4009:2010]

2.490.5 (EN) EXTERNAL NETWORK

A network not controlled by the organization. [CNSSI_4009:2010]

2.491 EXTORSIÓN EN LA RED

Ver:

- *Denegación de servicio*

2.491.1 EXTORSIÓN

Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.

DRAE. Diccionario de la Lengua Española.

2.491.2 (EN) EXTORT

to make sb give you sth by threatening them

Oxford Advanced Learner's Dictionary.

2.491.3 (EN) CYBEREXTORTION

Cyberextortion is a form of online criminal activity in which the Web site, e-mail server, or computer infrastructure of an enterprise is subjected repeatedly to denial of service or other attacks by crackers (malicious hackers), who then demand money in return for promising to stop the attacks. Such crackers are called cyberextortionists. As the number of enterprises that rely on the Internet for their business has increased, opportunities for cyberextortionists have exploded.

http://searchsoftwarequality.techtarget.com/glossary/

2.492 FAILOVER

Ver:

- *Alta disponibilidad*

2.492.1 FAILOVER

Configuración de equipos en la que un segundo equipo de hace cargo de las funciones del principal en caso de detención de éste. De esta forma, el servicio no se ve interrumpido.

2.492.2 (EN) FAILOVER

The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system. [NIST-SP800-53:2013]

2.492.3 (EN) FAILOVER

The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system. [CNSSI_4009:2010]

2.492.4 (EN) FAILOVER

A configuration that allows a secondary machine to take over in the event of a stoppage in the first machine, thus allowing normal use to return or continue.

http://www.watchguard.com/glossary/

2.493 FALSO NEGATIVO

2.493.1 FALSO NEGATIVO

Error producido cuando el sistema diagnostica como actividad normal un ataque. [CCN-STIC-432:2006]

2.493.2 FALSA ACEPTACIÓN

Error de un sistema de autenticación biométrico que autoriza el acceso a un impostor. Su probabilidad de ocurrencia (probabilidad de falsa aceptación) es una de sus características significativas.

Habitualmente, estos sistemas pueden ajustarse para variar esta probabilidad dentro de un amplio margen. Desgraciadamente, cuanto más pequeña sea la probabilidad de falsa aceptación, mayor es la probabilidad de falso rechazo.

[Ribagorda:1997]

2.493.3 (EN) FALSE REJECTION

In biometrics, the instance of a security system failing to verify or identify an authorized person. It does not necessarily indicate a flaw in the biometric system; for example, in a fingerprint-based system, an incorrectly aligned finger on the scanner or dirt on the scanner can result in the scanner misreading the fingerprint, causing a false rejection of the authorized user. [CNSSI_4009:2010]

2.493.4 (EN) FALSE REJECTION RATE (FRR)

The measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. A system's false rejection rate typically is stated as the ratio of the number of false rejections divided by the number of identification attempts. [CNSSI_4009:2010]

2.493.5 (EN) FALSE NEGATIVE

An instance in which an intrusion detection and prevention technology fails to identify malicious activity as being such. [NIST-SP800-94:2007]

2.493.6 (EN) FALSE NEGATIVE

An instance in which a security tool intended to detect a particular threat fails to do so. [NIST-SP800-83:2005]

2.494 FALSO POSITIVO

2.494.1 FALSO POSITIVO

Error producido cuando el sistema diagnostica como ataque una actividad normal. [CCN-STIC-432:2006]

2.494.2 FALSO RECHAZO

Error de un sistema de autenticación biométrico que deniega el acceso a un individuo legítimamente autorizado. Su probabilidad de ocurrencia (probabilidad de falso rechazo) es una de sus características significativas.

Habitualmente, estos sistemas pueden ajustarse para variar esta probabilidad dentro de un amplio margen. Desgraciadamente, cuanto más pequeña sea la probabilidad de falso rechazo, mayor es la probabilidad de falsa aceptación.

[Ribagorda:1997]

2.494.3 (EN) FALSE ACCEPTANCE

In biometrics, the instance of a security system incorrectly verifying or identifying an unauthorized person. It typically is considered the most serious of biometric security errors as it gives unauthorized users access to systems that expressly are trying to keep them out. [CNSSI_4009:2010]

2.494.4 (EN) FALSE ACCEPTANCE RATE (FAR)

The measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's false acceptance rate typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts. [CNSSI_4009:2010]

2.494.5 (EN) FALSE POSITIVE

An instance in which an intrusion detection and prevention technology incorrectly identifies benign activity as being malicious. [NIST-SP800-94:2007]

2.494.6 (EN) FALSE POSITIVE

An instance in which a security tool incorrectly classifies benign content as malicious. [NIST-SP800-83:2005]

2.494.7 (EN) FALSE POSITIVE

This occurs when the system classifies an action as anomalous (a possible intrusion) when it is a legitimate action.

http://www.csoonline.com/glossary/

2.494.8 (EN) FALSE REJECTS

False Rejects are when an authentication system fails to recognize a valid user.

http://www.sans.org/security-resources/glossary-of-terms/

2.495 FEAL - FAST DATA ENCIPHERMENT ALGORITHM

Acrónimos: FEAL

2.495.1 FEAL (FAST DATA ENCIPHERMENT ALGORITHM)

Familia de algoritmos en bloque diseñada por A. Akihiro y S. Miyaguchi para NTT Japón. Transforma en N vueltas, de modo similar al DES, una entrada de 64 bits. Es importante en el desarrollo de técnicas criptoanalíticas [CESID:1997]

2.495.2 (EN) FEAL

(O) A family of symmetric block ciphers that was developed in Japan; uses a 64-bit block, keys of either 64 or 128 bits, and a variable number of rounds; and has been successfully attacked by cryptanalysts. [Schn] [RFC4949:2007]

2.495.3 (EN) FEAL (FAST DATA ENCIPHERMENT ALGORITHM)

The Fast Data Encipherment Algorithm is a family of algorithms that maps 64 plaintext to 64-bit ciphertext blocks under a 64-bit secret key. It is similar to DES but with a far simpler ffunction. It was designed for speed and simplicity, making it suitable for less complex microprocessors (e.g. smartcards).

2.496 FIABILIDAD

2.496.1 FIABILIDAD

fiabilidad

1. f. Cualidad de fiable.

fiable

1. adj. Dicho de una persona: Que es digna de confianza.

2. adj. Que ofrece seguridad o buenos resultados. Mecanismo fiable. Método fiable.

3. adj. Creíble, fidedigno, sin error. Datos fiables.

DRAE. Diccionario de la Lengua Española.

2.496.2 FIABILIDAD

Propiedad relativa a la consistencia en el comportamiento y en los resultados deseados. [UNE-ISO/IEC 27000:2014]

2.496.3 (EN) RELIABILITY

property of consistent intended behaviour and results [ISO/IEC 27000:2014]

2.496.4 (EN) RELIABILITY

(I) The ability of a system to perform a required function under stated conditions for a specified period of time. (Compare: availability, survivability.) [RFC4949:2007]

2.496.5 (FR) FIABILITÉ

La propriété qu'un système IT se maintienne sur une période de temps donnée conforme, doté d'un comportement prévu et digne de confiance quant aux opérations qu'il effectue.

Threat and Risk Assessment Working Guide, Government of Canada, 1999

2.497 FICHEROS OCULTOS DE CONTRASEÑAS

Ver:

- *Contraseña*

2.497.1 FICHEROS OCULTOS DE CONTRASEÑAS

Se trata de un fichero que almacena las contraseñas para autenticar a los usuarios del sistema. Como característica singular, estos ficheros permanecen fuera del alcance de los usuarios, previniendo su uso como fuente de información para descubrir contraseñas.

2.497.2 (EN) SHADOW PASSWORD FILES

A system file in which encryption user password are stored so that they aren't available to people who try to break into the system.

http://www.sans.org/security-resources/glossary-of-terms/

2.498 FILTRADO DE PAQUETES

Ver:

- *Router con filtros*
- *Filtrado de paquetes con estado*

2.498.1 FILTRADO DE ENTRADA/SALIDA

Filtrado realizado en los puntos de comunicación del perímetro de la Organización con el exterior. [CCN-STIC-400:2006]

2.498.2 (EN) PACKET FILTER

A firewall technology that makes decisions based on information contained in an IP packet header, such as service type, source, or destination.

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.499 FILTRADO DE PAQUETES CON ESTADO

Ver:

- *Router con filtros*
- *Filtrado de paquetes*

2.499.1 INSPECCIÓN COMPLETA

También denominada “dynamic packet filtering” (filtrado dinámico de paquetes). Firewall que, al realizar un seguimiento del estado de las conexiones de la red, proporciona una seguridad mejorada. Al estar programado para distinguir los paquetes legítimos de las diversas conexiones, el firewall permitirá solamente aquellos paquetes que coinciden con una conexión establecida, y rechazará a todos los demás.

http://es.pcisecuritystandards.org

2.499.2 STATEFUL FIREWALL

La condición "stateful" se refiere a la capacidad de guardar registro de las conexiones establecidas y establecer reglas de filtrado en base a la correcta secuencia de las mismas. [CCN-STIC-641:2006]

2.499.3 FILTRADO DE PAQUETES CON INFORMACIÓN DE ESTADO

Filtrado de paquetes que memoriza las comunicaciones a nivel de transporte previamente establecidas. [CCN-STIC-400:2006]

2.499.4 FILTRADO DE PAQUETES SIN INFORMACIÓN DE ESTADO

Filtrado de paquetes básico que trata los paquetes de manera individual sin tener en cuenta información del estado de la comunicación. [CCN-STIC-400:2006]

2.499.5 FILTRADO DE PAQUETES CON INFORMACIÓN DE ESTADO E INSPECCIÓN

Filtrado de paquetes que además de memorizar las comunicaciones a nivel de transporte, inspecciona el contenido de los paquetes utilizando decodificadores de protocolo para así interpretar los flujos dinámicos de comunicaciones asociados. [CCN-STIC-400:2006]

2.499.6 (EN) STATEFUL INSPECTION:

Also called “dynamic packet filtering,” it is a firewall capability that provides enhanced security by keeping track of communications packets. Only incoming packets with a proper response (“established connections”) are allowed through the firewall.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.499.7 (EN) STATEFUL PACKET FILTERING

"Packet filtering" means using a firewall to examine where each packet comes from (by IP source address), where it's going (IP destination), and what port it's using. This information helps the firewall determine whether to allow or deny the packet's passage through your network. In stateful inspection, the firewall also examines more of the packet's delivery information and its conditions, including what port the packet is using, and maintains a sense of context. For example, a packet might arrive looking like a valid Reply packet, but if you never issued a Request, through dynamic packet filtering the firewall can sense that this is a spurious packet, and deny it.

http://www.watchguard.com/glossary/

2.499.8 (EN) STATEFUL INSPECTION

A technology developed by Check Point Software Technologies that accesses an analysis all data derived from all communications layers. The state and context data is stored and updated dynamically, providing virtual session information for tracking connectionless protocols. The cumulative data are used to decide on a appropriate action.

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.499.9 (EN) STATEFUL INSPECTION

Also referred to as dynamic packet filtering. Stateful inspection is a firewall architecture that works at the network layer. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection examines not just the header information but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination.

http://www.sans.org/security-resources/glossary-of-terms/

2.499.10 (FR) CONTRÔLE AVEC ÉTAT

Également nommé «filtrage des paquets dynamique». Capacité de pare-feu qui fournit une sécurité renforcée en gardant la trace du statut des connexions de réseau. Programmé pour distinguer les paquets légitimes pour diverses connexions, uniquement les paquets contenant une connexion établie seront autorisés par le pare-feu, les autres seront rejetés.

http://fr.pcisecuritystandards.org/

2.500 FILTRADO DE PAQUETES POR RUTA DE ORIGEN

2.500.1 FILTRADO DE PAQUETES POR RUTA DE ORIGEN

Tecnología que se utiliza en los routers IP para tratar de evitar la suplantación de la dirección de origen, que se utiliza a menudo por ataques DenialOfService. El router analiza la dirección origen de los paquetes recibidos y la compara con la información de encaminamiento de que dispone. Si hay una diferencia en la interfaz de recepción y de envío, desecha el paquete.

2.500.2 (EN) RPF – REVERSE PATH FILTERING

Reverse Path Filtering (RPF) is a technology that is used on IP routers to try and prevent source address spoofing, which is often used for Denial-Of-Service attacks. RPF works by checking the source IP of each packet received on an interface against the routing table. If the best route for the source IP address does not use the same interface that the packet was received on the packet is dropped. There are some situations where this feature will obviously not be the desired behaviour and will need to be disabled. In general if you are not multi-homed then enabling RPF on your router will not be a problem.

http://wiki.wlug.org.nz/ReversePathFiltering

2.501 FILTRO DE ENTRADA

Ver:

- *Router con filtros*

2.501.1 FILTRADO DE INGRESO

Método que permite filtrar el tráfico entrante de una red, de modo que sólo el tráfico explícitamente autorizado pueda ingresar a la red.

http://es.pcisecuritystandards.org

2.501.2 FILTRADO DE CAMINO INVERSO

Técnica de filtrado del tráfico entrante basada en la verificación de la dirección origen de los paquetes con la tabla de enrutamiento para comprobar que dicha red es alcanzable por dicho interfaz de entrada. [CCN-STIC-400:2006]

2.501.3 (EN) INGRESS FILTERING

(I) A method [R2827] for countering attacks that use packets with false IP source addresses, by blocking such packets at the boundary between connected networks. [RFC4949:2007]

2.501.4 (EN) INGRESS FILTERING

Method of filtering inbound network traffic such that only explicitly allowed traffic is permitted to enter the network.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.501.5 (FR) FILTRAGE D'ENTRÉE

Méthode de filtrage du trafic entrant du réseau, de sorte que seul le trafic explicitement autorisé ait l'autorisation d'entrer sur le réseau.

http://fr.pcisecuritystandards.org/

2.502 FILTRO DE SALIDA

2.502.1 FILTRADO DE EGRESO

Método que permite filtrar el tráfico saliente de una red, de modo que sólo el tráfico explícitamente autorizado pueda salir de la red.

http://es.pcisecuritystandards.org

2.502.2 (EN) EGRESS FILTERING:

Method of filtering outbound network traffic such that only explicitly allowed traffic is permitted to leave the network.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.502.3 (FR) FILTRAGE DE SORTIE

Méthode de filtrage du trafic sortant du réseau, de sorte que seul le trafic explicitement autorisé ait l'autorisation de quitter le réseau.

http://fr.pcisecuritystandards.org/

2.503 FIPS

2.503.1 FIPS

Normas de nivel federal de los EEUU. Cubren aspectos de las tecnologías de la información buscando un nivel común de calidad y unas ciertas garantías de interoperabilidad.

2.503.2 (EN) FEDERAL INFORMATION PROCESSING STANDARD (FIPS)

A standard for adoption and use by Federal agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability. [CNSSI_4009:2010]

2.504 FIPS 140-2

Ver:

- http://csrc.nist.gov/cryptval/140-2.htm

2.504.1 FIPS PUB 140-2

Security Requirements for Cryptographic Modules

2.504.2 (EN) FIPS PUB 140-2

Security Requirements for Cryptographic Modules

2.504.3 (EN) FIPS 140-2 CERTIFICATION

FIPS 140-2 Certification describes US government requirements that IT products must meet for Sensitive But Unclassified (SBU) use. The standard was published by the National Institute of Standards and Technology (NIST), has been adopted by the Communication Security Establishment (CSE) of Canada, and is likely to be adopted by the financial community through the American National Standards Institute (ANSI).

FIPS 140-2 defines the security requirements that must be satisfied by a cryptographic module used in a security system protecting unclassified information within IT systems. There are four levels of security: Level 1 is the lowest and Level 4 is the highest. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be deployed. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include basic design and documentation, module interfaces, authorized roles and services, physical security, software security, operating system security, key management, cryptographic algorithms, electromagnetic interference/electromagnetic compatibility (EMI/EMC), and selftesting.

http://www.spectralogic.com/index.cfm?fuseaction=home.displayFile&DocID=1235

2.505 FIRMA CIEGA

Ver:

- *Firma digital*

2.505.1 FIRMA CIEGA

Protocolo mediante el que se obtiene un documento en claro firmado digitalmente, sin que el signatario tenga medio de conocerlo en el momento de estampar su firma.

Constituye la base de otros protocolos criptográficos, como el de votación electrónica o el del dinero electrónico.

[Ribagorda:1997]

2.505.2 FIRMA CIEGA

Protocolo de firma digital en el que una entidad solicita a otra la firma de un mensaje, a partir de la cual puede obtener otra firma del firmante válida para otro mensaje desconocido para él. [CESID:1997]

2.505.3 (EN) BLIND SIGNATURE

Blind signature schemes allow a person to get a message signed by another party without revealing any information about the message to the other party.

http://www.rsasecurity.com/rsalabs/faq/

2.506 FIRMA DE UN VIRUS

Ver:

- *Virus*

2.506.1 FIRMA DE UN VIRUS

Ristra de caracteres característica del código de un virus, o conjunto de ellos, que permite su identificación.

Se distingue la firma de contaminación, cadena de caracteres que el virus usa para reconocer los programas que ya ha contaminado; y la firma de diagnóstico insertos en el código del virus. A diferencia de la primera firma, elegida por el autor del virus, la segunda queda a la elección del producto antivirus.

[Ribagorda:1997]

2.506.2 (EN) SIGNATURE

The 'fingerprint' that is used by anti-virus software to detect an infection.

http://www.getsafeonline.org/

2.506.3 (FR) SIGNATURE (VIRUS)

Portion de code contenu dans un programme de type virus, vers, chevaux de Troie et malwares en général permettant son identification par des logiciels anti-virus. Les logiciels anti-virus ont longtemps utilisé la signature des virus comme mécanisme permettant de leur détection sur un système, cependant de nombreux virus se transforment, comme sont en mesure de le faire les virus polymorphes, cette technique de reconnaissance des virus ne suffit plus aujourd'hui.

http://www.cases.public.lu/functions/glossaire/

2.507 FIRMA DIGITAL

Ver:

- *Criptografía de clave pública*
- *Algoritmo Diffie-Hellman*
- *DSA - Digital Signature Algorithm*
- *Criptografía de curvas elípticas*
- *El Gamal*
- *RSA - Rivest, Shamir y Adelman*
- *Firma electrónica*

2.507.1 FIRMA DIGITAL

Datos añadidos a un conjunto de datos, o transformación de éstos, que permite al receptor probar el origen e integridad del conjunto de datos recibidos, así como protegerlos contra falsificaciones; por ejemplo, del propio receptor (ISO-7498-2). [Ribagorda:1997]

2.507.2 FIRMA DIGITAL

Datos añadidos o transformación criptográfica de una unidad de datos que prueba al receptor de dicha información la fuente y/o integridad de los datos contra posibles falsificaciones. Es un mecanismo de seguridad, e incluye el proceso de firmado y el de verificación de la firma. [CESID:1997]

2.507.3 FIRMA DIGITAL CON APÉNDICE

Protocolo criptográfico de firma digital que requiere el mensaje original como entrada del algoritmo de verificación. [CESID:1997]

2.507.4 FIRMA DIGITAL CON RECUPERACIÓN DE MENSAJE

Protocolo de firma digital que no requiere el mensaje original como entrada del algoritmo de verificación. En este caso, el mensaje original se recupera a partir de la propia firma. [CESID:1997]

2.507.5 FIRMA DIGITAL NO NEGABLE

Protocolo de firma digital en el que la verificación de la firma requiere la participación del firmante. [CESID:1997]

2.507.6 FIRMA DIGITAL

Datos añadidos a una unidad de datos, o transformación criptográfica (véase criptografía) de una unidad de datos que permite al recibiente de la unidad de datos probar la fuente y la integridad de la unidad de datos y proteger contra la falsificación (por ejemplo, por el recibiente). [ISO-7498-2:1989]

2.507.7 (EN) DIGITAL SIGNATURE

Cryptographic process used to assure data object originator authenticity, data integrity, and time stamping for prevention of replay.

[CNSSI_4009:2010]

2.507.8 (EN) DIGITAL SIGNATURE

1. (I) A value computed with a cryptographic algorithm and associated with a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity. (See: data origin authentication service, data integrity service, signer. Compare: digitized signature, electronic signature.)

2. (O) "Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient." [ISO-7498-2]

[RFC4949:2007]

2.507.9 (EN) DIGITAL SIGNATURE

The result of a cryptographic transformation of data that, when properly implemented with supporting infrastructure and policy, provides the services of:

- origin authentication
- data integrity, and
- signer non-repudiation.

[NIST-SP800-57:2007]

2.507.10 (EN) DIGITAL SIGNATURE

data appended to, or a cryptographic transformation of a data unit that allows the recipient of the data unit to prove the origin and integrity of the data unit and protect against forgery (e.g., by the recipient). [ISO-19790:2006]

2.507.11 (EN) DIGITAL SIGNATURE

The result of a cryptographic transformation of data which, when properly implemented, provides the services of:

- origin authentication
- data integrity, and
- signer non-repudiation.

[FIPS-140-2:2001]

2.507.12 (EN) DIGITAL SIGNATURE

A data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the origin and integrity of the data unit and protect the sender and the recipient of the data unit against forgery by third parties, and the sender against forgery by the recipient. [ISO-11770-3:2008]

2.507.13 (EN) DIGITAL SIGNATURE

Data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. [ISO-7498-2:1989]

2.507.14 (FR) SIGNATURE NUMÉRIQUE

Données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon (par le destinataire, par exemple). [ISO-7498-2:1989]

2.508 FIRMA ELECTRÓNICA

Ver:

- *Firma electrónica avanzada*
- *Firma electrónica cualificada*
- *Firma digital*

2.508.1 FIRMA ELECTRÓNICA

«firma electrónica», los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar; [PE-CONS 60/14]

2.508.2 FIRMA ELECTRÓNICA

conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante. [Ley-59:2003]

2.508.3 (EN) ELECTRONIC SIGNATURE

'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign; [PE-CONS 60/14]

2.508.4 (EN) ELECTRONIC SIGNATURE

The process of applying any mark in electronic form with the intent to sign a data object. See also digital signature. [CNSSI_4009:2010]

2.508.5 (EN) ELECTRONIC SIGNATURE

means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

[Directive-1999/93/EC:1999]

2.508.6 (FR) SIGNATURE ÉLECTRONIQUE

"signature électronique", des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer; [PE-CONS 60/14]

2.508.7 (FR) SIGNATURE (ÉLECTRONIQUE / NUMÉRIQUE)

Résultat d'une fonction mathématique dite de hachage permettant de garantir l'authenticité de l'expéditeur et de garantir l'intégrité de l'information échangée.

http://www.cases.public.lu/functions/glossaire/

2.509 FIRMA ELECTRÓNICA AVANZADA

Ver:

- *Firma electrónica*
- *Firma electrónica cualificada*

2.509.1 FIRMA ELECTRÓNICA AVANZADA

«firma electrónica avanzada», la firma electrónica que cumple los requisitos contemplados en el artículo 26;

Artículo 26 -- Requisitos para firmas electrónicas avanzadas

Una firma electrónica avanzada cumplirá los requisitos siguientes:

a) estar vinculada al firmante de manera única;

b) permitir la identificación del firmante;

c) haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y

d) estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

[PE-CONS 60/14]

2.509.2 FIRMA ELECTRÓNICA AVANZADA

La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control. [Ley-59:2003]

2.509.3 (EN) ADVANCED ELECTRONIC SIGNATURE

'advanced electronic signature' means an electronic signature which meets the requirements set out in Article 26;

Article 26 Requirements for advanced electronic signatures

An advanced electronic signature shall meet the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

[PE-CONS 60/14]

2.509.4 (EN) ADVANCED ELECTRONIC SIGNATURE

Advanced electronic signature means an electronic signature which meets the following requirements:

- it is uniquely linked to the signatory;
- it is capable of identifying the signatory;
- it is created using means that the signatory can maintain under his sole control; and
- it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

[Directive-1999/93/EC:1999]

2.509.5 (FR) SIGNATURE ÉLECTRONIQUE AVANCÉE

"signature électronique avancée", une signature électronique qui satisfait aux exigences énoncées à l'article 26:

Article 26 Exigences relatives à une signature électronique avancée

Une signature électronique avancée satisfait aux exigences suivantes:

a) être liée au signataire de manière univoque;

b) permettre d'identifier le signataire;

c) avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif; et

d) être lié aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

[PE-CONS 60/14]

2.510 FIRMA ELECTRÓNICA CUALIFICADA

Ver:

- *Firma electrónica*

2.510.1 FIRMA ELECTRÓNICA CUALIFICADA

«firma electrónica cualificada», una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica; [PE-CONS 60/14]

2.510.2 CERTIFIADO CUALIFICADO DE FIRMA ELECTRÓNICA

«certificado cualificado de firma electrónica», un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I; [PE-CONS 60/14]

2.510.3 (EN) QUALIFIED ELECTRONIC SIGNATURE

'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures; [PE-CONS 60/14]

2.510.4 (EN) QUALIFIED CERTIFICATE FOR ELECTRONIC SIGNATURE

'qualified certificate for electronic signature' means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I; [PE-CONS 60/14]

2.510.5 (FR) SIGNATURE ÉLECTRONIQUE QUALIFIÉE

"signature électronique qualifiée", une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique; [PE-CONS 60/14]

2.510.6 (FR) CERTIFICAT QUALIFIE DE SIGNATURE ELECTRONIQUE

"certificat qualifié de signature électronique", un certificat de signature électronique, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'annexe I; [PE-CONS 60/14]

2.511 FIRMA ELECTRÓNICA RECONOCIDA

Ver:

- *Firma electrónica*
- *Firma electrónica avanzada*
- *Firma electrónica cualificada*
- *Dispositivo de creación de firma*

2.511.1 FIRMA ELECTRÓNICA RECONOCIDA

firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

[Ley-59:2003]

2.512 FIRMANTE

Ver:

- *Firma electrónica*

2.512.1 FIRMANTE

El firmante es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa. [Ley-59:2003]

2.512.2 (EN) SIGNATORY

means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents.

[Directive-1999/93/EC:1999]

2.513 FIRST - FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS

Acrónimos: FIRST

Ver:

- *CERT - Equipo de reacción rápida ante incidentes informáticos*

2.513.1 FIRST - FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS

Foro internacional de organismos de respuesta a incidentes de seguridad.

2.513.2 (EN) FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST)

(N) An international consortium of CSIRTs (e.g., CIAC) that work together to handle computer security incidents and promote preventive activities. (See: CSIRT, security incident.) [RFC4949:2007]

2.514 FISMA - FEDERAL INFORMATION SECURITY MANAGEMENT ACT

Acrónimos: FISMA

2.514.1 FISMA

Legislación de los EEU que define un marco holístico para proteger la información y los sistemas de información gubernamentales frente a amenazas naturales o de origen humano.

2.514.2 (EN) FISMA

The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002.

http://whatis.techtarget.com/

2.515 FLAW

Ver:

- *Bug*
- *Defecto (en programas)*

2.515.1 FLAW

Defecto en un programa a nivel de arquitectura o diseño. Estos defectos pueden no ser evidentes examinando únicamente el código fuente.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/risk/248-BSI.html

2.515.2 (EN) FLAW

Error of commission, omission, or oversight in an information system that may allow protection mechanisms to be bypassed. [CNSSI_4009:2010]

2.515.3 (EN) FLAW (DESIGN)

A software security defect at the architecture or design level. Flaws may not be apparent given only source code of a software system.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/risk/248-BSI.html

2.515.4 (EN) FLAWS

Flaws are software problems that exist in the software design. A flaw may or may not represent a vulnerability in the underlying software. Mitigating a flaw typically involves significantly more effort than simply modifying a few lines of code. The problem does not lie solely in the implementation; the underlying design is flawed, and therefore, any implementation that follows the design would contain the flaw. For instance, performing sensitive business logic in an untrusted client application is a design flaw that cannot be mitigated by a simple measure such as modifying array bounds.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/attack/590-BSI.html

2.516 FORMAL

Ver:

- *Informal*
- *Semiformal*
- *Criterios comunes*

2.516.1 FORMAL

Expreso, preciso, determinado.

DRAE. Diccionario de la Lengua Española.

2.516.2 (EN) FORMAL

expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts. [CC:2006]

2.517 FORTALEZA CRIPTOGRÁFICA

2.517.1 FORTALEZA CRIPTOGRÁFICA

Una cifra, relacionada con la cantidad de trabajo requerido para violar un algoritmo o dispositivo criptográfico. Es frecuente expresar la fortaleza de un sistema de cifra en bits: 80, 112, 128, 192, 512,

2.517.2 (EN) SECURITY STRENGTH

(Also bits of security)

A number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system. In this Recommendation, security strength is specified in bits and is a specific value from the set {80, 112, 128, 192, 256}. [NIST-SP800-57:2007]

2.518 FORTIFICAR

Ver:

- *Bastión*

- *Bastionado*

2.519 FRASE DE ACCESO

Ver:

- *Contraseña*
- http://en.wikipedia.org/wiki/Passphrase

2.519.1 FRASE DE ACCESO

Frase larga (por ejemplo, de 80 caracteres) pero fácil de recordar por el usuario, que realiza las mismas funciones de autenticación que una contraseña, con la ventaja de ser más difícil de conjeturar. [Ribagorda:1997]

2.519.2 (EN) PASSPHRASE

A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security. Passphrases are often used to control both access to, and operation of, cryptographic programs and systems. Passphrases are particularly applicable to systems that use the passphrase as an encryption key. The origin of the term is by analogy with "password". The modern concept of passphrases is believed to have been invented by Sigmund N. Porter (1) in 1982.

http://en.wikipedia.org/wiki/Passphrase

2.520 FRAUDE DE IDENTIDAD

Ver:

- *Identidad*
- *Impostura*
- *Robo de identidades*

2.520.1 FRAUDE DE IDENTIDAD

Acto delictivo basado en la usurpación de la identidad de otra persona.

La mayoría de los fraudes de identidad se realizan con ayuda de ordenadores.

2.520.2 (EN) IDENTITY FRAUD

Any offence involving the misuse of a personal identity. The majority of identity crime is committed with the help of computers. [CSS NZ:2011]

2.520.3 (EN) IDENTITY FRAUD/THEFT

The exploitation by malevolent third parties of unwarranted access to clients' or consumers' identities. Often the result of lax data security or privacy measures.

http://cyber.law.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas

2.521 FUGA, PÉRDIDA

2.521.1 MEMORIA PERDIDA

Se dice cuando un programa o proceso solicita recursos de memoria; pero no los libera, quedando inútiles recursos que pudieran ser valiosos. La consecuencia suele ser que el sistema agota los recursos insensatamente.

2.521.2 (EN) MEMORY LEAK

Memory Leak means the fact that an action uses memory which is never released. It results in a security issue because repeating the action will consume all the memory. A usual consequence is Denial of Service.

http://www.securitylex.org/glossary

2.522 FUNCIÓN DE VERIFICACIÓN CRIPTOGRÁFICA

Ver:

- *Código de autenticación de mensajes*

2.522.1 FUNCIÓN DE VERIFICACIÓN CRIPTOGRÁFICA

Función que obtiene una información realizando un proceso criptográfico en la unidad de datos (ISO-7498-2).

Es término sinónimo de "función resumen".

[Ribagorda:1997]

2.522.2 VALOR DE COMPROBACIÓN CRIPTOGRÁFICO

Información que se obtiene realizando una transformación criptográfica (véase criptografía) sobre una unidad de datos.

NOTA. El valor de comprobación puede obtenerse en uno o más pasos y es el resultado de una función matemática de la clave y una unidad de datos. Suele utilizarse para verificar la integridad de una unidad de datos.

[ISO-7498-2:1989]

2.522.3 (EN) CRYPTOGRAPHIC CHECK-VALUE

Information which is derived by performing a cryptographic transformation (see cryptography) on the data unit.

NOTE. The derivation of the check-value may be performed in one or more steps and is a result of a mathematical function of the key and a data unit. It is usually used to check the integrity of a data unit.

[ISO-7498-2:1989]

2.522.4 (FR) VALEUR DE CONTRÔLE CRYPTOGRAPHIQUE

Information obtenue en réalisant une transformation cryptographique sur une unité de données.

Remarque. La valeur de contrôle peut être obtenue en une ou plusieurs étapes et résulte d'une fonction mathématique utilisant la clé et une unité de données. Elle permet de vérifier l'intégrité d'une unité de données.

[ISO-7498-2:1989]

2.523 FUNCIÓN IRREVERSIBLE

Ver:

- *Algoritmo irreversible*

2.523.1 FUNCIÓN UNIDIRECCIONAL

Función (matemática) f que es fácil de calcular, pero que para un valor y en la gama es difícil de calcular para hallar un valor x en el dominio de modo que f(x) = y. Puede haber unos pocos valores y para los cuales hallar x no sea fácil computacionalmente. [X.509:2005]

2.523.2 FUNCIÓN IRREVERSIBLE

1. Función matemática que es fácilmente computable, pero cuya inversa es computacionalmente intratable. (ISO/IEC ISO-10181-2).

2. Función matemática, f, que es fácil de calcular, pero para la cual dado un valor cualquiera, y, perteneciente a su rango es computacionalmente muy difícil encontrar un valor, x, en su dominio tal que f(x) = y. Quizás haya unos pocos valores de y para los cuales encontrar x no sea computacionalmente difícil (ISO/IEC 9594-2, ITU-T X.509).

[Ribagorda:1997]

2.523.3 FUNCIÓN IRREVERSIBLE CON TRAMPA (TRAPDOOR ONE-WAY FUNCTION)

Función fácil de calcular, pero cuya inversa es computacionalmente inviable de obtener salvo conocimiento de una información privilegiada.

Estas funciones constituyen la base de las técnicas criptográficas asimétricas. En este caso, la información privilegiada la constituye la clave privada.

[Ribagorda:1997]

2.523.4 FUNCIÓN DE UN SOLO SENTIDO

Función matemática fácil de calcular en un sentido, pero muy difícil en el sentido contrario. [CESID:1997]

2.523.5 FUNCIÓN DE UN SOLO SENTIDO CON TRAMPA

Función de un solo sentido en el que conociendo una determinada información es fácil de calcular en ambos sentidos. [CESID:1997]

2.523.6 FUNCIÓN UNIDIRECCIONAL

Función (matemática) cuyo cálculo es fácil pero que, cuando se conoce un resultado, no es factible, mediante cálculo, hallar cualquiera de los valores que pueden haber sido suministrados para obtenerlo. [X.810:1995]

2.523.7 (EN) ONE-WAY FUNCTION

(I) "A (mathematical) function, f, [that] is easy to compute, but which for a general value y in the range, it is computationally difficult to find a value x in the domain such that f(x) = y. There may be a few values of y for which finding x is not computationally difficult." [X509] [RFC4949:2007]

2.523.8 (EN) ONE-WAY FUNCTION

A (mathematical) function f which is easy to compute, but which for a general value y in the range, it is computationally difficult to find a value x in the domain such that f(x) = y. There may be a few values y for which finding x is not computationally difficult. [X.509:2005]

2.523.9 (EN) ONE-WAY FUNCTION

A function with the property that it is easy to compute the output for a given input but it is computationally infeasible to find for a given output an input which maps to this output. [ISO-11770-3:2008]

2.523.10 (EN) ONE-WAY FUNCTION

A (mathematical) function that is easy to compute but, when knowing a result, it is computationally infeasible to find any of the values that may have been supplied to obtain it. [X.810:1995]

2.523.11 (FR) FONCTION NON RÉVERSIBLE

fonction mathématique facile à calculer, mais qui, pour une valeur quelconque y du domaine image, il est difficile de trouver une valeur x du domaine source telle que f(x) = y. Il peut exister un nombre réduit de valeurs de y pour lesquelles le calcul de x est trivial. [X.509:2005]

2.523.12 (FR) FONCTION UNIDIRECTIONNELLE

fonction (mathématique) qu'il est facile de calculer mais pour laquelle, lorsque le résultat est connu, il n'est pas possible de trouver, de façon informatique, n'importe laquelle des valeurs qui auraient pu être fournies pour obtenir celui-ci. [X.810:1995]

2.524 FUNCIÓN RESUMEN

Ver:

- *Hash code*
- *Valor resumen*
- *Hash*

2.524.1 FUNCIÓN HASH O FUNCIÓN RESUMEN (DIGEST)

Función de un solo sentido que calcula, a partir de una cadena de bits de longitud arbitraria, otra, aparentemente aleatoria, de longitud fija.

2.524.2 FUNCIÓN DE HASHING CRIPTOGRÁFICO

Proceso que vuelve ilegibles los datos de titulares de tarjetas convirtiendo los datos en un resumen de mensaje de longitud fija mediante la Criptografía sólida. La función de hashing criptográfico es una función (matemática) en la cual un algoritmo conocido toma un mensaje de longitud arbitraria como entrada y produce un resultado de longitud fija (generalmente denominado “código hash” o “resumen de mensaje”). Una función de hash criptográfico debe tener las siguientes propiedades:

(1) Que no se pueda determinar informáticamente la entrada original si sólo se tiene el código hash,

(2) Que no se puedan hallar informáticamente dos entradas que generen el mismo código hash.

En el contexto de las PCI DSS, la función de hash criptográfico se debe aplicar a todo el PAN para que se considere que el código hash es ilegible. Se recomienda que los datos de titulares de tarjetas en valores hash incluyan un valor de entrada (por ejemplo, un valor de "sal") en la función de hashing criptográfico para reducir o disminuir la efectividad de los ataques de las tablas rainbow computadas previamente (consulte Variable de entrada).

http://es.pcisecuritystandards.org

2.524.3 FUNCIÓN DE TROCEO

Función (matemática) que hace corresponder valores de un dominio grande (posiblemente muy grande) con una gama más pequeña. La función de troceo es "buena" cuando los resultados de la aplicación de la función a un (gran) conjunto de valores en el dominio se distribuyen uniformemente (y aparentemente al azar) en la gama. [X.509:2005]

2.524.4 FUNCIÓN RESUMEN

1. Función matemática que transforma valores de un conjunto de valores más pequeño. (ISO/IEC ISO-10181-2).

Una "buena" función resumen hará que los valores transformados se distribuyan uniformemente (y aparentemente de modo aleatorio) sobre su rango (ISO/IEC 9594-8, ITU-T X.509).

2. Función resistente a colisiones que transforma una cadena arbitraria de bits en otra cadena de bits de longitud fija (ISO/IEC ISO-10118-1).

[Ribagorda:1997]

2.524.5 FUNCIÓN HASH O FUNCIÓN RESUMEN (DIGEST)

Función de un solo sentido que calcula, a partir de una cadena de bits de longitud arbitraria, otra, aparentemente aleatoria, de longitud fija. [CESID:1997]

2.524.6 FUNCIÓN DE CÁLCULO DE CLAVE

Función (matemática) que transforma los valores de un conjunto de valores (posiblemente muy) grande en una gama de valores más pequeña. [X.810:1995]

2.524.7 FUNCIÓN DE CÁLCULO DE CLAVE UNIDIRECCIONAL

Función (matemática) que es a la vez una función unidireccional y una función de cálculo de clave. [X.810:1995]

2.524.8 (EN) HASH FUNCTION

1. (I) A function H that maps an arbitrary, variable-length bit string, s, into a fixed-length string, h = H(s) (called the "hash result"). For most computing applications, it is desirable that given a string s with H(s) = h, any change to s that creates a different string s' will result in an unpredictable hash result H(s') that is, with high probability, not equal to H(s).

2. (O) "A (mathematical) function which maps values from a large (possibly very large) domain into a smaller range. A 'good' hash function is such that the results of applying the function to a (large) set of values in the domain will be evenly distributed (and apparently at random) over the range." [X509]

[RFC4949:2007]

2.524.9 (EN) HASH FUNCTION

A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:

- (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and
- (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.

[NIST-SP800-57:2007]

2.524.10 (EN) HASH FUNCTION

A (mathematical) function which maps values from a large (possibly very large) domain into a smaller range. A "good" hash function is such that the results of applying the function to a (large) set of values in the domain will be evenly distributed (and apparently at random) over the range. [X.509:2005]

2.524.11 (EN) HASH-FUNCTION

function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties:

- it is computationally infeasible to find for a given output, an input which maps to this output;
- it is computationally infeasible to find for a given input, a second input which maps to the same output

NOTE. Computational feasibility depends on the specific security requirements and environment.

[ISO-10118-1:2000]

2.524.12 (EN) HASH FUNCTION

A (mathematical) function that maps values from a (possibly very) large set of values into a smaller range of values. [X.810:1995]

2.524.13 (EN) ONE-WAY HASH FUNCTION

A (mathematical) function that is both a one-way function and a hash function. [X.810:1995]

2.524.14 (EN) HASHING:

Process of rendering cardholder data unreadable by converting data into a fixed-length message digest via Strong Cryptography. Hashing is a (mathematical) function in which a non-secret algorithm takes any arbitrary length message as input and produces a fixed length output (usually called a “hash code” or “message digest”). A hash function should have the following properties:

(1) It is computationally infeasible to determine the original input given only the hash code,

(2) It is computationally infeasible to find two inputs that give the same hash code.

In the context of PCI DSS, hashing must be applied to the entire PAN for the hash code to be considered rendered unreadable. It is recommended that hashed cardholder data includes a salt value as input to the hashing function (see Salt).

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.524.15 (FR) FONCTION DE HACHAGE

fonction (mathématique) qui fait correspondre un argument pris dans un domaine étendu (éventuellement très étendu) à une valeur appartenant à un domaine plus réduit. Une "bonne" fonction de hachage est telle que l'application de la fonction à un ensemble (étendu) d'arguments du premier domaine fournira des valeurs réparties de manière égale (apparemment aléatoire) dans le second domaine. [X.509:2005]

2.524.16 (FR) FONCTION DE HACHAGE

fonction (mathématique) qui fait correspondre les valeurs d'un grand ensemble (potentiellement très grand) de valeurs à une gamme plus réduite de valeurs. [X.810:1995]

2.524.17 (FR) FONCTION DE HACHAGE UNIDIRECTIONNELLE

fonction (mathématique) qui est à la fois une fonction unidirectionnelle et une fonction de hachage. [X.810:1995]

2.524.18 (FR) HACHAGE

Processus qui consiste à rendre des données de titulaire de carte illisibles en les convertissant en un message condensé de longueur fixe par le biais d’une cryptographie performante. Le hachage est une fonction unilatérale (mathématique) dans laquelle un algorithme non secret acquiert en

entrée un message de longueur aléatoire et produit une sortie de longueur fixe (généralement appelé «code de hachage» ou «empreinte cryptographique»). Une fonction de hachage doit avoir les propriétés suivantes:

(1) Il doit être impossible de déterminer, à l'aide de l'informatique, une entrée initiale donnée avec uniquement le code de hachage,

(2) Il doit être impossible de trouver, à l'aide de l'informatique, deux entrées donnant le même code de hachage.

Dans le cadre de lanorme PCI DSS, le hachage doit être appliqué à la totalité du PAN entier pour que le code de hachage soit considéré comme illisible. Il est recommandé d'inclure une entrée variable à la fonction de hachage (par exemple, un «sel») pour les données de titulaire de carte hachées afin de réduire ou de vaincre l'efficacité des tableaux d'attaque arc-en-ciel précalculés (voir variable d'entrée).

http://fr.pcisecuritystandards.org/

2.524.19 (FR) HACHAGE

Une fonction de hachage permet de construire l'empreinte d'un ensemble de données par un mécanisme prédéterminé. Ce mécanisme est unidirectionnel, c'est-à-dire que deux données différentes produisent toujours deux empreintes différentes. Les algorithmes SHA-1 et MD5 sont parmis les fonctions de hachage les plus fréquemment utilisées.

http://www.cases.public.lu/functions/glossaire/

2.524.20 (FR) FONCTION DE HACHAGE

Fonction non-réversible qui associe un ensemble de chaînes de caractères arbitraires à un ensemble de chaînes d'octets de longueur fixe. Une fonction de hachage résistant à la collision possède la propriété selon laquelle il est impossible de construire, par un calcul sur ordinateur, des données d'entrées distinctes associées aux mêmes données de sortie. [ISO-11568-4:2007]

2.525 FUNCTIONAL_REQUIREMENT

Ver:

- *Garantía*
- *Criterios comunes*

2.525.1 (EN) SECURITY FUNCTIONAL REQUIREMENT

Functional specification of the security functions to be implemented to contribute to covering one or more security objectives for the target system. [EBIOS:2005]

2.525.2 (FR) EXIGENCE FONCTIONNELLE DE SÉCURITÉ

Spécification fonctionnelle des fonctions de sécurité à mettre en œuvre afin de participer à la couverture d'un ou plusieurs objectifs de sécurité portant sur le système-cible. [EBIOS:2005]

2.526 GARANTÍA

Ver:

- *Garantía de la información*
- *Criterios comunes*

2.526.1 GARANTÍA

Seguridad o certeza que se tiene sobre algo.

De garantía. Que ofrece confianza.

DRAE. Diccionario de la Lengua Española.

2.526.2 REQUERIMIENTO DE ASEGURAMIENTO

Especificación de aseguramiento de las funciones de seguridad que deben implementarse para alcanzar uno o varios objetivos de seguridad, centrada generalmente en el entorno de desarrollo del sistema. [EBIOS:2005]

2.526.3 CERTEZA

1. Confianza que puede depositarse en la seguridad suministrada por el Objeto de Evaluación (ITSEC)

2. Confianza depositada en un sistema para alcanzar su Objetivo de Seguridad.

[Ribagorda:1997]

2.526.4 CERTEZA

Seguridad de que un sistema alcanza los objetivos de seguridad para los que ha sido diseñado. [CESID:1997]

2.526.5 (EN) GUARANTEE

Something that makes something else certain to happen.

Oxford Advanced Learner's Dictionary.

2.526.1 (EN) ASSURANCE

Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. [CNSSI_4009:2010]

2.526.2 (EN) ASSURANCE

in the context of this document: Grounds for confidence that a deliverable meets its security objectives [ISO/IEC 15408].

NOTE. This definition is generally accepted within the security community; within ISO the more generally used definition is: Activity resulting in a statement giving confidence that a product, process or service fulfills specified requirements [ISO/IEC Guide 2].

[ISO-21827:2007]

2.526.3 (EN) ASSURANCE ARGUMENT

a set of structured assurance claims, supported by evidence and reasoning, that demonstrate clearly how assurance needs have been satisfied. [ISO-21827:2007]

2.526.4 (EN) ASSURANCE CLAIM

an assertion or supporting assertion that a system meets a security need. Claims address both direct threats (e.g., system data are protected from attacks by outsiders) and indirect threats (e.g., system code has minimal flaws). [ISO-21827:2007]

2.526.5 (EN) ASSURANCE EVIDENCE

data on which a judgment or conclusion about an assurance claim may be based. The evidence may consist of observation, test results, analysis results and appraisals. [ISO-21827:2007]

2.526.6 (EN) SECURITY ASSURANCE

1. (I) An attribute of an information system that provides grounds for having confidence that the system operates such that the system's security policy is enforced. (Compare: trust.)

2. (I) A procedure that ensures a system is developed and operated as intended by the system's security policy.

[RFC4949:2007]

2.526.7 (EN) ASSURANCE

Grounds for confidence that a TOE meets the SFRs.

TOE - Target of Evaluation

SFR - Security Functional Requirement

[CC:2006]

2.526.8 (EN) SECURITY ASSURANCE REQUIREMENT

Specification of the assurance provided by security functions to be implemented to contribute to one or more security objectives, and generally concerning the system development environment. [EBIOS:2005]

2.526.9 (EN) ASSURANCE

Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass. [NIST-SP800-27:2004]

2.526.10 (EN) ASSURANCE APPROACH

A grouping of assurance methods according to the aspect examined. [ISO-15443-1:2005]

2.526.11 (EN) ASSURANCE ASSESSMENT

Verification and recording of the overall types and amounts of assurance associated with the deliverable (entered into the assurance argument). [ISO-15443-1:2005]

2.526.12 (EN) ASSURANCE

Grounds for confidence that the other four security objectives (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. Adequately met includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass. [NIST-SP800-33:2001]

2.526.13 (EN) ASSURANCE

the confidence that may be held in the security provided by a Target of Evaluation. [ITSEC:1991]

2.526.14 (FR) EXIGENCE D'ASSURANCE DE SÉCURITÉ

Spécification d'assurance des fonctions de sécurité à mettre en œuvre pour participer à la couverture d'un ou plusieurs objectifs de sécurité, et portant généralement sur l'environnement de développement du système. [EBIOS:2005]

2.527 GARANTÍA DE LA INFORMACIÓN

Ver:

- *Garantía*
- *Seguridad de la información*

2.527.1 GARANTÍA DE LA INFORMACIÓN

Medidas que protegen la información frente a ataques a su disponibilidad, integridad, autenticidad, confidencialidad y no-repudio. Entre dichas medidas podemos encontrar mecanismos de recuperación, de protección, detección y reacción.

2.527.2 (EN) INFORMATION ASSURANCE (IA)

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [CNSSI_4009:2010]

2.528 GCM - GALOIS / COUNTER MODE

Acrónimos: GCM

Ver:

- *Modo de operación (1)*
- [NIST-SP800-38D:2007]
- *Criptografía de clave secreta*

2.528.1 GCM - GALOIS / COUNTER MODE

Variación del modo de cifrado CTR incluyendo un mecanismo de autenticación basado en una función resumen.

2.528.2 (EN) GCM - GALOIS / COUNTER MODE

GCM combines a variation of the Counter Mode for encryption with an authentication mechanism that is based on a universal hash function. The underlying (approved) block cipher must have a block size of 128 bits (i.e., the AES algorithm) and the size of the authentication tag is 96-128 bits.

2.529 GENERACIÓN DE CLAVES

Ver:

- *Clave*
- *Clave criptográfica*

2.529.1 GENERADOR DE CLAVES

Equipo criptográfico usado para generar claves criptográficas y, si es necesario, vectores de iniciación (ISO-8732, CD 11166). [Ribagorda:1997]

2.529.2 GENERADOR DE CLAVES

Dispositivo o algoritmo que produce una secuencia pseudoaleatoria de claves. [CESID:1997]

2.529.3 (EN) KEY GENERATION

(I) A process that creates the sequence of symbols that comprise a cryptographic key. (See: key management.) [RFC4949:2007]

2.529.4 (EN) KEY GENERATOR

1. (I) An algorithm that uses mathematical rules to deterministically produce a pseudorandom sequence of cryptographic key values.

2. (I) An encryption device that incorporates a key-generation mechanism and applies the key to plain text to produce cipher text (e.g., by exclusive OR-ing (a) a bit-string representation of the key with (b) a bit-string representation of the plaintext).

[RFC4949:2007]

2.529.5 (EN) KEY GENERATION ALGORITHM

method for generating asymmetric key pairs. [ISO-18033-2:2006]

2.530 GENERADOR DE NÚMEROS ALEATORIOS

Acrónimos: RNG

Ver:

- *Aleatorio*
- *Seudoaleatorio*
- *Generador de números seudo-aleatorio*

2.530.1 GENERADOR ALEATORIO

Dispositivo utilizado para producir una secuencia aleatoria de caracteres. [CESID:1997]

2.530.2 (EN) RANDOM NUMBER GENERATOR (RNG)

A process used to generate an unpredictable series of numbers. Each individual value is called random if each of the values in the total population of values has an equal probability of being selected. [CNSSI_4009:2010]

2.530.3 (EN) RANDOMIZER

Analog or digital source of unpredictable, unbiased, and usually independent bits. Randomizers can be used for several different functions, including key generation or to provide a starting state for a key generator. [CNSSI_4009:2010]

2.530.4 (EN) RANDOM NUMBER GENERATOR (RNG)

A process used to generate an unpredictable series of numbers. Each individual value is called random if each of the values in the total population of values has an equal probability of being selected. [NIST-SP800-57:2007]

2.530.5 (EN) RANDOM BIT GENERATOR (RBG)

A device or algorithm that outputs a sequence of bits that appears to be statistically independent and unbiased. [ISO-19790:2006]

2.530.6 (EN) RANDOM NUMBER GENERATOR

A module that generates streams of random numbers. The random source could be analog oscillator (ARNG) or Digital oscillator (DRNG).

2.531 GENERADOR DE NÚMEROS SEUDO-ALEATORIO

Acrónimos: DRBG, PRNG

Ver:

- *Semilla (1)*

2.531.1 GENERADOR DE NÚMEROS SEUDOALEATORIOS

Algoritmo matemático que produce una sucesión indefinida de números aparentemente aleatorios (seudoaleatorios), es decir, que satisfacen, en mayor o menor grado, las pruebas habituales de aleatoriedad. Para su arranque precisan de un valor inicial denominado semilla.

La generación de números aleatorios es de trascendental importancia en criptografía; por ejemplo, en la obtención de claves criptográficas, en sistemas de autenticación pregunta-respuesta, en ciertos protocolos de autenticación fuerte, etc.

Ejemplos de estos generadores son los congruenciales y los de registro de desplazamiento de realimentación lineal (LFSR).

[Ribagorda:1997]

2.531.2 (EN) PSEUDO RANDOM NUMBER GENERATOR (PRNG)

An algorithm that produces a sequence of bits that are uniquely determined from an initial value called a seed. The output of the PRNG "appears" to be random, i.e., the output is statistically indistinguishable from random values. A cryptographic PRNG has the additional property that the output is unpredictable, given that the seed is not known. [CNSSI_4009:2010]

2.531.3 (EN) DETERMINISTIC RANDOM BIT GENERATOR (DRBG)

An algorithm that produces a sequence of bits that are uniquely determined from an initial value called a seed. The output of the DRBG appears to be random, i.e., the output is statistically indistinguishable from random values. A cryptographic DRBG has the additional property that the output is unpredictable, given that the seed is not known. A DRBG is sometimes also called a Pseudo Random Number Generator (PRNG) or a deterministic random number generator. [NIST-SP800-57:2007]

2.531.4 (EN) PSEUDO RANDOM NUMBER GENERATOR

A module that generates streams of numbers (in the form of bits) that appears random.

2.532 GESTIÓN DE CAMBIOS

Ver:

- *Cambio*

2.532.1 CHANGE MANAGEMENT

(Service Transition) The Process responsible for controlling the Lifecycle of all Changes. The primary objective of Change Management is to enable beneficial Changes to be made, with minimum disruption to IT Services. [ITIL:2007]

2.532.2 GESTIÓN DE CAMBIOS

El principal objetivo de la Gestión de Cambios es la evaluación y planificación del proceso de cambio para asegurar que, si éste se lleva a cabo, se haga de la forma más eficiente, siguiendo los

procedimientos establecidos y asegurando en todo momento la calidad y continuidad del servicio TI.

http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_cambios/vision_general_gestion_de_cambios/vision_general_gestion_de_cambios.php

2.532.3 (EN) CHANGE MANAGEMENT

(Service Transition) The Process responsible for controlling the Lifecycle of all Changes. The primary objective of Change Management is to enable beneficial Changes to be made, with minimum disruption to IT Services. [ITIL:2007]

2.532.4 (EN) CHANGE MANAGEMENT

The process of controlling modifications to hardware, software, firmware, and documentation to ensure that information technology resources are protected against improper modification before, during, and after system implementation.

http://www.utexas.edu/its/policies/glossary.html

2.532.5 (FR) GESTION DES CHANGEMENTS

(Transition de Services) Processus en charge de contrôler le cycle de vie de tous les changements. Le principal objectif de la gestion des changements et de rendre possible la mise en œuvre de changements bénéfiques avec un minimum d'interruption des services des TI. [ITIL:2007]

2.533 GESTIÓN DE CLAVES

Acrónimos: KMI

Ver:

- *Clave*
- *Clave criptográfica*

2.533.1 ADMINISTRACIÓN DE CLAVES CRIPTOGRÁFICAS

Conjunto de procesos y mecanismos que respaldan el establecimiento y mantenimiento de las claves, así como el reemplazo de claves anteriores por nuevas claves, según sea necesario.

http://es.pcisecuritystandards.org

2.533.2 GESTIÓN DE CLAVES

Proceso de generación, almacenamiento, distribución y aplicación de claves criptográficas de acuerdo con una política de seguridad (ISO-8732, ISO-7498-2). [Ribagorda:1997]

2.533.3 GESTIÓN DE CLAVES

Proceso que comprende la generación, distribución, almacenamiento, utilización, archivo y destrucción de las claves empleadas en un criptosistema. [CESID:1997]

2.533.4 SISTEMA NACIONAL DE GESTIÓN DE CLAVES

Proceso que controla de modo seguro los procedimientos que regulan la actuación del Algoritmo Nacional de Cifra. [CESID:1997]

2.533.5 GESTIÓN DE CLAVES

Generación, almacenamiento, distribución, supresión, archivo y aplicación de claves de acuerdo con una política de seguridad. [ISO-7498-2:1989]

2.533.1 (EN) KEY MANAGEMENT

The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization. [CNSSI_4009:2010]

2.533.2 (EN) KEY MANAGEMENT DEVICE

A unit that provides for secure electronic distribution of encryption keys to authorized users. [CNSSI_4009:2010]

2.533.3 (EN) KEY MANAGEMENT INFRASTRUCTURE (KMI)

All parts – computer hardware, firmware, software, and other equipment and its documentation; facilities that house the equipment and related functions; and companion standards, policies, procedures, and doctrine that form the system that manages and supports the ordering and delivery of cryptographic material and related information products and services to users. [CNSSI_4009:2010]

2.533.4 (EN) KEY MANAGEMENT

1a. (I) The process of handling keying material during its life cycle in a cryptographic system; and the supervision and control of that process. (See: key distribution, key escrow, keying material, public-key infrastructure.)

Usage: Usually understood to include ordering, generating, storing, archiving, escrowing, distributing, loading, destroying, auditing, and accounting for the material.

1b. (O) /NIST/ "The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs, counters) during the entire life cycle of the keys, including their generation, storage, distribution, entry and use, deletion or destruction, and archiving." [FP140, SP57]

2. (O) /OSIRM/ "The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy." [ISO-7498-2]

[RFC4949:2007]

2.533.5 (EN) KEY MANAGEMENT

The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction. [NIST-SP800-57:2007]

2.533.6 (EN) KEY MANAGEMENT ARCHIVE

A function in the lifecycle of keying material; a repository containing keying material of historical interest. [NIST-SP800-57:2007]

2.533.7 (EN) KEY MANAGEMENT POLICY

The Key Management Policy is a high-level statement of organizational key management policies that identifies high-level structure, responsibilities, governing standards and recommendations, organizational dependencies and other relationships, and security policies. [NIST-SP800-57:2007]

2.533.8 (EN) KEY MANAGEMENT PRACTICES STATEMENT

The Key Management Practices Statement is a document or set of documentation that describes in detail the organizational structure, responsible roles, and organization rules for the functions identified in the Key Management Policy. [NIST-SP800-57:2007]

2.533.9 (EN) KEY MANAGEMENT

the administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy. [ISO-19790:2006]

2.533.10 (EN) KEY MANAGEMENT

the activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization. [FIPS-140-2:2001]

2.533.11 (EN) KEY MANAGEMENT

The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy. [ISO-7498-2:1989]

2.533.12 (EN) KEY MANAGEMENT:

In cryptography, it is the set of processes and mechanisms which support key establishment and maintenance, including replacing older keys with new keys as necessary.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.533.13 (FR) GESTION DE CLÉ CRYPTOGRAPHIQUE

L'ensemble des mécanismes et processus qui prennent en charge l'établissement et la maintenance des clés, notamment le remplacement d'anciennes clés par des nouvelles, le cas échéant.

http://fr.pcisecuritystandards.org/

2.533.14 (FR) GESTION DE CLÉS

Production, stockage, distribution, suppression, archivage et application de clés conformément à la politique de sécurité. [ISO-7498-2:1989]

2.534 GESTIÓN DE CRISIS

Ver:

- *Continuidad*

2.534.1 GESTIÓN DE CRISIS

El Proceso responsable para gestionar las implicaciones más amplias de Continuidad de Negocio. Un equipo de Gestión de Crisis es responsable de temas Estratégicos tales como gestión de medios y confianza de accionistas, y decide cuándo invocar los Planes de Continuidad de Negocio. [ITIL:2007]

2.534.2 (EN) CRISIS MANAGEMENT

The Process responsible for managing the wider implications of Business Continuity. A Crisis Management team is responsible for Strategic issues such as managing media relations and share-holder confidence, and decides when to invoke Business Continuity Plans. [ITIL:2007]

2.534.3 (EN) CRISIS MANAGEMENT

The process of managing an institution's operations in response to an emergency or event which threatens business continuity. An institution's ability to communicate with employees, customers, and the media, using various communications devices and methods, is a key component of crisis management.

http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-b-glossary.aspx

2.534.4 (EN) CRISIS MANAGEMENT TEST / EXERCISE

A testing exercise that validates the capabilities of crisis management teams to respond to specific events. Crisis management exercises typically test the call tree notification process with employees, vendors, and key clients. Escalation procedures and disaster declaration criteria may also be validated.

http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-b-glossary.aspx

2.534.5 (FR) GESTION DE CRISES

Processus en charge de la gestion des implications plus larges de la Continuité du Business. L'équipe de gestion de crise est responsable des questions stratégiques, comme la gestion des relations avec les média et la confiance des actionnaires, c'est elle qui décide du déclenchement des Plans de Continuité du Business. [ITIL:2007]

2.535 GESTIÓN DE DERECHOS DE ACCESO

Ver:

- *Acceso*

2.535.1 GESTIÓN DEL ACCESO

(Operación del Servicio) Proceso responsable de permitir a los Usuarios hacer uso de los Servicios de TI, datos, u otros Activos. La Gestión de Acceso ayuda a proteger la Confidencialidad, la Integridad y la Disponibilidad de los Activos, asegurando que sólo Usuarios autorizados pueden acceder o modificar los Activos. Algunas veces también es posible referirse a la Gestión del Acceso como Gestión de Derechos o como Gestión de la Identidad. [ITIL:2007]

2.535.2 (EN) ACCESS MANAGEMENT

(Service Operation) The Process responsible for allowing Users to make use of IT Services, data, or other Assets. Access Management helps to protect the Confidentiality, Integrity and Availability of Assets by ensuring that only authorized Users are able to access or modify the Assets. Access Management is sometimes referred to as Rights Management or Identity Management. [ITIL:2007]

2.535.3 (FR) GESTION DES ACCÈS

(Exploitation de Services) Le processus responsable d'autoriser les utilisateurs à faire usage des services des TI, des données ou autres actifs. La Gestion de l'accès contribue à protéger la confidentialité, l'intégrité et la disponibilité des actifs en assurant que seuls les utilisateurs autorisés peuvent accéder ou modifier les actifs. La Gestion de l'accès est parfois appelée Gestion des Droits ou Gestion de l'Identification. [ITIL:2007]

2.536 GESTIÓN DE DISPOSITIVOS MÓVILES

Acrónimos:

MDM – Mobile Device Management

MAM – Mobile Application Management

MEAM – Mobile Enterprise Application Management

MCM – Mobile Content Management

2.536.1 GESTIÓN DE DISPOSITIVOS MÓVILES

Software que se instala en dispositivos móviles para poder imponer la política establecda por la organización. Constituye un medio de configuración y control remoto de la configuración de un dispositivo móvil.

2.536.2 (EN) MOBILE DEVICE MANAGEMENT (MDM)

Mobile device management (MDM) includes software that provides the following functions: software distribution, policy management, inventory management, security management and service management for smartphones and media tablets. MDM functionality is similar to that of PC configuration life cycle management (PCCLM) tools; however, mobile-platform-specific requirements are often part of MDM suites.

http://www.gartner.com/it-glossary/

2.536.3 (EN) MOBILE DEVICE MANAGEMENT (MDM) SERVICES

Mobile device management (MDM) services involve sourcing, provisioning, securing and managing handheld mobile devices (primarily smartphones and media tablets) to a third party. This may include PC cards, pagers, notebooks and other mobile devices. MDM services may also include support for any or all of these main areas: hardware (inventory, provisioning and asset), software (configuration management, software distribution and updates), security (black list, encryption, antivirus, authentication, jailbreak/rooted notification) and network service management.

http://www.gartner.com/it-glossary/

2.536.4 (EN) MOBILE DEVICE MANAGENEMT (MDM)

Mobile device management (MDM) is the administrative area dealing with deploying, securing, monitoring, integrating and managing mobile devices, such as smartphones, tablets and laptops, in the workplace. The intent of MDM is to optimize the functionality and security of mobile devices within the enterprise, while simultaneously protecting the corporate network.

Mobile device management software allows distribution of applications, data and configuration settings and patches for such devices. Ideally, MDM software allows administrators to oversee mobile devices as easily as desktop computers and provides optimal performance for users. MDM tools should include application management, file synchronization and sharing, data security tools, and support for either a corporate-owned or personally owned device.

The ideal mobile device management tool:

- Is compatible with all common handheld device operating platforms and applications.
- Can function through multiple service providers.
- Can be implemented directly over the air, targeting specific devices as necessary.
- Can deploy next-generation hardware, operating platforms and applications quickly.
- Can add or remove devices from the system as necessary to ensure optimum network efficiency and security.

http://searchmobilecomputing.techtarget.com/

2.537 GESTIÓN DE EVENTOS DE SEGURIDAD

Acrónimos: SEM

Ver:

- *Evento*

2.537.1 SIEM

En inglés System Informatíon and Event Manager, es una herramienta que recolecta y centraliza todos los eventos de seguridad e información de los registros de actividad de una infraestructura TIC.

http://www.inteco.es/glossary/Formacion/Glosario/

2.537.2 SIM

Security information management (SIM) es el término específico de la industria en seguridad informática se refiere a la recogida de datos (normalmente logs o registros de actividad) en un repositorio central para el análisis de tendencias.

Abarcan generalmente los agentes de software que se ejecutan en los sistemas , se comunica con un servidor centralizado que actúa como "consola de seguridad", que muestra los informes, tablas y gráficos de esa información, a menudo en tiempo real.

http://www.inteco.es/glossary/Formacion/Glosario/

2.537.3 GESTIÓN DE EVENTOS DE SEGURIDAD

Sistema para la clasificación y análisis de eventos de seguridad mediante el uso de técnicas de correlación de trazas de registro de múltiples dispositivos. [CCN-STIC-400:2006]

2.537.4 (EN) SECURITY EVENT MANAGEMENT

A Security Event Manager (SEM) is a computerised tool used on enterprise data networks to centralize the storage and interpretation of logs, or events, generated by other software running on the network.

http://www.gss.co.uk/glossary/

2.537.5 (EN) SECURITY EVENT MANAGEMENT

A Security Event Manager (SEM) is a computerized tool used on enterprise data networks to centralize the storage and interpretation of logs, or events, generated by other software running on the network.

http://en.wikipedia.org/wiki/Security_Event_Manager

2.537.6 (EN) SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Security information and event management (SIEM) is an approach to security management that seeks to provide a holistic view of an organization’s information technology (IT) security. SIEM combines SIM (security information management) and SEM (security event management) functions into one security management system. The acronym is pronounced "sim" with a silent e.

http://searchsecurity.techtarget.com/

2.537.7 (EN) SECURITY INFORMATION MANAGEMENT (SIM)

Security information management (SIM) is the practice of collecting, monitoring and analyzing security-related data from computer logs. A security information management system (SIMS) automates that practice. Security information management is sometimes called security event management (SEM) or security information and event management (SIEM).

http://searchsecurity.techtarget.com/

2.538 GESTIÓN DE INCIDENTES

Ver:

- *Incidente*

2.538.1 GESTIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Procesos para la detección, notificación, evaluación, respuesta, tratamiento, y aprendizaje de incidentes de seguridad de información. [UNE-ISO/IEC 27000:2014]

2.538.2 GESTIÓN DE INCIDENTES

Plan de acción para atender a los incidentes que se den. Además de resolverlos debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas. [ENS:2010]

2.538.3 GESTIÓN DE INCIDENCIAS

(Operación del Servicio) Proceso responsable de la gestión del Ciclo de vida de todos los Incidentes. El objetivo primario de la Gestión de Incidencias es recuperar el Servicio de TI para los Usuarios lo antes posible. [ITIL:2007]

2.538.4 (EN) INFORMATION SECURITY INCIDENT MANAGEMENT

processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents [ISO/IEC 27000:2014]

2.538.5 (EN) INCIDENT RESPONSE PLAN

The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of an incident against an organization’s IT systems(s). [CNSSI_4009:2010]

2.538.6 (EN) INCIDENT MANAGEMENT

(Service Operation) The Process responsible for managing the Lifecycle of all Incidents. The primary Objective of Incident Management is to return the IT Service to Users as quickly as possible. [ITIL:2007]

2.538.7 (EN) INCIDENT MANAGEMENT PLAN

clearly defined and documented plan of action for use at the time of an incident, typically covering the key personnel, resources, services and actions needed to implement the incident management process. [BS25999-1:2006]

2.538.8 (EN) INFORMATION SECURITY INCIDENT MANAGEMENT

the formal process of responding to and dealing with information security events and incidents. [ISO-18028-1:2006] [ISO-18044:2004]

2.538.9 (EN) INCIDENT RESPONSE PLAN

The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organizations IT systems(s). [NIST-SP800-34:2002]

2.538.10 (EN) INCIDENT HANDLING

Incident Handling is an action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is comprised of a six step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

http://www.sans.org/security-resources/glossary-of-terms/

2.538.11 (EN) INCIDENT RESPONSE

The ability to deliver the event or set of events to an incident management system or a HelpDesk system to resolve and track incidents.

http://www.symantec.com/avcenter/refa.html

2.538.12 (EN) INCIDENT RESPONSE CYCLE

The sequence of phases that a security event goes through from the time it is identified as a security compromise or incident to the time it is resolved and reported.

http://www.symantec.com/avcenter/refa.html

2.538.13 (FR) GESTION DES INCIDENTS

(Exploitation de Services) Processus en charge de la gestion du cycle de vie de tous les incidents. L'objectif principal de la Gestion des incidents est de rendre le service des TI aux utilisateurs aussi rapidement que possible. [ITIL:2007]

2.539 GESTIÓN DE LA CONFIGURACIÓN

Ver:

- *Configuración*
- *Control de configuración*

2.539.1 GESTIÓN DE LA CONFIGURACIÓN

(Transición del Servicio) Proceso responsable de mantener información sobre los Elementos de Configuración requeridos para la provisión de un Servicio de TI, incluyendo las Relaciones entre ellos. Esta información se gestiona durante todo el Ciclo de Vida del CI. La Gestión de la Configuración forma parte de un Activo del Servicio global y del Proceso de Gestión de la Configuración. [ITIL:2007]

2.539.2 (EN) CONFIGURATION MANAGEMENT

(Service Transition) The Process responsible for maintaining information about Configuration Items required to deliver an IT Service, including their Relationships. This information is managed

throughout the Lifecycle of the CI. Configuration Management is part of an overall Service Asset and Configuration Management Process. [ITIL:2007]

2.539.3 (FR) GESTION DES CONFIGURATIONS

(Transition de Services) Processus en charge de tenir à jour les informations concernant les éléments de configuration nécessaires pour fournir un service informatique ainsi que leurs relations. Ces informations sont gérées tout au long du cycle de vie du CI. La Gestion des configurations fait partie du processus global de Gestion des configurations et des actifs de service. [ITIL:2007]

2.540 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (BCM)

Acrónimos: BCM

Ver:

- *Continuidad*

2.540.1 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (BCM)

(Diseño del Servicio) Es el Proceso de Negocio responsable de gestionar el Riesgo que puede tener un alto impacto en el Negocio. BCM protege los intereses de los principales interesados, la reputación, la marca y las actividades que aportan valor al Negocio. Los Procesos de BCM incluyen reducir el Riesgo a un nivel aceptable y planificar el restablecimiento de los Procesos de Negocio ante una situación. BCM establece los Objetivos, el Ámbito y los Requerimientos para una Gestión de la Continuidad del Servicio. [ITIL:2007]

2.540.2 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (BCM)

Proceso de gestión integral en materia de continuidad. Analiza las amenazas relevantes y desarrolla para la Organización un esquema de resistencia y de respuesta que salvaguarde de forma efectiva los intereses de las partes y del negocio.

2.540.3 (EN) BUSINESS CONTINUITY MANAGEMENT (BCM)

(Service Design) The Business Process responsible for managing Risks that could seriously impact the Business. BCM safeguards the interests of key stakeholders, reputation, brand and value creating activities. The BCM Process involves reducing Risks to an acceptable level and planning for the recovery of Business Processes should a disruption to the Business occur. BCM sets the Objectives, Scope and Requirements for IT Service Continuity Management. [ITIL:2007]

2.540.4 (EN) BUSINESS CONTINUITY MANAGEMENT

business continuity management (BCM) holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities [BS25999-1:2006]

2.540.5 (EN) BUSINESS CONTINUITY MANAGEMENT

the process to ensure that recovery of operations will be assured should any unexpected or unwanted incident occur that is capable of negatively impacting the continuity of essential business functions and supporting elements. (The process should also ensure that recovery is achieved in the required priorities and timescales, and subsequently all business functions and supporting elements will be recovered back to normal. The key elements of this process need to ensure that the necessary plans and facilities are put in place, and tested, and that they encompass information, business processes, information systems and services, voice and data communications, people and physical facilities.) [ISO-18028-1:2006]

2.540.6 (FR) GESTION DE LA CONTINUITE DU BUSINESS (BCM)

(Conception de services) Il s'agit du processus business en charge de la gestion des risques pouvant avoir un impact sérieux sur le business. La gestion de la continuité du business protège les intérêts des intervenants, la réputation de la marque et sa valeur en créant des activités. Le processus de la BCM implique la réduction des risques à un niveau acceptable et la planification de la reprise des processus business suite à une interruption de celui-ci. La BCM définit les objectifs, l'étendue et les besoins de la Gestion de la continuité du Service des TI. [ITIL:2007]

2.541 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Ver:

- *Sistema de gestión de la seguridad de la información (SGSI)*

2.541.1 GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN

(Diseño del Servicio) Proceso que asegura la Confidencialidad, Integridad y Disponibilidad de los Activos de una Organización, información, datos y Servicios de TI. La Gestión de la Seguridad de la información forma parte normalmente de la Gestión de la Seguridad de la Organización, la cual tiene un ámbito más amplio que las del Proveedor de Servicio de TI e incluye accesos a edificios, llamadas de teléfonos, etc para toda la Organización. [ITIL:2007]

2.541.2 GESTIÓN

actividades coordinadas para dirigir y controlar una organización. [ISO-9000_es:2000]

2.541.3 SEGURIDAD ADMINISTRATIVA Y ORGANIZATIVA

Aspecto de la seguridad relacionado con la gestión de la misma. Se manifiesta en la formulación de políticas y procedimientos de seguridad.

Más concretamente, se establece mediante: la asignación d responsabilidades, el establecimiento de una política de clasificación de la información, de una política de personal (selección y formación en temas de seguridad informática, cláusulas de penalización en contratos por abuso o negligencia, etc.), de procedimientos de registro de incidente, de auditoría, etc. También comprende la gestión de riesgos y los planes de contingencia.

[Ribagorda:1997]

2.541.4 (EN) INFORMATION SECURITY MANAGEMENT (ISM)

(Service Design) The Process that ensures the Confidentiality, Integrity and Availability of an Organisation's Assets, information, data and IT Services. Information Security Management usually forms part of an Organisational approach to Security Management which has a wider scope than the IT Service Provider, and includes handling of paper, building access, phone calls etc., for the entire Organisation. [ITIL:2007]

2.541.5 (FR) GESTION DE LA SECURITE DE L'INFORMATION (ISM)

(Conception de services) Processus qui assure la confidentialité, l'intégrité et la disponibilité des actifs, informations, données et services des TI d'une organisation. La Gestion de la Sécurité de l'Information fait habituellement partie d'une approche organisationnelle de la Gestion de la Sécurité avec une étendue plus large que la fourniture de services informatiques. Elle inclut la manipulation des papiers, l'accès aux bâtiments, les appels téléphoniques, etc, de toute l'organisation. [ITIL:2007]

2.542 GESTIÓN DE RIESGOS

Ver:

- *Riesgo*
- *Gestión del riesgo empresarial*

2.542.1 GESTIÓN DEL RIESGO

Actividades coordinadas para dirigir y controlar una organización, con respecto al riesgo. [ISO Guía 73:2010]

[UNE-ISO/IEC 27000:2014]

2.542.2 GESTIÓN DEL RIESGO

Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo [UNE Guía 73:2010]

2.542.3 MARCO DE TRABAJO DE LA GESTIÓN DEL RIESGO

Conjunto de elementos que proporcionan los fundamentos y las disposiciones de la organización para el diseño, la implantación, el seguimiento, la revisión y la mejora continua de la gestión del riesgo en toda la organización. [UNE Guía 73:2010]

2.542.4 PROCESO DE GESTIÓN DEL RIESGO

Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo [UNE Guía 73:2010]

2.542.5 GESTIÓN DE RIESGOS

Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos. [UNE-71504:2008]

2.542.6 GESTIÓN DE RIESGO

El Proceso responsable por la identificación, determinación y control de Riesgos.

Ver Determinación de Riesgos.

[ITIL:2007]

2.542.7 (EN) RISK MANAGEMENT

The process of identifying, assessing, and responding to risk.

Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, February 12, 2014

2.542.8 (EN) RISK MANAGEMENT

coordinated activities to direct and control an organisation with regard to risk [ISO Guide 73:2009]

[ISO/IEC 27000:2014]

2.542.9 (EN) RISK MANAGEMENT

coordinated activities to direct and control an organisation with regard to risk [ISO Guide 73:2009]

2.542.10 (EN) RISK MANAGEMENT FRAMEWORK

set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization [ISO Guide 73:2009]

2.542.11 (EN) RISK MANAGEMENT PROCESS

systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk [ISO Guide 73:2009]

2.542.1 (EN) RISK CONTROL

deliberate action taken to reduce the potential for harm or maintain it at an acceptable level

DHS Risk Lexicon, September 2008

2.542.2 (EN) ENTERPRISE RISK MANAGEMENT

The discipline by which an enterprise in any industry assesses, controls, exploits, finances and monitors risks from all sources for the purpose of increasing the enterprise's short- and long-term value to its stakeholders. [RiskIT-PG:2009]

2.542.3 (EN) RISK MANAGEMENT

Has been used in this publication as an overall generic term that covers both governance and management. [RiskIT-PG:2009]

2.542.4 (EN) RISK MANAGEMENT

The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes:

(i) the conduct of a risk assessment;

(ii) the implementation of a risk mitigation strategy; and

(iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

[FIPS 200, Adapted] [NIST-SP800-53:2013]

2.542.1 (EN) RISK MANAGEMENT

The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation or use of an information system, and includes: 1) the conduct of a risk assessment; 2) the implementation of a risk mitigation strategy; 3) employment of techniques and procedures for the continuous monitoring of the security state of the information system; and 4) documenting the overall risk management program.

NIST SP 800-53: The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system, and includes: 1. the conduct of a risk assessment; 2. the implementation of a risk mitigation strategy; and 3. employment of techniques and procedures for the continuous monitoring of the security state of the information system.

[CNSSI_4009:2010]

2.542.2 (EN) RISK MANAGEMENT FRAMEWORK (RMF)

A structured approach used to oversee and manage risk for an enterprise. [CNSSI_4009:2010]

2.542.3 (EN) RISK MANAGEMENT

process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost

Annotation: The primary goal of risk management is to reduce or eliminate risk through mitigation measures (avoiding the risk or reducing the negative effect of the risk), but also includes the concepts of acceptance and/or transfer of responsibility for the risk as appropriate. Risk management principles acknowledge that, while risk often cannot be eliminated, actions can usually be taken to reduce risk.

DHS Risk Lexicon, September 2008

2.542.4 (EN) RISK MANAGEMENT ALTERNATIVES DEVELOPMENT:

Definition: process of systematically examining risks to develop a range of options and their anticipated effects for decision makers

Annotation: The risk management alternatives development step of the risk management process generates options for decision-makers to consider before deciding on which option to implement.

DHS Risk Lexicon, September 2008

2.542.5 (EN) RISK MANAGEMENT

1. (I) The process of identifying, measuring, and controlling (i.e., mitigating) risks in information systems so as to reduce the risks to a level commensurate with the value of the assets protected. (See: risk analysis.)

2. (I) The process of controlling uncertain events that may affect information system resources.

3. (O) "The total process of identifying, controlling, and mitigating information system-related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws." [SP30]

[RFC4949:2007]

2.542.6 (EN) RISK MANAGEMENT

The Process responsible for identifying, assessing and controlling Risks.

See Risk Assessment.

[ITIL:2007]

2.542.7 (EN) RISK MANAGEMENT

The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system. [FIPS-200:2006]

2.542.8 (EN) RISK MANAGEMENT

The total process of identifying, controlling, and mitigating information technology related risks. It includes risk analysis; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission/business and constraints due to policy, regulations, and laws. [NIST-SP800-33:2001]

2.542.9 (EN) RISK MANAGEMENT

The identification, assessment, and mitigation of probabilistic security events (risks) in information systems to a level commensurate with the value of the assets protected. [CIAO:2000]

2.542.10 (EN) RISK MANAGEMENT

A security philosophy which considers actual threats, inherent vulnerabilities, and the availability and costs of countermeasures as the underlying basis for making security decisions (JSCR 1994).

http://www.ioss.gov/docs/definitions.html

2.542.11 RISK MANAGEMENT

Risk management includes RIDM and CRM in an integrated framework. This is done in order to foster proactive risk management, to better inform decision making through better use of risk information, and then to more effectively manage implementation risks by focusing the CRM process on the baseline performance requirements emerging from the RIDM process.

NASA Risk Management Handbook, NASA/SP-2011-3422, Version 1.0, November 2011

2.542.12 (FR) MANAGEMENT DU RISQUE

activités coordonnées dans le but de diriger et piloter un organisme vis-à-vis du risque [ISO Guide 73:2009]

2.542.13 (FR) CADRE ORGANISATIONNEL DE MANAGEMENT DU RISQUE

ensemble d'éléments établissant les fondements et dispositions organisationnelles présidant à la conception, la mise en oeuvre, la surveillance, la revue et l'amélioration continue du management du risque dans tout l'organisme [ISO Guide 73:2009]

2.542.14 (FR) PROCESSUS DE MANAGEMENT DU RISQUE

application systématique de politiques, procédures et pratiques de management aux activités de communication, de concertation, d'établissement du contexte, ainsi qu'aux activités d'identification, d'analyse, d'évaluation, de traitement, de surveillance et de revue des risques [ISO Guide 73:2009]

2.542.15 (FR) GESTION DES RISQUES

Processus en charge d'identifier, évaluer et contrôler les risques.

Voir Évaluation du risque.

[ITIL:2007]

2.543 GESTIÓN DE VULNERABILIDADES

Ver:

- *Vulnerabilidad*
- *Evaluación de vulnerabilidad*
- *Escáner de vulnerabilidades*
- *Análisis de vulnerabilidades*

2.543.1 GESTIÓN DE VULNERABILIDADES

Proceso proactivo de seguridad consistente en identificar vulnerabilidades y reducirlas antes de que sean causa de un incidente de seguridad.

2.543.2 (EN) VULNERABILITY MANAGEMENT

Vulnerability management is a pro-active approach to managing network security. It includes processes for:

- Checking for vulnerabilities: This process should include regular network scanning, firewall logging, penetration testing or use of an automated tool like a vulnerability scanner.
- Identifying vulnerabilities: This involves analyzing network scans and pen test results, firewall logs or vulnerability scan results to find anomalies that suggest a malware attack or other malicious event has taken advantage of a security vulnerability, or could possibly do so.
- Verifying vulnerabilities: This process includes ascertaining whether the identified vulnerabilities could actually be exploited on servers, applications, networks or other systems. This also includes classifying the severity of a vulnerability and the level of risk it presents to the organization.
- Mitigating vulnerabilities: This is the process of figuring out how to prevent vulnerabilities from being exploited before a patch is available, or in the event that there is no patch. It can involve taking the affected part of the system off-line (if it's non-critical), or various other work-arounds.
- Patching vulnerabilities: This is the process of getting patches -- usually from the vendors of the affected software or hardware -- and applying them to all the affected areas in a timely way. This is sometimes an automated process, done with patch management tools. This step also includes patch testing,

http://searchsecurity.techtarget.in/

2.544 GESTIÓN DEL RIESGO EMPRESARIAL

Ver:

- *Gestión de riesgos*

2.544.1 GESTIÓN DEL RIESGO EMPRESARIAL

Métodos y procesos utilizados en las empresas para atender a los riesgos y gestionar la confianza de que la empresa alcance sus objetivos. Incluye la identificación de las dependencias entre los objetivos y los medios y capacidades de la empresa para conseguirlos, así como la identificación y priorización de las amenazas sobre dichos medios y la implantación de medidas de seguridad que los afronten. En conjunto proporciona tanto una seguridad estática como una respuesta dinámica efectiva.

2.544.2 (EN) ENTERPRISE RISK MANAGEMENT

The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of mission dependencies on enterprise capabilities, the identification and prioritization of risks due to defined threats, the implementation of countermeasures to provide both a static risk posture and an effective dynamic response to active threats; and it assesses enterprise performance against threats and adjusts countermeasures as necessary. [CNSSI_4009:2010]

2.544.3 (EN) ENTERPRISE RISK MANAGEMENT (ERM)

Enterprise risk management (ERM) is the process of planning, organizing, leading, and controlling the activities of an organization in order to minimize the effects of risk on an organization's capital and earnings. Enterprise risk management expands the process to include not just risks associated with accidental losses, but also financial, strategic, operational, and other risks.

http://searchcio.techtarget.com/definition/enterprise-risk-management

2.544.4 ENTERPRISE

An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. [CNSSI_4009:2010]

2.544.5 ENTERPRISE ARCHITECTURE (EA)

The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture.

2.544.6 ENTERPRISE SERVICE [CNSSI 4009:2010]

A set of one or more computer applications and middleware systems hosted on computer hardware that provides standard information systems capabilities to end users and hosted mission applications and services. [CNSSI_4009:2010]

2.545 GESTIÓN UNIFICADA DE AMENAZAS

Acrónimo: UTM

2.545.1 GESTIÓN UNIFICADA DE AMENAZAS

UTM (en inglés: Unified Threat Management) o Gestión Unificada de Amenazas. El término fue utilizado por primera vez por Charles Kolodgy, de International Data Corporation (IDC), en 2004.

Se utiliza para describir los cortafuegos de red que engloban múltiples funcionalidades en una misma máquina. Algunas de las funcionalidades que puede incluir son las siguientes: UDP, VPN,

Antispam, Antiphishing, Antispyware, Filtro de contenidos, Antivirus, Detección/Prevención de Intrusos (IDS/IPS).

Se trata de cortafuegos a nivel de capa de aplicación que pueden trabajar de dos modos:

- Modo proxy: hacen uso de proxies para procesar y redirigir todo el tráfico interno.
- Modo Transparente: no redirigen ningún paquete que pase por la línea, simplemente lo procesan y son capaces de analizar en tiempo real los paquetes. Este modo, como es de suponer, requiere de unas altas prestaciones de hardware.

Desventajas:

- Se crea un punto único de fallo y un cuello de botella, es decir si falla este sistema la organización queda desprotegida totalmente.
- Tiene un coste fijo periódico.

Ventajas: Se pueden sustituir varios sistemas independientes por uno solo facilitando su gestión.

UTM es un término que se refiere a un firewall de red con múltiples funciones añadidas, trabajando a nivel de aplicación. Realiza el proceso del tráfico a modo de proxy, analizando y dejando pasar el tráfico en función de la política implementada en el dispositivo.

https://es.wikipedia.org/wiki/Unified_Threat_Management

2.545.2 (EN) UTM – UNIFIED THREAT MANAGEMENT

Unified threat management (UTM) or unified security management (USM), is a solution in the network security industry, and since 2004 it has gained currency as a primary network gateway defense solution for organizations. In theory, UTM is the evolution of the traditional firewall into an all-inclusive security product able to perform multiple security functions within one single system: network firewalling, network intrusion prevention and gateway antivirus (AV),gateway antispam, VPN, content filtering, load balancing, data leak prevention and on-appliance reporting.

The worldwide UTM market was approximately worth $1.2 billion in 2007, with a forecast of 35-40% compounded annual growth rate through 2011. The primary market of UTM providers is the SMB and enterprise segments, although a few providers are now providing UTM solutions for small offices/remote offices.

The term UTM was originally coined by market research firm IDC. The advantages of unified security lie in the fact that rather than administering multiple systems that individually handle antivirus, content filtering, intrusion prevention and spam filtering functions, organizations now have the flexibility to deploy a single UTM appliance that takes over all their functionality into a single rack mountable network appliance.

https://en.wikipedia.org/wiki/Unified_threat_management

2.546 GOBERNANZA

2.546.1 GOBIERNO

Asegurar que las Políticas y Estrategias se implementan, y que los Procesos requeridos se siguen correctamente. El Gobierno incluye definir los Roles y Responsabilidades, medir y reportar, y tomar acciones para resolver cualquier asunto identificado. [ITIL:2007]

2.546.2 (EN) IT GOVERNANCE

The responsibility of executives and the board of directors; consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives

ISACA, Cybersecurity Glossary, 2014

2.546.3 (EN) GOVERNANCE

Ensuring that Policies and Strategy are actually implemented, and that required Processes are correctly followed. Governance includes defining Roles and responsibilities, measuring and reporting, and taking actions to resolve any issues identified. [ITIL:2007]

2.546.4 (FR) GOUVERNANCE

S'assurer que les politiques et la stratégie sont réellement mises en œuvre et que les processus requis sont correctement suivis. La gouvernance inclut la définition des rôles et des responsabilités, la réalisation de mesures et de rapports, ainsi la réalisation d'actions pour résoudre tout problème identifié. [ITIL:2007]

2.547 GOBIERNO, GESTIÓN DE RIESGOS Y CUMPLIMIENTO

2.547.1 GOBIERNO, GESTIÓN DE RIESGOS Y CUMPLIMIENTO

Término empleado para referirse de forma conjunta a tres disciplinas responsables de la protección de los activos y las operaciones de una empresa.

2.547.2 (EN) GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE (GRC)

A business term used to group the three close-related disciplines responsible for the protection of assets, and operations

ISACA, Cybersecurity Glossary, 2014

2.548 GOST

Ver

- RFC 4357 - Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms
- RFC 4490 - Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms witH Cryptographic Message Syntax (CMS)
- RFC 4491 - Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- RFC 5830 - GOST 28147-89: Encryption, Decryption, and Message Authentication Code (MAC) Algorithms
- RFC 5831 - GOST R 34.11-94: Hash Function Algorithm
- RFC 5832 - GOST R 34.10-2001: Digital Signature Algorithm

- RFC 5933 - Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC
- RFC 6986 - GOST R 34.11-2012: Hash Function
- RFC 7091 - GOST R 34.10-2012: Digital Signature Algorithm

2.548.1 GOST

GOST, abreviatura de Gosudarstvenny Standart (Государственный Стандарт, en español: Estándar del estado) que es un conjunto de estándares internacionales del CEI, desarrollado en la antigua URSS y actualmente mantenido por el Consejo Interestatal para la Estandartización, Meteorología y Certificación (EASC por sus siglas en inglés).

http://es.wikipedia.org/wiki/GOST

2.548.2 GOST

Algoritmo de cifrado en bloque para aplicaciones gubernamentales de la antigua Unión Soviética. Emplea bloques de 64 bits, claves de 256 bits y cajas S secretas. [CESID:1997]

2.548.3 (EN) GOST

GOST refers to a set of technical standards maintained by the Euro-Asian Council for Standardization, Metrology and Certification (EASC), a regional standards organization operating under the auspices of the Commonwealth of Independent States (CIS).

http://en.wikipedia.org/wiki/GOST

2.549 GPG - GNU PRIVACY GUARD

Acrónimos: GPG, GnuPG

Ver:

- http://www.gnupg.org/
- *PGP - Pretty Good Privacy*
- *OpenPGP - Open Pretty Good Privacy*

2.549.1 GPG

GPG o GNU Privacy Guard es una herramienta para cifrado y firmas digitales, que viene a ser un remplazo del PGP (Pretty Good Privacy) pero con la principal diferencia que es software libre licenciado bajo la GPL. GPG utiliza el estándar del IETF denominado OpenPGP.

http://es.wikipedia.org/wiki/GPG

2.549.2 (EN) GNU PRIVACY GUARD

The GNU Privacy Guard (GnuPG or GPG) is a free software replacement for the PGP suite of cryptographic software, released under the GNU General Public License. It is a part of the Free Software Foundation's GNU software project, and has received major funding from the German government. GnuPG is completely compliant with RFC 2440, the IETF standard for OpenPGP.

Current versions of PGP (and Veridis' Filecrypt) are interoperable with GnuPG and other OpenPGP-compliant systems. Although some older versions of PGP are also interoperable, not all features of newer software are supported by the older software.

http://en.wikipedia.org/wiki/GNU_Privacy_Guard

2.549.3 (FR) GNU PRIVACY GUARD

Le logiciel GNU Privacy Guard (GPG ou GnuPG) permet à ses utilisateurs de transmettre des messages signés et/ou chiffrés. Cela permet ainsi de garantir l'authenticité dans le premier cas et/ou, dans le second cas, la confidentialité du message.

GPG est un remplacement libre de la suite PGP de logiciels cryptographiques (plus précisément, de cryptographie asymétrique). Il est disponible selon les termes de la GNU General Public License.

http://fr.wikipedia.org/wiki/GPG

2.550 GUARDIA

Ver:

- *Protección del perímetro*
- *Pasarela de seguridad*

2.550.1 GUARDIA

Equipo que (a) actúa como pasarela entre dos redes sometidas a diferentes políticas de seguridad y (b) merece la confianza de ambas redes como intermediario en los intercambios de información entre ellas.

2.550.2 (EN) GUARD

(I) A computer system that (a) acts as gateway between two information systems operating under different security policies and (b) is trusted to mediate information data transfers between the two. (See: controlled interface, cross-domain solution, domain, filter. Compare: firewall.) [RFC4949:2007]

2.551 GUERRA DE INFORMACIÓN

2.551.1 GUERRA DE INFORMACIÓN

Batalla entre atacantes y defensores utilizando la información como arma.

2.551.2 (EN) ELECTRONIC WARFARE:

The use of electromagnetic (EM) or directed energy to exploit the electromagnetic spectrum. It may include interception or identification of EM emissions, employment of EM energy, preventionof hostile use of the EM spectrum by an adversary, and actions to ensure efficient employment of that spectrum by the user-State.

The Tallinn Manual, 2013

2.551.3 (EN) CYBERWARFARE

Activities supported by military organizations with the purpose to threat the survival and well-being of society/foreign entity society/foreign entity

ISACA, Cybersecurity Glossary, 2014

2.551.4 (EN) INFORMATION WARFARE

Information Warfare is the competition between offensive and defensive players over information resources.

http://www.sans.org/security-resources/glossary-of-terms/

2.552 GUÍA DE SEGURIDAD

2.552.1 GUÍA

1. Aquello que dirige o encamina.

2. Tratado en que se dan preceptos para encaminar o dirigir en cosas, ya espirituales o abstractas, ya puramente mecánicas. "Guía de pecadores. Guía del agricultor."

3. Lista impresa de datos o noticias referentes a determinada materia. "Guía del viajero. Guía de ferrocarriles."

DRAE. Diccionario de la Lengua Española.

2.552.2 DIRECTRIZ

La descripción de un modo particular de lograr algo, la cual es menos prescriptiva que un procedimiento. [COBIT:2006]

2.552.3 (EN) GUIDELINES

rules or instructions that are given by an official organization telling you how to do sth, especially sth difficult.

Oxford Advanced Learner's Dictionary.

2.552.4 (EN) SECURITY GUIDELINE

A description of a particular way of accomplishing something that is less prescriptive than a procedure. [COBIT:2006]

2.552.5 (EN) INFORMATION SECURITY GUIDELINES

An Information Security Guidelines is a suggested action or recommendation to address an area of the Information Security Policy. A security guideline is not a mandatory action, and no disciplinary action should result from non adoption. However, Information Security Guidelines are considered Best Practice and should be implemented whenever possible.

http://www.passwordnow.com/en/glossary/information-security-guidelines.html

2.553 GUSANO INFORMÁTICO

Ver:

- *Código dañino*

http://en.wikipedia.org/wiki/Computer_worm

2.553.1 GUSANO

Programa que está diseñado para copiarse y propagarse por sí mismo mediante mecanismos de red. No realizan infecciones a otros programas o ficheros. [CCN-STIC-430:2006]

2.553.2 GUSANO INFORMÁTICO

Programa que puede autoaplicarse y enviar copias de si mismo de un ordenador a otro de una red. Tras su instalación en uno de éstos repite el proceso anterior, además de realizar alguna otra tarea indeseable, quizás hasta colapsar el sistema anfitrión. [Ribagorda:1997]

2.553.3 GUSANO

Es un programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos realizan copias de ellos mismos, infectan a otros ordenadores y se propagan automáticamente en una red independientemente de la acción humana.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.553.4 (EN) WORM

Malware that is able to copy itself from one computer to another, unlike a virus that relies on embedding in another application in order to propagate itself from one computer to another.

The Tallinn Manual, 2013

2.553.5 (EN) WORM

A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. See malicious code. [CNSSI_4009:2010]

2.553.6 (EN) WORM

(I) A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume system resources destructively. (See: mobile code, Morris Worm, virus.) [RFC4949:2007]

2.553.7 (EN) WORM

A self-replicating program that is completely self-contained and self-propagating. [NIST-SP800-83:2005]

2.553.8 (EN) WORM

A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. [NIST-SP800-61:2004]

2.553.9 (EN) WORM

A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

http://www.sans.org/security-resources/glossary-of-terms/

2.553.10 (EN) WORM

A program that can replicate and send itself between computer systems. A worm can cause damage by itself or act as a delivery agent for a virus.

http://www.csoonline.com/glossary/

2.553.11 (EN) WORMS

A worm is a program that makes and facilitates the distribution of copies of itself; for example, from one disk drive to another, or by copying itself using email or another transport mechanism. The worm may do damage and compromise the security of the computer. It may arrive via exploitation of a system vulnerability or by clicking on an infected e-mail.

http://www.symantec.com/avcenter/refa.html

2.553.12 (FR) VER

Un ver est un logiciel très similaire à un virus. Cependant et contrairement au virus, un ver n'a ni besoin de l'intervention humaine, ni d'un programme hôte pour infecter une machine. Il dispose de son propre moteur, un automatisme qui lui permet de délivrer et d'exécuter automatiquement son code, comme par exemple un mini serveur de mail lui permettant de transmettre une copie de son code par e-mail, puis, par la suite, de chercher des nouvelles cibles à infecter.

http://www.cases.public.lu/functions/glossaire/

2.554 HABILITACIÓN

Ver:

- *Etiqueta de sensibilidad*
- http://en.wikipedia.org/wiki/Security_clearance

2.554.1 HABILITACIÓN

1. Atributo de los sujetos que indica el nivel de autoridad que tienen otorgado. Este nivel se usa para controlar el acceso a los objetos clasificados con cierto nivel de confidencialidad (o, en ocasiones, integridad).

2. Autorización concedida por una autoridad competente a un individuo para el acceso a informaciones clasificadas hasta un cierto nivel. (CESID)

[Ribagorda:1997]

2.554.2 HABILITACIÓN

1. De seguridad: Autorización otorgada por la autoridad competente a un individuo para el acceso a información clasificada hasta un grado determinado.

2. Propiedad que proporciona a un sujeto derechos de acceso a un recurso (privilegio).

[CESID:1997]

2.554.1 (EN) CLEARANCE

Formal certification of authorization to have access to classified information other than that protected in a special access program (including SCI). Clearances are of three types: confidential, secret, and top secret. A top secret clearance permits access to top secret, secret, and confidential material; a secret clearance, to secret and confidential material; and a confidential clearance, to confidential material. [CNSSI_4009:2010]

2.554.2 (EN) SECURITY CLEARANCE

(I) A determination that a person is eligible, under the standards of a specific security policy, for authorization to access sensitive information or other system resources. (See: clearance level.) [RFC4949:2007]

2.554.3 (EN) CLEARANCE

authorization for a subject, generally a user, to access sensitive information or other system resources. Whereas a subject or user is assigned a clearance, an object or data is given a sensitivity label.

2.554.4 (EN) PERSONNEL (SECURITY) CLEARANCE (PCL).

An administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted. [DoD 5220:2006]

2.554.5 (EN) SECURITY CLEARANCE

indicates successful completion of a security assessment; with a need to know, allows access to classified information. There are three Security Clearance levels: Confidential, Secret and Top Secret.

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

2.555 HACKER

Ver:

- *Cracker*

2.555.1 HACKER

Genio de la informática (no confundir con "cracker"). Experto en informática.

2.555.2 HACKER

Persona que a través de medios técnicos o de ingeniería social consigue acceder o introducirse en un sistema informático con intenciones diversas. Ya sea por simple entretenimiento o con la intención de descifrar el funcionamiento interno de los equipos y servidores de Internet asaltando así, los sistemas de seguridad sin ocasionar daños en ellos.

http://www.inteco.es/glossary/Formacion/Glosario/

2.555.3 HACKER / HACKING

Es el neologismo empleado para referirse a un experto. [CCN-STIC-435:2006]

2.555.4 (EN) HACKER:

A person who gains or attempts to gain unauthorized access to hardware and/or software.

The Tallinn Manual, 2013

2.555.1 (EN) HACKER

Unauthorized user who attempts to or gains access to an information system. [CNSSI_4009:2010]

2.555.2 (EN) HACKER

1. (I) Someone with a strong interest in computers, who enjoys learning about them, programming them, and experimenting and otherwise working with them. (See: hack. Compare: adversary, cracker, intruder.)

Usage: This first definition is the original meaning of the term (circa 1960); it then had a neutral or positive connotation of "someone who figures things out and makes something cool happen".

[RFC4949:2007]

2.555.3 (EN) HACKER

A term used by programmers to mean a good programmer.

2.555.4 (EN) HACKER

Hacker is a slang term for a technically sophisticated computer user who enjoys exploring computer systems and programs, sometimes to the point of obsession.

http://www.passwordnow.com/en/glossary/hacker.html

2.555.5 (FR) WHITE HAT (HACKER) / CHAPEAU BLANC

Individu possédant des connaissances de haut niveau en systèmes et réseaux de l'information et de la communication, cherchant à pénétrer des réseaux sans intention véritable de nuire, mais visant une connaissance encore plus approfondie. Souvent à rapprocher du terme "hacker". Les chapeaux

blancs sont souvent à l'origine des découvertes des failles de sécurité mais aussi des correctifs permettant de se protéger.

http://www.cases.public.lu/functions/glossaire/

2.556 HACKING

Ver:

- *Hacker*

2.556.1 HACKING

Intento no autorizado, con éxito o sin él, de acceder a un sistema de información, usualmente con malas intenciones.

2.556.2 (EN) HACKING

An attempt by an unauthorised person, whether successful or not, to access an information system, usually for malicious purposes. [CSS NZ:2011]

2.557 HACKTIVISMO

Activismo digital antisocial. Sus practicantes persiguen el control de ordenadores o sitios web para promover su causa, defender su posicionamiento político, o interrumpir servicios, impidiendo o dificultando el uso legítimo de los mismos.

2.557.1 (EN) HACKTIVIST:

A private citizen who on his or her own initiative engages in hacking for, inter alia, ideological, political, religious, or patriotic reasons.

The Tallinn Manual, 2013

2.557.2 (EN) HACKTIVIST

A portmanteau of "hacker" and "activist." Individuals that have a political motive for their activities, and identify that motivation by their actions, such as defacing opponents' websites with counter-information or disinformation.

http://cyber.law.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas

2.557.3 (EN) HACTIVISM

hacking for a politically or socially motivated purpose[ISO/IEC 27032:2012]

2.557.4 (EN) HACKTIVISM

Hacktivists seek to gain control over computer systems or websites to manipulate them to promote a cause, make a political statement or disrupt services, for example, by overloading websites with botnet attacks, which can deny or prevent the legitimate use of the service. [NZ CSS:2011]

2.557.5 (EN) HACKTIVISM

Hacktivism uses cyber attacks based on political motivations who use cyber sabotage to promote a specific cause. As opposed to the hacking industry intent on data theft, hacktivism is not motivated by money and high visibility is key. Hacktivisms are motivated by revenge, politics, ideology, protest and a desire to humiliate victims. Profit is not a factor. And visibility is key: what's the point of embarrassing someone if you they didn't know who performed the attack?

http://www.imperva.com/resources/glossary/glossary.html

2.558 HALONES

2.558.1 HALONES

Familia de agentes extintores halogenados de acción anticatalítica y pequeña toxicidad. Fueron profusamente usados hasta que su gran efecto destructor de la capa de ozono (su ODP, Ozone depletion potential, llega a alcanzar la cifra de 10, valor elevadísimo) hizo que su producción fuese prohibida por la convención de Montreal.

Sus componentes más populares son el Halón 1211, usado en extintores manuales, el halón 1301, usado en procedimientos de inundación y el halón 2402.

[Ribagorda:1997]

2.558.2 (EN) HALON

Halon 1211 and Halon 1301 are special-purpose fire extinguishing agents that were banned by the Montreal Protocol.

http://en.wikipedia.org/wiki/Halon

2.559 HANDSHAKING

2.559.1 HANDSHAKING

Diálogo entre dos sistemas de información para sincronizarse, identificarse y autenticarse entre sí.

2.559.2 (EN) HANDSHAKING PROCEDURES

Dialogue process between two information systems for synchronizing, identifying, and authenticating themselves to one another. [CNSSI_4009:2010]

2.560 HASH

Ver:

- *Hash code*
- *Valor resumen*
- *Resumen criptográfico*
- *Función resumen*
- *Resistente a colisiones*
- *MD2 - algoritmo resumen*

- *MD4 - algoritmo resumen*
- *MD5 - algoritmo resumen*
- *RIPEMD*
- *SHA - Secure Hash Algorithm*
- *Whirlpool - Algoritmo resumen (hash)*

2.561 HASH CODE

Ver:

- *Valor resumen*
- *Resumen criptográfico*
- *Función resumen*
- *Hash*

2.561.1 HASH CODE

Bits obtenidos como resultado de aplicar una función resumen a unos datos.

2.561.2 (EN) HASH-CODE

The string of bits which is the output of a hash-function.

NOTE. The literature on this subject contains a variety of terms that have the same or similar meaning as hash-code. Modification Detection Code, Manipulation Detection Code, digest, hash-result, hash-value and imprint are some examples.

[ISO-10118-1:2000]

2.562 HEARTBLEED

Ver

- *TLS - Transport Layer Security*
- *SSL - Secure Sockets Layer*

2.562.1 HEARTBLEED

Heartbleed (español: hemorragia de corazón) es un agujero de seguridad (bug) de software en la biblioteca de código abierto OpenSSL, solo vulnerable en su versión 1.0.1f, que permite a un atacante leer la memoria de un servidor o un cliente, permitiéndole por ejemplo, conseguir las claves privadas SSL de un servidor.

http://es.wikipedia.org/wiki/Heartbleed

2.562.2 (EN) HEARTBLEED

Heartbleed is a security bug in the OpenSSL cryptography library that gained widespread attention in April 2014. OpenSSL is a widely used implementation of the Transport Layer Security (TLS) protocol. Heartbleed may be exploited whether the party using a vulnerable OpenSSL instance for TLS is a server or a client. Heartbleed results from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension, the heartbeat being the basis

for the bug's name. The vulnerability is classified as a buffer over-read, a situation where software allows more data to be read than should be allowed.

http://en.wikipedia.org/wiki/Heartbleed

2.563 HIPAA - HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT

Acrónimos: HIPAA

2.563.1 HIPAA - HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT

Norma norteamericana relativa a los historiales médicos de los pacientes, estableciendo requisitos de seguridad en los sistemas de almacenamiento y transmisión.

2.563.2 (EN) HIPAA

(N) Health Information Portability and Accountability Act of 1996, a U.S. law (Public Law 104-191) that is intended to protect the privacy of patients' medical records and other health information in all forms, and mandates security for that information, including for its electronic storage and transmission. [RFC4949:2007]

2.563.3 (EN) HIPAA

HIPAA is the United States Health Insurance Portability and Accountability Act of 1996. There are two sections to the Act. HIPAA Title I deals with protecting health insurance coverage for people who lose or change jobs. HIPAA Title II includes an administrative simplification section which deals with the standardization of healthcare-related information systems. In the information technology industries, this section is what most people mean when they refer to HIPAA. HIPAA establishes mandatory regulations that require extensive changes to the way that health providers conduct business.

http://whatis.techtarget.com/

2.563.4 (EN) HIPAA

U.S. law that protects employees' health insurance coverage when they change or lose their jobs (Title I) and provides standards for patient health, and administrative and financial data interchange (Title II). The latter also governs the privacy and security of health information records and transactions, and recommends the use of encryption. HIPAA took effect in 2001 with compliance required in phases up to 2004.

http://www.spectralogic.com/index.cfm?fuseaction=home.displayFile&DocID=1235

2.564 HMAC - HASH-BASED MESSAGE AUTHENTICATION CODE

Acrónimos: HMAC

Ver:

- http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf
- http://www.ietf.org/rfc/rfc4634
- http://www.ietf.org/rfc/rfc4231

- http://www.ietf.org/rfc/rfc2286
- http://www.ietf.org/rfc/rfc2202
- http://www.ietf.org/rfc/rfc2104
- *CMAC authentication mode*

2.564.1 HMAC - HASH-BASED MESSAGE AUTHENTICATION CODE

Técnica de autenticación de mensajes que incluye una clave secreta. De esta forma se detecta la manipulación del contenido al tiempo que se chequea una clave de autenticación.

2.564.2 (EN) HASH-BASED MESSAGE AUTHENTICATION CODE (HMAC)

A message authentication code that uses a cryptographic key in conjunction with a hash function. [CNSSI_4009:2010]

2.564.3 (EN) HMAC

(I) A keyed hash [R2104] that can be based on any iterated cryptographic hash (e.g., MD5 or SHA-1), so that the cryptographic strength of HMAC depends on the properties of the selected cryptographic hash. (See: [R2202, R2403, R2404].) [RFC4949:2007]

2.564.4 (EN) HMAC - HASH-BASED MESSAGE AUTHENTICATION CODE

a message authentication code that utilizes a keyed hash. [FIPS-140-2:2001]

2.565 HOLOCRÍPTICO

Ver:

- *Seguridad incondicional*

2.565.1 HOLOCRÍPTICO

Sistema incondicionalmente seguro u holocriptico: Criptosistema en el que matemáticamente se puede demostrar que sin el conocimiento de la clave no se puede obtener el texto claro correspondiente a un texto cifrado. [CESID:1997]

2.565.2 (EN) HOLOCRIPTIC

Wholly or completely concealing; incapable of being deciphered.

Holocryptic cipher: a cipher so constructed as to afford no clew to its meaning to one ignorant of the key.

2.566 HOT STANDBY

Ver:

- *Opción de recuperación*
- *Sala preparada*

2.566.1 RECUPERACIÓN RÁPIDA

(Diseño del Servicio) Una Opción de Recuperación que es también conocida como Reserva Caliente. Recuperación del Servicio de TI en un corto período de tiempo, típicamente menos de 24 horas. La Recuperación Rápida normalmente usa una Facilidad Fija dedicada con Sistemas y Software configurado y dispuesto a correr los Servicios de TI. La Recuperación Inmediata puede llevar hasta 24 horas si hay necesidad de Recuperar datos de Copias de Respaldo. [ITIL:2007]

2.566.2 RECUPERACIÓN INMEDIATA

(Diseño del Servicio) Opción de Recuperación también conocida como Reserva Medio. Recuperación del Servicio de TI en un periodo de tiempo entre 24 y 72 horas. La recuperación Intermedia emplea normalmente Facilidades Fijas o Portátiles compartidas que contienen Sistemas informáticos y Componentes de Red. El hardware y software necesita ser configurado y los datos deben ser restaurados como parte integrante del Plan de Continuidad del Servicio de TI. [ITIL:2007]

2.566.3 (EN) HOT STANDBY

Synonym for Fast Recovery or Immediate Recovery. [ITIL:2007]

2.566.4 (EN) FAST RECOVERY

(Service Design) A Recovery Option which is also known as Hot Standby. Provision is made to Recover the IT Service in a short period of time, typically less than 24 hours. Fast Recovery typically uses a dedicated Fixed Facility with computer Systems, and software configured ready to run the IT Services. Immediate Recovery may take up to 24 hours if there is a need to Restore data from Backups. [ITIL:2007]

2.566.5 (EN) IMMEDIATE RECOVERY

(Service Design) A Recovery Option which is also known as Hot Standby. Provision is made to Recover the IT Service with no loss of Service. Immediate Recovery typically uses mirroring, load balancing and split site technologies. [ITIL:2007]

2.566.6 (FR) REPRISE RAPIDE

(Conception de services) Une option de reprise également connue sous le nom de reprise immédiate (Hot Standby). Une provision est effectuée afin de reprendre le service des TI dans les plus brefs délais, normalement en moins de 24 heures. La reprise immédiate utilise habituellement un lieu (local ?) fixe dédié, équipé de systèmes informatiques et de logiciels configurés prêts à fonctionner pour relancer les services des TI. Une reprise immédiate peut prendre jusqu'à 24 heures s'il est nécessaire de restaurer les données à partir de copies de sauvegarde. [ITIL:2007]

2.566.7 (FR) REPRISE IMMÉDIATE

(Conception de services) Une option de reprise également connue sous le nom de Hot Standby. Une provision est effectuée afin de reprendre le service des TI sans aucune perte de service. La reprise immédiate utilise habituellement des technologies de sites miroir, de sites dédoublés avec équilibrage des charges. [ITIL:2007]

2.567 HTTP SEGURO

Acrónimos: HTTPS

Ver:

- *SSL - Secure Sockets Layer*

2.567.1 HTTPS

Acrónimo de “hypertext transfer protocol over secure socket layer” (protocolo de transferencia de hipertexto a través de una capa de conexión segura). HTTP seguro que proporciona autenticación y comunicación cifrada en la World Wide Web diseñado para comunicaciones que dependen de la seguridad, tales como los inicios de sesión basados en la web.

http://es.pcisecuritystandards.org

2.567.2 HTTP SEGURO

Ejecución del protocolo HTTP (intercambios web) sobre un túnel SSL que proporciona seguridad: autenticación, confidencialidad e integridad.

2.567.1 (EN) HTTPS

Acronym for “hypertext transfer protocol over secure socket layer.” Secure HTTP that provides authentication and encrypted communication on the World Wide Web designed for security-sensitive communication such as web-based logins.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.567.2 (EN) HTTPS

(I) When used in the first part of a URL (the part that precedes the colon and specifies an access scheme or protocol), this term specifies the use of HTTP enhanced by a security mechanism, which is usually SSL. (Compare: S-HTTP.) [RFC4949:2007]

2.567.3 (FR) HTTPS

Acronyme de «hypertext transfer protocol over secure socket layer», protocole de transfert hypertexte sur couche de socket sécurisée. Protocole HTTP sécurisé fournissant une authentification et une communication cryptée sur le Web, conçu pour les communications de sécurité sensible, comme les connexions en ligne.

http://fr.pcisecuritystandards.org/

2.567.4 (FR) HTTPS - SECURE HYPERTEXT TRANSFER PROTOCOL

HTTPS est une version sécurisée de HTTP assurant les services de sécurité:

- Authentification (éventuellement mutuelle).
- Confidentialité (chiffrement des données échangées).
- Intégrité des données (au cours de leur transport).

HTTPS s'appuie sur le protocole SSL et les algorithmes cryptographiques associés, de sorte qu'il supporte les certificats X.509.

HTTPS utilise le port standard 443.

Remarque. ne pas confondre HTTPS et SHTTP.

http://securit.free.fr/glossaire.htm

2.568 HUELLA DIGITAL

Ver:

- *Hash*

2.568.1 HUELLA DIGITAL

Característica de un conjunto de datos, como el valor obtenido al aplicarlos una función resumen, específica de los mismos, tal que es computacionalmente inviable encontrar otro conjunto de datos que posea la misma característica (ISO/IEC ISO-10181-2). [Ribagorda:1997]

2.568.2 HUELLA DACTILAR DIGITAL

Característica de un ítem de datos, por ejemplo un valor de comprobación criptográfico o el resultado de la ejecución de una función de cálculo unidireccional sobre los datos, que es suficientemente peculiar del ítem de datos y que no es factible, mediante cálculo, hallar otro ítem de datos que posea las mismas características. [X.810:1995]

2.568.3 (EN) DIGITAL FINGERPRINT

A characteristic of a data item, such as a cryptographic check-value or the result of performing a one-way hash function on the data, that is sufficiently peculiar to the data item that it is computationally infeasible to find another data item that will possess the same characteristics. [X.810:1995]

2.568.4 (FR) EMPREINTE NUMÉRIQUE

caractéristique d'un élément de données, telle qu'une valeur de contrôle cryptographique ou le résultat de la réalisation d'une fonction de hachage unidirectionnelle sur les données, qui est suffisamment spécifique à l'élément de données pour qu'il ne soit pas possible de trouver, de façon informatique, un autre élément de données ayant les mêmes caractéristiques. [X.810:1995]

2.569 HUELLA DIGITAL

Ver:

- *Protección de derechos de autor*
- *Marcas de agua*

2.569.1 FINGERPRINTING

La huella digital es un mecanismo para defender los derechos de autor y combatir la piratería que consiste en introducir una serie de bits imperceptibles sobre un producto de soporte electrónico (CD-ROM, DVD,...) de forma que se puedan detectar las copias ilegales.

http://es.wikipedia.org/wiki/Fingerprinting

2.569.2 (EN) FINGERPRINTING

Another name for digital watermarking, a Digital Rights Management (DRM) antipiracy and copy-protection technology.

2.570 IA

Acrónimos: I&A

Ver:

- *Identificación*
- *Autenticación*

2.571 IDEA - INTERNATIONAL DATA ENCRYPTION ALGORITHM

Acrónimos: IDEA

Ver:

- *Cifrado en bloque*
- *Criptografía de clave secreta*

2.571.1 IDEA - INTERNATIONAL DATA ENCRYPTION ALGORITHM

Algoritmo de cifra basado en un secreto compartido (clave). Cifra el texto en bloques de 64 bits. Utiliza claves de 128 bits.

2.571.2 IDEA

Algoritmo de cifra creado durante los primeros años de la década de los 90 por Lay y Masey con el nombre de International Data Encryption Algorithm (más conocido por sus siglas, IDEA).

Es un cifrado de bloque, que opera sobre textos en claro de 64 bits con una clave de 128 bits (sin paridad). El algoritmo usado en el descifrado es el mismo que el empleado en el cifrado.

IDEA una tanto técnicas de confusión como de difusión, realizando complejas operaciones matemáticas (o-exclusivo, adiciones módulo 2 16 y multiplicaciones módulo 2 16) sobre subbloques de 16 bits de entrada. Esto último significa que el algoritmo es eficiente incluso con procesadores de 16 bits.

En opinión de numerosos criptógrafos, IDEA es el mejor y más recomendable cifrado de bloque de los que actualmente se comercializan, siendo muchos los que lo consideran el mejor sustituto al venerable DES. Prueba de lo anterior se tiene en los numerosos paquetes de programas de seguridad para ordenadores personales o redes que incluyen el IDEA como algoritmo de cifrado.

[Ribagorda:1997]

2.571.3 IDEA

Algoritmo público, diseñado por X. Lay y J. Massey en 1990, de cifrado en bloque de 64 bits que emplea claves de 128 bits. [CESID:1997]

2.571.4 (EN) INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA)

(N) A patented, symmetric block cipher that uses a 128-bit key and operates on 64-bit blocks. [Schn] (See: symmetric cryptography.) [RFC4949:2007]

2.571.5 (EN) IDEA

The International Data Encryption Algorithm is an encryption algorithm created by Xuejia Lai and James Massey in 1992 that uses a block cipher with a 128-bit key (64-bit blocks with a 128 bit key), and is generally considered to be very secure. It is considered among the best publicly known algorithms. In the several years that it has been in use, no practical attacks on it have been published despite of a number of attempts to find some.

2.572 IDENTIDAD

Ver:

- *Identificación*
- *Robo de identidades*
- *Identidad federada*

2.572.1 IDENTIDAD

Conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás.

DRAE. Diccionario de la Lengua Española.

2.572.2 IDENTIDAD

(Operación del Servicio) Un nombre único empleado para identificar a un Usuario, persona o Rol. La identidad se usa para garantizar Derechos a ese Usuario, persona o Rol. Ejemplos pueden ser "Nombre de Usuario = SmithJ" o "el Rol de 'Gestor de Cambios'". [ITIL:2007]

2.572.3 (EN) IDENTITY

A set of attributes that uniquely describe a person within a given context. [NIST-SP800-63:2013]

2.572.4 IDENTITY PROOFING

The process by which a CSP and a Registration Authority (RA) collect and verify information about a person for the purpose of issuing credentials to that person. [NIST-SP800-63:2013]

2.572.5 (EN) IDENTITY

The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager’s responsibility, is sufficient to distinguish that entity from any other entity. [CNSSI_4009:2010]

2.572.6 (EN) IDENTITY REGISTRATION

The process of making a person's identity known to the Personal Identity Verification (PIV) system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system. [CNSSI_4009:2010]

2.572.7 (EN) IDENTITY

(I) The collective aspect of a set of attribute values (i.e., a set of characteristics) by which a system user or other system entity is recognizable or known. (See: authenticate, registration. Compare: identifier.) [RFC4949:2007]

2.572.8 (EN) IDENTITY

(Service Operation) A unique name that is used to identify a User, person or Role. The Identity is used to grant Rights to that User, person, or Role. Example identities might be the username SmithJ or the Role "Change manager". [ITIL:2007]

2.572.9 (EN) IDENTITY

The distinguishing character or personality of an individual or entity. [NIST-SP800-57:2007]

2.572.10 (EN) IDENTITY

a representation (e.g. a string) uniquely identifying an authorised user, which can either be the full or abbreviated name of that user or a pseudonym. [CC:2006]

2.572.11 (EN) IDENTITY

Information that is unique within a security domain and which is recognized as denoting a particular entity within that domain. [NIST-SP800-33:2001]

2.572.12 (EN) AUTHENTICATED IDENTITY

A distinguishing identifier of a principal that has been assured through authentication. [ISO-10181-2:1996]

2.572.13 (EN) IDENTITY

Identity is whom someone or what something is, for example, the name by which something is known.

2.572.14 (EN) IDENTITY

A reference or designation used to distinguish a unique and particular individual, organization or device.

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

2.572.15 (EN) IDENTITY MANAGEMENT

The set of principles, practices, processes and procedures used to realize an organization's mandate and its objectives related to identity.

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

2.572.16 (FR) IDENTITÉ

(Exploitation de Services) Un nom unique servant identifier un utilisateur, une personne ou un rôle. L'identité permet de garantir les droits de cet utilisateur, personne ou rôle. Des exemples d'identités peuvent être un nom d'usage comme SmithJ ou de rôle comme "Gestionnaire des changements". [ITIL:2007]

2.572.17 (FR) IDENTITÉ

Référence ou désignation utilisée pour distinguer une personne, une organisation ou un appareil unique et particulier.

http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578

2.572.18 (FR) GESTION DE L'IDENTITÉ

Ensemble de principes, de pratiques, de processus et de procédures permettant de remplir le mandat d'une organisation et d'atteindre ses objectifs liés à l'identité.

http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578

2.573 IDENTIDAD FEDERADA

Ver:

- *Identidad*
- *Infraestructura de clave pública*

2.573.1 IDENTIDAD FEDERADA)

(n.) Fusión de la información de cuenta de todos los proveedores de servicios a los que accede un usuario (por ejemplo, datos personales, información de autenticación, hábitos e historial de compra, preferencias de compra, etc.). El usuario proporciona la información y, con el consentimiento del usuario, se comparte de forma segura con el proveedor que haya elegido el usuario.

http://docs.sun.com/app/docs/doc/819-4627?l=es

2.573.2 (EN) FEDERATED IDENTITY MANAGEMENT (FIM)

is an arrangement that can be made among multiple enterprises that lets subscribers use the same identification data to obtain access to the networks of all enterprises in the group. The use of such a system is sometimes called identity federation.

Identity federation offers economic advantages, as well as convenience, to enterprises and their network subscribers. For example, multiple corporations can share a single application, with resultant cost savings and consolidation of resources. In order for FIM to be effective, the partners

must have a sense of mutual trust. Authorization messages among partners in an FIM system can be transmitted using Security Assertion Markup Language (SAML) or a similar XML standard that allows a user to log on once for affiliated but separate Web sites or networks.

http://searchsoftwarequality.techtarget.com/glossary/

2.574 IDENTIFICACIÓN

Ver:

- *Identidad*
- *Autenticación*

2.574.1 IDENTIFICACIÓN

Procedimiento de reconocimiento de la identidad de un usuario.

Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

2.574.2 IDENTIFICACIÓN ELECTRÓNICA

«identificación electrónica», el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica; [PE-CONS 60/14]

2.574.3 MEDIOS DE IDENTIFICACIÓN ELECTRÓNICA

«medios de identificación electrónica», una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea; [PE-CONS 60/14]

2.574.4 DATOS DE IDENTIFICACIÓN DE LA PERSONA

«datos de identificación de la persona», un conjunto de datos que permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a una persona jurídica; [PE-CONS 60/14]

2.574.5 SISTEMA DE IDENTIFICACIÓN ELECTRÓNICA

«sistema de identificación electrónica», un régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a las personas físicas o jurídicas o a una persona física que representa a una persona jurídica; [PE-CONS 60/14]

2.574.6 (EN) ELECTRONIC IDENTIFICATION

'electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person; [PE-CONS 60/14]

2.574.7 (EN) ELECTRONIC IDENTIFICATION MEANS

'electronic identification means' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service; [PE-CONS 60/14]

2.574.8 (EN) 'PERSON IDENTIFICATION DATA'

'person identification data' means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established; [PE-CONS 60/14]

2.574.9 (EN) ELECTRONIC IDENTIFICATION SCHEME

'electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons; [PE-CONS 60/14]

2.574.1 (EN) IDENTIFICATION

An act or process that presents an identifier to a system so that the system can recognize a system entity (e.g., user, process, or device) and distinguish that entity from all others. [CNSSI_4009:2010]

2.574.2 (EN) IDENTIFICATION

(I) An act or process that presents an identifier to a system so that the system can recognize a system entity and distinguish it from other entities. (See: authentication.) [RFC4949:2007]

2.574.3 (FR) IDENTIFICATION ÉLECTRONIQUE

"identification électronique", le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale; [PE-CONS 60/14]

2.574.4 (FR) MOYEN D'IDENTIFICATION ÉLECTRONIQUE

"moyen d'identification électronique", un élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne; [PE-CONS 60/14]

2.574.5 (FR) DONNÉES D'IDENTIFICATION PERSONNELLE

"données d'identification personnelle", un ensemble de données permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale; [PE-CONS 60/14]

2.574.6 (FR) SCHÉMA D'IDENTIFICATION ÉLECTRONIQUE

"schéma d'identification électronique", un système pour l'identification électronique en vertu duquel des moyens d'identification électronique sont délivrés à des personnes physiques ou morales, ou à des personnes physiques représentant des personnes morales; [PE-CONS 60/14]

2.575 IDENTIFICACIÓN DE LOS RIESGOS

Ver:

- *Riesgo*

2.575.1 IDENTIFICACIÓN DE LOS RIESGOS

Identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información.

2.575.2 IDENTIFICACIÓN DEL RIESGO

Proceso que comprende la búsqueda, el reconocimiento y la descripción de los riesgos. [UNE-ISO GUÍA 73:2010]

NOTA 1 La identificación del riesgo implica la identificación de las fuentes de riesgo, los sucesos, sus causas y sus consecuencias potenciales.

NOTA 2 La identificación del riesgo puede implicar datos históricos, análisis teóricos, opiniones informadas y de expertos, así como necesidades de las partes interesadas.

[UNE-ISO/IEC 27000:2014]

2.575.3 IDENTIFICACIÓN DEL RIESGO:

Proceso que comprende la búsqueda, el reconocimiento y la descripción de los riesgos.

NOTA 1. La identificación del riesgo implica la identificación de las fuentes de riesgo, los sucesos, sus causas y sus consecuencias potenciales

[UNE Guía 73:2010]

2.575.4 (EN) RISK IDENTIFICATION

process of finding, recognizing and describing risks [ISO Guide 73:2009]

NOTE 1: Risk identification involves the identification of risk sources, events, their causes and their potential consequences.

NOTE 2: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs.

[ISO/IEC 27000:2014]

2.575.5 (EN) RISK IDENTIFICATION

process of finding, recognizing and describing risks

NOTE 1. Risk identification involves the identification of risk sources, events, their causes and their potential consequences

[ISO Guide 73:2009]

2.575.6 (EN) RISK IDENTIFICATION

process of finding, recognizing, and describing potential risks

DHS Risk Lexicon, September 2008

2.575.7 (FR) IDENTIFICATION DES RISQUES

processus de recherche, de reconnaissance et de description des risques

NOTE 1. L'identification des risques comprend l'identification des sources de risque, des événements, de leurs causes et de leurs conséquences potentielles.

[ISO Guide 73:2009]

2.576 IDENTIFICADOR

2.576.1 IDENTIFICADOR

Datos que representan una identidad singular, distinta de todas las demás. Típicamente, una cadena de caracteres.

2.576.2 (EN) IDENTIFIER

A data object - often, a printable, non-blank character string - that definitively represents a specific identity of a system entity, distinguishing that identity from all others. [CNSSI_4009:2010]

2.577 IEEE 802.11I

Acrónimos: 802.11i, WPA2

Ver:

- *WEP - Wired Equivalent Privacy*
- *WPA - Wi-Fi Protected Access*

2.577.1 IEEE 802.11I

Estándar para asegurar redes inalámbricas 802.11. También se conoce como WPA2 y sustituye al WEP original.

2.577.2 (EN) IEEE 802.11I

IEEE 802.11i, also known as WPA2, is an amendment to the 802.11 standard specifying security mechanisms for wireless networks (see Wi-Fi). The draft standard was ratified on 24 June 2004, and supersedes the previous security specification, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses. Wi-Fi Protected Access (WPA) had previously been introduced by the Wi-Fi Alliance as an intermediate solution to WEP insecurities. WPA implemented a subset of 802.11i. The Wi-Fi Alliance refers to their approved, interoperable implementation of the full 802.11i as WPA2. 802.11i makes use of the Advanced Encryption Standard (AES) block cipher; WEP and WPA use the RC4 stream cipher.

http://en.wikipedia.org/wiki/IEEE_802.11i

2.578 IEEE P1363 - STANDARD FOR PUBLIC-KEY CRYPTOGRAPHY

Ver:

- http://grouper.ieee.org/groups/1363/
- *DSA - Digital Signature Algorithm*
- *ECDSA - Elliptic Curve Digital Signature Algorithm*
- *RSA - Rivest, Shamir y Adelman*
- *Negociación de claves*
- *Firma digital*
- *Cifrado*

2.578.1 IEEE P1363 - STANDARD FOR PUBLIC-KEY CRYPTOGRAPHY

Grupo de trabajo del IEEE dedicado a la criptografía de clave pública.

2.578.2 (EN) IEEE P1363

(N) An IEEE working group, Standard for Public-Key Cryptography, engaged in developing a comprehensive reference standard for asymmetric cryptography. Covers discrete logarithm (e.g., DSA), elliptic curve, and integer factorization (e.g., RSA); and covers key agreement, digital signature, and encryption. [RFC4949:2007]

2.579 IKE - INTERNET KEY EXCHANGE

Acrónimos: IKE

Ver:

- http://www.ietf.org/rfc/rfc4306
- *IPsec - IP security*
- *Asociación de seguridad (SA)*

2.579.1 IKE - INTERNET KEY EXCHANGE

Internet Key Exchange es un protocolo usado para establecer una asociación de seguridad (SA) en el protocolo IPsec. [CCN-STIC-414:2006]

2.579.2 (EN) IKE (INTERNET KEY EXCHANGE)

A standard proposed in RFC 2409 used with IPSec virtual private networks (VPNs) for automating the process of negotiating encryption keys, changing keys, and determining when to change keys. IKE first mutually authenticates the two endpoints that plan to set up IPSec tunnels between them; then the endpoints can establish mutually agreed-upon security parameters.

http://www.watchguard.com/glossary/

2.580 IMPACTO

Ver:

- *consecuencia*

2.580.1 IMPACTO

Huella o señal que deja.

DRAE. Diccionario de la Lengua Española.

2.580.2 IMPACTO

(Operación del Servicio) (Transición del Servicio) Una medida del efecto de un Incidente, Problema o Cambio en los Procesos de Negocio. El Impacto está a menudo basado en como serán afectados los Niveles de Servicio. El Impacto y la Urgencia se emplean para asignar la Prioridad. [ITIL:2007]

2.580.3 IMPACTO

Consecuencia que sobre un activo tiene la materialización de una amenaza. [Magerit:2012]

2.580.4 IMPACTO RESIDUAL

Impacto remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información. [Magerit:2012]

2.580.5 IMPACTO

Consecuencia para el organismo de la materialización de una amenaza. [EBIOS:2005]

2.580.6 (EN) IMPACT LEVEL

The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. [CNSSI_4009:2010]

2.580.7 (EN) POTENTIAL IMPACT

The loss of confidentiality, integrity, or availability that could be expected to have a limited (low) adverse effect, a serious (moderate) adverse effect, or a severe or catastrophic (high) adverse effect on organizational operations, organizational assets, or individuals. [CNSSI_4009:2010]

2.580.8 (EN) IMPACT

(Service Operation) (Service Transition) A measure of the effect of an Incident, Problem or Change on Business Processes. Impact is often based on how Service Levels will be affected. Impact and Urgency are used to assign Priority. [ITIL:2007]

2.580.9 (EN) POTENTIAL IMPACT

The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals. [FIPS 199]

2.580.10 (EN) IMPACT

evaluated consequence of a particular outcome. [BS25999-1:2006]

2.580.11 (EN) IMPACT

Consequences for an organisation when a threat is accomplished. [EBIOS:2005]

2.580.12 (EN) IMPACT

The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. [NIST-SP800-60V2:2004]

2.580.13 (EN) IMPACT

The effect of a threat on an organization's mission and business objectives. [Octave:2003]

2.580.14 (EN) IMPACT

The effect on the organisation of a breach in security. [CRAMM:2003]

2.580.15 (EN) IMPACT

The effect, acceptable or unacceptable, of an incident on a system, operation, schedule, or cost. Unacceptable impact is impact deemed, by the system owner and as compared to the missions and goals of the U.S. Department of Defense (DOD), as severe enough to degrade an essential mission, capability, function, or system causing an unacceptable result. Like impact, unacceptable impact refers to the total system and all areas of operational concern, not only confidentiality.

http://www.symantec.com/avcenter/refa.html

2.580.16 (EN) IMPACT

Impact is the effect that the organization using vulnerable software faces if a vulnerability were to be exploited. Impact could range from specific tangible values such as monetary fines from the breach of a law or regulation to intangible values such as brand and reputation damage.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/attack/590-BSI.html

2.580.17 (FR) IMPACT

(Exploitation de Services) (Transition de Services) Mesure de l'effet d'un incident, problème ou changement sur les processus business. L'impact est souvent basé sur la manière dont les niveaux de service seront affectés. L'impact et l'urgence servent à assigner une priorité. [ITIL:2007]

2.580.18 (FR) IMPACT

Conséquence sur l'organisme de la réalisation d'une menace. [EBIOS:2005]

2.580.19 (FR) IMPACT

Une des composantes de l'évaluation des risques est la mesure des impacts possibles. Il va de soi que la dynamique des faiblesses d'un système d'information et de communication et de son exploitation va engendrer une multitude d'impacts possibles et que la valeur des éléments impliqués va permettre de définir le risque encouru.

Il faut, dans un premier temps, faire une distinction entre les dégâts causés par un événement et l'impact résultant de cet événement.

http://www.cases.public.lu/functions/glossaire/

2.581 IMPOSTURA

Ver:

- *Robo de identidades*
- *Spoof*

2.581.1 IMPOSTURA

Pretensión de una entidad de ser otra diferente, para así acceder sin autorización a los recursos a los que aquella tiene acceso. (ISO-7498-2). [Ribagorda:1997]

2.581.2 DECEPCIÓN IMITATIVA O SUPLANTACIÓN

Pretensión de una entidad de hacerse pasar por otra y transmitir mensajes por una red no estando autorizada a ello. [CESID:1997]

2.581.3 USURPACIÓN DE IDENTIDAD (O IMPOSTURA)

Pretención de una entidad de pasar por una entidad diferente. [ISO-7498-2:1989]

2.581.4 (EN) MASQUERADING

A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity. [CNSSI_4009:2010]

2.581.5 (EN) MASQUERADE

(I) A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity. (See: deception.)

Usage: This type of threat action includes the following subtypes:

- "Spoof": Attempt by an unauthorized entity to gain access to a system by posing as an authorized user.
- "Malicious logic": In context of masquerade, any hardware, firmware, or software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic. (See: corruption, incapacitation, main entry for "malicious logic", misuse.)

[RFC4949:2007]

2.581.6 (EN) MASQUERADE ATTACK

A type of attack in which one system entity illegitimately poses as (assumes the identity of) another entity.

http://www.sans.org/security-resources/glossary-of-terms/

2.581.7 (EN) MASQUERADE

The pretence by an entity to be a different entity. [ISO-7498-2:1989]

2.581.8 (FR) USURPATION D'IDENTITÉ

Prétention qu'a une entité d'en être une autre. [ISO-7498-2:1989]

2.581.9 (FR) MASQUERADE

L'usurpation par un entité qui se révèle être une entité différente de celle annoncée.

http://www.cases.public.lu/functions/glossaire/

2.582 IMPUTABILIDAD

Ver:

- *Trazabilidad (imputabilidad)*

2.583 INCIDENTE

Ver:

- *Evento*
- *Incidente de seguridad*
- *Gestión de incidentes*

2.583.1 INCIDENTE

Que sobreviene en el curso de un asunto o negocio y tiene con este algún enlace.

DRAE. Diccionario de la Lengua Española.

2.583.2 INCIDENTE

(Operación del Servicio) Interrupción no planificada de un Servicio de TI o reducción en la Calidad de un Servicio de TI. También lo es el Fallo de un Elemento de Configuración que no ha impactado todavía en el Servicio. Por ejemplo el Fallo de uno de los discos de un "mirror". [ITIL:2007]

2.583.3 INCIDENTE

Cualquier evento que no sea parte de la operación estándar de un servicio que ocasione, o pueda ocasionar, una interrupción o una reducción de la calidad de ese servicio (alineado a ITIL). [COBIT:2006]

2.583.4 INCIDENCIA

Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

2.583.5 (EN) INCIDENT

something that happens, especially sth unusual or unpleasant.

Oxford Advanced Learner's Dictionary.

2.583.1 (EN) INCIDENT

An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [CNSSI_4009:2010]

2.583.2 (EN) INCIDENT

occurrence, caused by either human action or natural phenomena, that may cause harm and that may require action

Annotation:

1. Homeland security incidents can include major disasters, emergencies, terrorist attacks, terrorist threats, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, law enforcement encounters and other occurrences requiring a mitigating response.
2. Harm can include human casualties, destruction of property, adverse economic impact, and/or damage to natural resources.

DHS Risk Lexicon, September 2008

2.583.3 (EN) INCIDENT

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. [NIST-SP800-94:2007]

2.583.4 (EN) INCIDENT

(Service Operation) An unplanned interruption to an IT Service or a reduction in the Quality of an IT Service. Failure of a Configuration Item that has not yet impacted Service is also an Incident. For example Failure of one disk from a mirror set. [ITIL:2007]

2.583.5 (EN) INCIDENT

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [FIPS-200:2006]

2.583.6 (EN) INCIDENT

situation that might be, or could lead to, a business disruption, loss, emergency or crisis. [BS25999-1:2006]

2.583.7 (EN) INCIDENT

Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service (aligned to ITL). [COBIT:2006]

2.583.8 (EN) INCIDENT

The actualization of a risk. The event or result of a threat that exploits a system vulnerability.

http://www.symantec.com/avcenter/refa.html

2.583.9 (FR) INCIDENT

(Exploitation de Services) Une interruption non prévue (planifiée ?) d'un service des TI ou une réduction de la qualité d'un service des TI. La défaillance d'un élément de configuration qui n'a pas encore eu d'impact sur le service est aussi un incident. Par exemple, la défaillance d'un seul des disques d'un ensemble de disques miroirs. [ITIL:2007]

2.584 INCIDENTE DE SEGURIDAD

Ver:

- *Incidente*

2.584.1 INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Evento singular o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información. [UNE-ISO/IEC 27000:2014]

2.584.2 INCIDENTE DE SEGURIDAD

Suceso (inesperado o no deseado) con consecuencias en detrimento de la seguridad del sistema de información. [UNE-71504:2008]

2.584.1 (EN) INFORMATION SECURITY INCIDENT

single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security [ISO/IEC 27000:2014]

2.584.1 (EN) INCIDENT

An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [CNSSI_4009:2010]

2.584.2 (EN) SECURITY INCIDENT

1. (I) A security event that involves a security violation. (See: CERT, security event, security intrusion, security violation.) [RFC4949:2007]

2.584.1 (EN) INFORMATION SECURITY INCIDENT

A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. [ISO-18028-1:2006] [ISO-18044:2004]

2.584.2 (EN) INFORMATION SECURITY INCIDENT

An Information Security incident is an event which appears to be a breach of the organizations Information Security safeguards. It is important to respond calmly and to follow a logical procedure, first to prevent the breach from continuing, if possible, and second, to inform the appropriate person(s) within the organization; this usually includes the appointed Security Officer.

http://www.passwordnow.com/en/glossary/information-security-incident.html

2.584.1 (EN) IT SECURITY INCIDENT (INCIDENT)

is any activity that harms or represents a serious threat to the whole or part of Yale's computer, telephone and network-based resources such that there is an absence of service, inhibition of functioning systems, including unauthorized changes to hardware, firmware, software or data, unauthorized exposure, change or deletion of PHI, or a crime or natural disaster that destroys access to or control of these resources. Routine detection and remediation of a virus', malware' or similar issue that has little impact on the day-to-day business of the University is not considered an Incident under this policy.

http://www.hipaa.yale.edu/overview/glossary.html

2.584.1 (EN) SECURITY INCIDENT

Any workplace violence toward an employee or any act, event or omission that could result in the compromise of information, assets or services.

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

2.584.1 (FR) INCIDENT LIE A LA SECURITE DE L'INFORMATION

un incident lié à la sécurité de l'information est indiqué par un ou plusieurs événement(s) de sécurité de l'information indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information. [ISO-18044:2004]

2.584.2 (FR) INCIDENT DE SÉCURITÉ

Tout acte de violence en milieu de travail manifestée à l'endroit d'un employé ou tout acte, événement ou omission pouvant entraîner la compromission d'informations, de biens ou de services.

http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578

2.585 INDICADOR

Ver:

- *Medida*
- *Métrica*

2.585.1 INDICAR

Mostrar o significar [algo] con indicios y señales.

DRAE. Diccionario de la Lengua Española.

2.585.2 INDICADOR

Medida que proporciona una estimación o una evaluación de determinados atributos usando un modelo analítico para satisfacer unas determinadas necesidades de informaciön [UNE-ISO/IEC 27000:2014]

2.585.3 INDICADOR

(1) Instrumento que se utiliza para controlar la operación o estado de un motor, un horno, una red eléctrica, un depósito o un sistema físico.

(2) Química. Compuesto químico que cambia de color y estructura cuando se expone a ciertas condiciones y, por tanto, es útil para las pruebas químicas.

(3) Ecología. Vegetal o animal cuya existencia en un área es un fuerte indicativo de ciertas condiciones ambientales.

(4) Cualquiera de los diversos valores estadísticos que, en conjunto, proporcionan una indicación de la situación de la economía o hacia dónde se dirige.

2.585.4 INDICADOR

Resultado o dato, producto de un estudio o investigación, que trata de cuantificar y/o calificar, en definitiva de sintetizar, una variable o dimensión de la realidad.

http://www.n-economia.com/glosario/glosario.asp

2.585.5 (EN) INDICATOR

measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to defined information needs [ISO/IEC 27000:2014]

2.585.6 (EN) INDICATOR

(1) An instrument used to monitor the operation or condition of an engine, furnace, electrical network, reservoir, or other physical system; a meter or gauge.

(2) Chemistry. A chemical compound that changes color and structure when exposed to certain conditions and is therefore useful for chemical tests.

(3) Ecology: A plant or animal whose existence in an area is strongly indicative of specific environmental conditions.

(4) Any of various statistical values that together provide an indication of the condition or direction of the economy.

2.585.7 (EN) INDICATOR

Observed value representative of a phenomenon to study. In general, indicators quantify information by aggregating different and multiple data. The resulting information is therefore synthesised. In short, indicators simplify information that can help to reveal complex phenomena.

http://glossary.eea.europa.eu/EEAGlossary/

2.585.8 (EN) INFORMATION SECURITY INDICATOR

outcome of applying an analytical model to one or more measures in relation to decision criteria or an information need.

2.586 INDICADOR CLAVE DE RIESGO

Acrónimo: KRI

2.586.1 INDICADOR DE RIESGOS CLAVE

Un indicador de riesgos clave (KRI) es una métrica para determinar qué tan posible es que la probabilidad de un evento, combinada con sus consecuencias, supere el apetito de riesgo de la organización (es decir, el nivel de riesgo que la compañía está preparada para aceptar), y tenga un impacto profundamente negativo en la capacidad de tener éxito de una organización. Si una organización se especializa en ventas al por menor, por ejemplo, un indicador de riesgo clave podría ser el número de quejas de los clientes, porque el aumento de este KRI podría ser una indicación temprana de que hay que resolver un problema operativo.

El desafío para una organización no es solo identificar cuáles indicadores de riesgo deben ser identificados como claves (los más importantes), sino también comunicar esa información de tal manera que todo el mundo en la organización entienda claramente su significado. Identificar indicadores de riesgos clave requiere la comprensión de las metas de la organización.

Cada KRI debería ser capaz de ser medido con precisión y reflejar de manera precisa el impacto negativo que tendría sobre los indicadores de desempeño clave de la organización (KPI). Los indicadores de rendimiento clave, que a menudo se confunden con los indicadores de riesgos clave, son las métricas que ayudan a una organización a evaluar el progreso hacia los objetivos declarados.

http://searchdatacenter.techtarget.com/es/

2.586.2 (EN) KEY RISK INDICATOR (KRI)

A subset of risk indicators that are highly relevant and possess a high probability of predicting or indicating important risk

ISACA, Cybersecurity Glossary, 2014

2.586.3 (EN) KEY RISK INDICATORS

An enterprise may develop an extensive set of metrics to serve as risk indicators; however, it is not possible or feasible to maintain that full set of metrics as key risk indicators (KRIs). KRIs are differentiated as being highly relevant and possessing a high probability of predicting or indicating important risk.

The Risk IT Practitioner Guide. November 2009.

2.586.4 (EN) KEY RISK INDICATOR (KRI)

A key risk indicator (KRI) is a metric for measuring the likelihood that the combined probability of an event and its consequence will exceed the organization's risk appetite and have a profoundly negative impact on an organization's ability to be successful.

If an organization specializes in retail sales, for example, a key risk indicator might be the number of customer complaints because increase in this KRI could be an early indication that an operational problem needs to be addressed. The challenge for an organization is not only to identify which risk indicators should be identified as being key (most important) but also to communicate that information in such a way that everyone in the organization clearly understands its significance.

Identifying key risk indicators requires an understanding of the organization's goals. Each KRI should be able to be measured and accurately reflect the negative impact it would have on the organization's key performance indicators (KPIs). Key performance indicators, which are often confused with key risk indicators, are metrics that help an organization assess progress towards declared goals.

http://searchcio.techtarget.com/

2.586.5 KEY RISK INDICATOR

A Key Risk Indicator, also known as a KRI, is a measure used in management to indicate how risky an activity is. It differs from a Key Performance Indicator (KPI) in that the latter is meant as a measure of how well something is being done while the former is an indicator of the possibility of future adverse impact. KRI give us an early warning to identify potential event that may harm continuity of the activity/project.

http://en.wikipedia.org/wiki/Key_Risk_Indicator

2.587 INDICADOR DE COMPROMISO

2.587.1 INDICADOR DE COMPROMISO

En análisis forense, es un descriptor observado en una red o en un sistema operativo que con alta probabilidad indica una intrusión informática.

IOC típicos son las firmas de virus y las direcciones IP, los hashes MD5 de archivos o URLs de malware o nombres de dominio de servidores de comando y control de botnets. Una vez los IOC han sido identificados en un proceso de respuesta a incidentes y análisis forense, pueden ser utilizados en el futuro para la detección temprana de intentos de ataque que utilizan sistemas de detección de intrusos y antivirus.

2.587.2 (EN) IOC - INDICATOR OF COMPROMISE

Indicator of compromise (IOC) — in computer forensics is an artifact observed on a network or in an operating system that with high confidence indicates a computer intrusion.

Typical IOCs are virus signatures and IP addresses, MD5 hashes of malware files or URLs or domain names of botnet command and control servers. After IOCs have been identified in a process of incident response and computer forensics, they can be used for early detection of future attack attempts using intrusion detection systems and antivirus software.

https://en.wikipedia.org/wiki/Indicator_of_compromise

2.588 INDUSTRIA DE TARJETAS DE PAGO - NORMA DE SEGURIDAD DE DATOS

Acrónimos: PCI-DSS

2.589 INFALSIFICABLE

2.589.1 INFALSIFICABLE

Propiedad de una función criptográfica que indica que es [computacionalmente] imposible llegar al resultado correcto sin conocer las claves necesarias; es decir, que no se puede generar el resultado de forma fraudulenta.

Es una propiedad útil cuando se requiere autenticidad del origen de una cierta información.

2.589.2 (EN) UNFORGEABLE

(I) /cryptography/ The property of a cryptographic data structure (i.e., a data structure that is defined using one or more cryptographic functions, e.g., "digital certificate") that makes it computationally infeasible to construct (i.e., compute) an unauthorized but correct value of the structure without having knowledge of one of more keys. [RFC4949:2007]

2.590 INFORMACIÓN

Ver:

- *Datos*
- *Manejar información*
- *Responsable de la información*

2.590.1 INFORMACIÓN

Todo conocimiento que puede ser comunicado, presentado o almacenado en cualquier forma. [CCN-STIC-431:2006]

2.590.2 INFORMACIÓN

Elemento de conocimiento susceptible de representarse con ayuda de convenios para conservarse, tratarse o comunicarse. [CCN-STIC-207:2006]

2.590.3 INFORMACIÓN

Dato o elemento de conocimiento susceptible de ser representado bajo una forma adaptada a una comunicación, un registro o un tratamiento. [IGI 900] [REC 901] [EBIOS:2005]

2.590.4 INFORMACIÓN

datos que poseen significado [ISO-9000_es:2000]

2.590.5 (EN) INFORMATION

Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. [CNSSI_4009:2010]

2.590.6 (EN) INFORMATION

1. (I) Facts and ideas, which can be represented (encoded) as various forms of data.

2. (I) Knowledge -- e.g., data, instructions -- in any medium or form that can be communicated between system entities.

[RFC4949:2007]

2.590.7 (EN) INFORMATION

Knowledge that can be communicated in any form. [CCN-STIC-401:2007]

2.590.8 (EN) INFORMATION.

Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics. [DoD 5220:2006]

2.590.9 (EN) INFORMATION

An instance of an information type. [FIPS-199:2004]

2.590.10 (EN) INFORMATION TYPE

A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation. [CNSSI_4009:2010]

2.590.11 (EN) INFORMATION TYPE

A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation. [FIPS-199:2004]

2.590.12 (EN) INFORMATION

Information or item of knowledge that can be represented in a form allowing its communication, recording or processing. [IGI 900] [REC 901] [EBIOS:2005]

2.590.13 (EN) DATA / INFORMATION

In the area of Information Security, data (and the individual elements that comprise the data) is processed, formatted and re-presented, so that it gains meaning and thereby becomes information. Information Security is concerned with the protection and safeguard of that information which, in its various forms can be identified as Business Assets or Information Assets.

http://www.passwordnow.com/en/glossary/data--information.html

2.591 INFORMACIÓN CLASIFICADA

Ver:

- *Información sensible*
- *Esquema de clasificación*
- *Nivel de clasificación*
- *Etiqueta de clasificación*
- *Clasificar*
- *Desclasificar*
- *Agregación*
- *Clasificación*
- *Desclasificación*
- *Modo de operación (2)*

2.591.1 INFORMACIÓN CLASIFICADA

Aquella con una clasificación de confidencial, reservado o secreto.

2.591.2 INFORMACIÓN CLASIFICADA

En España, según la Ley 9/68 modificada por la 48/78, sobre Secretos Oficiales, es aquella: "cuyo conocimiento por personas no autorizadas, pueda dañar o poner en riesgo la seguridad y defensa del Estado".

Según la misma Ley, la clasificación comprende las categorías de secreto y reservado, siendo facultad exclusiva del Consejo de Ministros y de la Junta de Jefes de Estado Mayor la asignación de dicha clasificación.

[Ribagorda:1997]

2.591.3 INFORMACIÓN SENSIBLE O CLASIFICADA

Información que, dentro de un ámbito, se ha determinado que debe ser protegida, pues su destrucción, alteración o conocimiento por personal no autorizado puede causar perjuicios.

Dentro del ámbito del Estado este concepto se denomina materia clasificada, existiendo varios grados de clasificación.

[CESID:1997]

2.591.1 (EN) CLASSIFIED INFORMATION

See classified national security information. [CNSSI_4009:2010]

2.591.2 (EN) CLASSIFIED NATIONAL SECURITY INFORMATION

Information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. [CNSSI_4009:2010]

2.591.3 (EN) CLASSIFIED

1. (I) Refers to information (stored or conveyed, in any form) that is formally required by a security policy to receive data confidentiality service and to be marked with a security label (which, in some cases, might be implicit) to indicate its protected status. (See: classify, collateral information, SAP, security level. Compare: unclassified.) [RFC4949:2007]

2.591.4 (EN) CLASSIFIED INFORMATION

Any information (namely, knowledge that can be communicated in any form) or material determined to require protection against unauthorised disclosure and which has been so designated by a security classification. [CCN-STIC-401:2007]

2.591.5 (EN) CLASSIFIED INFORMATION.

Official information that has been determined, pursuant to reference (b) or any predecessor order, to require protection against unauthorized disclosure in the interest of national security and which has been so designated. [DoD 5220:2006]

2.591.6 (EN) CLASSIFICATION GUIDE.

A document issued by an authorized original classifier that identifies the elements of information regarding a specific subject that must be classified and prescribes the level and duration of classification and appropriate declassification instructions. (Classification guides are provided to contractors by the Contract Security Classification Specification.) [DoD 5220:2006]

2.592 INFORMACIÓN DE AUTENTICACIÓN

Ver:

- *Autenticación*

2.592.1 INFORMACIÓN DE AUTENTICACIÓN

Información empleada para verificar la pretendida identidad de un usuario.

2.592.2 INFORMACIÓN DE AUTENTICACIÓN

Información utilizada para establecer la validez de una identidad alegada. [ISO-7498-2:1989]

2.592.3 (EN) AUTHENTICATION INFORMATION

(I) Information used to verify an identity claimed by or for an entity. (See: authentication, credential, user. Compare: identification information.)

Tutorial: Authentication information may exist as, or be derived from, one of the following: (a) Something the entity knows (see: password); (b) something the entity possesses (see: token); (c) something the entity is (see: biometric authentication).

[RFC4949:2007]

2.592.4 (EN) AUTHENTICATION DATA

information used to verify the claimed identity of a user. [CC:2006]

2.592.5 (EN) AUTHENTICATION INFORMATION

Information used to establish the validity of a claimed identity. [ISO-7498-2:1989]

2.592.6 (FR) INFORMATION D'AUTHENTIFICATION

Information utilisée pour établir la validité d'une identité déclarée. [ISO-7498-2:1989]

2.593 INFORMACIÓN SENSIBLE

Ver:

- *Información*
- *Información clasificada*
- *Sensibilidad*

2.593.1 INFORMACIÓN SENSIBLE

Aquella, así definida por su propietario, que debe ser especialmente protegida, pues si revelación, alteración, pérdida o destrucción puede producir daños importantes a alguien o algo.

Caso de que este tipo de información sea sensible para un Estado, se suele denominar información clasificada.

[Ribagorda:1997]

2.593.2 (EN) SENSITIVE INFORMATION

Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals

are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (Systems that are not national security systems, but contain sensitive information, are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L.100-235).). See also controlled unclassified information. [CNSSI_4009:2010]

2.593.3 (EN) SENSITIVE INFORMATION

1. (I) Information for which (a) disclosure, (b) alteration, or (c) destruction or loss could adversely affect the interests or business of its owner or user. (See: data confidentiality, data integrity, sensitive. Compare: classified, critical.)

2. (O) /U.S. Government/ Information for which (a) loss, (b) misuse, (c) unauthorized access, or (d) unauthorized modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act of 1974, but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

[RFC4949:2007]

2.593.4 (EN) SENSITIVE INFORMATION

Information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something. [TCSEC:1985]

2.594 INFORMAL

Ver:

- *Semiformal*
- *Formal*
- *Criterios comunes*

2.594.1 INFORMAL

en lenguaje natural.

2.594.2 (EN) INFORMAL

expressed in natural language. [CC:2006]

2.595 INFORMATIVO

Ver:

- *Obligatorio*

2.595.1 ANEXOS INFORMATIVOS

Los anexos informativos no tienen carácter normativo.

Proporcionan una información adicional o suplementaria.

Deben situarse inmediatamente después de los elementos normativos de la norma.

No deben contener especificaciones.

Guía para la Redacción de Documentos Normativos UNE, AENOR, 2006.

2.595.2 (EN) INFORMATIVE

informative text provides additional information intended to assist the understanding or use of the document. (ISO/IEC). [CC:2006]

2.596 INFRAESTRUCTURA DE CLAVE PÚBLICA

Acrónimos: PKI

Ver:

- *Certificado de clave pública*
- http://www.ietf.org/rfc/rfc3280

2.596.1 INFRAESTRUCTURA DE CLAVES PÚBLICAS

Infraestructura capaz de soportar la gestión de claves públicas para los servicios de autenticación, criptación, integridad, o no repudio. [X.509:2005]

2.596.1 (EN) PUBLIC KEY INFRASTRUCTURE (PKI)

The framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates. [CNSSI_4009:2010]

2.596.2 (EN) PUBLIC-KEY INFRASTRUCTURE (PKI)

1. (I) A system of CAs (and, optionally, RAs and other supporting servers and agents) that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography. (See: hierarchical PKI, mesh PKI, security management infrastructure, trust-file PKI.)

2. (I) /PKIX/ The set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography.

[RFC4949:2007]

2.596.3 (EN) PUBLIC KEY INFRASTRUCTURE (PKI)

A framework that is established to issue, maintain and revoke public key certificates. [NIST-SP800-57:2007]

2.596.4 (EN) PUBLIC KEY INFRASTRUCTURE (PKI)

The infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services. [X.509:2005]

2.596.5 (EN) PUBLIC KEY INFRASTRUCTURE

The infrastructure needed to generate, distribute, manage and archive keys, certificates and certificate revocation lists and the repository to which certificates and certificate-revocation lists are to be posted. [ISO-11770-3:2008]

2.596.6 (EN) PUBLIC KEY INFRASTRUCTURE

Generally, the laws, policies, standards, and software that regulate or manipulate certificates and public and private keys.

http://www.getsafeonline.org/

2.596.7 (FR) INFRASTRUCTURE DE CLÉ PUBLIQUE

infrastructure pouvant prendre en charge la gestion de clés publiques afin de fournir des services d'authentification, de chiffrement, d'intégrité et de non répudiation. [X.509:2005]

2.596.8 (FR) INFRASTRUCTURE DE GESTION DE CLES

Une infrastructure de gestion de clés offre un environnement de confiance, ainsi qu'un ensemble de garanties et services relatifs aux certificats de clés publiques (SCSSI, PC2 v2.0).

Une infrastructure de gestion de clés est composée des éléments suivants:

- Autorité de certification.
- Autorité d'enregistrement.
- Système de publication/distribution des certificats (ex. annuaire).
- Autorité d'horodatage.
- Applications compatibles.

Une infrastructure de gestion de clés utilise les objets suivants:

- Bi-clés.
- Certificats.

http://securit.free.fr/glossaire.htm

2.597 INFRAESTRUCTURAS CRÍTICAS

Acrónimos: CIP

Ver:

- *Infraestructuras críticas de información (protección de)*

2.597.1 INFRAESTRUCTURAS CRÍTICAS

Infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. [Ley 8/2011]

2.597.2 INFRAESTRUCTURAS ESTRATÉGICAS

Instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales. [Ley 8/2011]

2.597.3 SERVICIO ESENCIAL

Servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas. [Ley 8/2011]

2.597.4 INFRAESTRUCTURAS CRÍTICAS

Las infraestructuras críticas son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros.

http://europa.eu/scadplus/leg/es/lvb/l33259.htm

2.597.5 (EN) CRITICAL INFRASTRUCTURE

Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.

Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, February 12, 2014

2.597.6 (EN) CRITICAL INFRASTRUCTURE:

Any infrastructure whose disruption could have severe impact on a nation or society. In the United States. Critical Infrastructures are defined by the Homeland Security Presidential Directive Seven as: Agriculture and Food; Banking and Finance: Chemical: Commercial Facilities: Critical Manufacturing: Dams: Defense Industrial Base: Drinking Water and Water Treatment Systems: Emergency Services: Energy: Government Facilities: Information Technology; National Monuments and Icons; Nuclear Reactors. Materials. and Waste; Postal and Shipping: Public Health and Healthcare: Telecommunications: and Transportation Systems. [knapp:2014]

2.597.7 (EN) CRITICAL INFRASTRUCTURE:

Physical or virtual systems and assets under the jurisdiction of a State that are so vital that their incapacitation or destruction may debilitate a State’s security, economy, public health or safety, or the environment

The Tallinn Manual, 2013

2.597.8 (EN) CRITICAL NATIONAL INFRASTRUCTURE

A term used by governments to describe assets that are essential for the functioning of a society and economy (e.g. electricity generation, gas production, telecommunications, water supply etc.). [CSS NZ:2011]

2.597.9 (EN) CRITICAL INFRASTRUCTURES

Critical infrastructures are organizations or institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, considerable disturbance of public security or other dramatic consequences. [CSS DE:2011]

2.597.10 (EN) CRITICAL INFRASTRUCTURE

Systems whose incapacity or destruction would have a debilitating effect on the economic security of an enterprise, community or nation.

ISACA, Cybersecurity Glossary, 2014

2.597.11 (EN) CRITICAL INFRASTRUCTURE

System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. [CNSSI_4009:2010]

2.597.12 (EN) CRITICAL INFRASTRUCTURES

Critical infrastructures can be defined as systems and assets, whether physical or virtual, so vital to a country that their improper functioning, incapacity or destruction would have a debilitating impact on national security and defence, economic security, public health or safety, or any combination of those matters. Countries define critical infrastructures differently. However, many countries consider critical infrastructures to include the energy, food, water, fuel, transport, communications, finance, industry, defence and governmental and public services sectors.

Cybercrime Convention Committee (T-CY)

2.598 INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN (PROTECCIÓN DE)

Acrónimos: CIIP

Ver:

- *CIP - Critical Infrastructure Protection*

2.598.1 (EN) CRITICAL INFORMATION INFRASTRUCTURE

(I) Those systems that are so vital to a nation that their incapacity or destruction would have a debilitating effect on national security, the economy, or public health and safety. [RFC4949:2007]

2.598.2 (EN) CIIP - CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

this is primarily a European approach to critical infrastructure protection, with an emphasis on cyber-related systems.

2.599 INGENIERÍA DE LA SEGURIDAD

2.599.1 INGENIERÍA DE LA SEGURIDAD

Conjunto multidisciplinar de técnicas y medios para construir sistemas seguros. Se centra en definir las necesidades de los usuarios, los requisitos de seguridad y la funcionalidad requerida desde los primeros pasos del proceso de desarrollo. Cubre desde el diseño hasta la validación del sistema final.

2.599.2 (EN) SECURITY ENGINEERING

An interdisciplinary approach and means to enable the realization of secure systems. It focuses on defining customer needs, security protection requirements, and required functionality early in the systems development lifecycle, documenting requirements, and then proceeding with design, synthesis, and system validation while considering the complete problem. [CNSSI_4009:2010]

2.600 INGENIERÍA INVERSA

2.600.1 INGENIERÍA INVERSA

El arte de acceder a información sensible a base de desensamblar y analizar el diseño de un sistema o componente.

2.600.2 (EN) REVERSE ENGINEERING

Acquiring sensitive data by disassembling and analyzing the design of a system component.

http://www.sans.org/security-resources/glossary-of-terms/

2.601 INGENIERÍA SOCIAL (PICARESCA)

Ver:

- http://en.wikipedia.org/wiki/Social_engineering_%28computer_security%29

2.601.1 INGENIERÍA SOCIAL

Mecanismo para obtener información o datos de naturaleza sensible.

Las técnicas de ingeniería social son tácticas de persuasión que suelen valerse de la buena voluntad y falta de precaución de los usuarios, y cuya finalidad consiste en obtener cualquier clase de información, en muchas ocasiones claves o códigos.

http://www.inteco.es/glossary/Formacion/Glosario/

2.601.2 INGENIERÍA SOCIAL

Son técnicas basadas en engaños que se emplean para dirigir la conducta de una persona u obtener información sensible. El afectado es inducido a actuar de determinada forma (pulsar en enlaces, introducir contraseñas, visitar páginas, etc.) convencido de que está haciendo lo correcto cuando realmente está siendo engañado por el ingeniero social.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.601.3 PICARESCA

Forma de vida o actuación aprovechada y tramposa.

DRAE. Diccionario de la Lengua Española.

2.601.4 INGENIERÍA SOCIAL

Eufemismo empleado para referirse a medios no técnicos o de baja complejidad tecnológica utilizados para atacar a sistemas de información, tales como mentiras, suplantaciones, engaños, sobornos y chantajes. [CCN-STIC-403:2006]

2.601.5 (EN) SOCIAL ENGINEERING

The act of deceiving an individual into revealing sensitive information by associating with the individual to gain confidence and trust. [NIST-SP800-63:2013]

2.601.6 (EN) SOCIAL ENGINEERING

The practice of obtaining otherwise secure information by tricking, exploiting human traits of trust and helpfulness, or manipulation of legitimate users. [CSS NZ:2011]

2.601.7 (EN) SOCIAL ENGINEERING

An attempt to trick someone into revealing information (e.g., a password) that can be used to attack an enterprise. [CNSSI_4009:2010]

2.601.8 (EN) SOCIAL ENGINEERING

(D) Euphemism for non-technical or low-technology methods, often involving trickery or fraud, that are used to attack information systems. Example: phishing. [RFC4949:2007]

2.601.9 (EN) SOCIAL ENGINEERING

An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. [NIST-SP800-61:2004]

2.601.10 (EN) SOCIAL ENGINEERING

A euphemism for non-technical or low-technology means - such as lies, impersonation, tricks, bribes, blackmail, and threats - used to attack information systems.

http://www.sans.org/security-resources/glossary-of-terms/

2.601.11 (EN) SOCIAL ENGINEERING

Social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures.

A social engineer runs what used to be called a "con game." For example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network's security. Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appeal to vanity, appeal to authority, appeal to greed, and old-fashioned eaves-dropping are other typical social engineering techniques.

http://searchsecurity.techtarget.com/

2.601.12 (EN) SOCIAL ENGINEERING

Potential attackers may persuade an authorised user to give them their password (e.g. by pretending to be involved in systems maintenance, by bribing).

2.601.13 (EN) SOCIAL ENGINEERING ATTACK

An attack that does not depend on technology as much as it depends upon tricking or persuading an individual to divulge privileged information to the attacker, usually unknowingly. For example, an attacker might phone a company's internal help desk, posing as an employee, and say, "This is Fred in Accounting. I was on vacation for five weeks and forgot my network password. Could you look it up for me?" If the gullible help desk technician reveals the password to the attacker, the attacker "socially engineered" it out of him.

http://www.watchguard.com/glossary/

2.601.14 (EN) SOCIAL ENGINEERING

Tricks performed by malicious users offline to gain access to secure systems, for example impersonating a technical support agent.

http://www.getsafeonline.org/

2.601.15 (FR) INGÉNIERIE SOCIALE

Technique de piratage consistant à profiter de la crédulité d'un utilisateur afin de lui sous-tirer des informations confidentielles attenantes à un système d'information cible. Le but principal est pour le pirate de pouvoir obtenir des informations lui permettant d'obtenir un accès valide sur le système d'information qu'il souhaite pénétrer. Le pirate informatique profite ainsi du maillon le plus faible de la chaîne pour pénétrer sur un système d'information.

http://www.cases.public.lu/functions/glossaire/

2.602 INSERCIÓN DE FICHEROS REMOTOS

Acrónimos: RFI

2.602.1 INSERCIÓN DE FICHEROS REMOTOS

Abuso de servidores de aplicaciones web a los que se les fuerza para que entreguen software dañino.

2.602.2 (EN) REMOTE FILE INCLUSION (RFI)

Remote File Inclusion (RFI) is an attack that targets the computer servers that run Web sites and their applications. RFI exploits are most often attributed to the PHP programming language used by many large firms including Facebook and SugarCRM. However, RFI can manifest itself in other environments and was in fact introduced initially as "SHTML injection". RFI works by exploiting applications that dynamically reference external scripts indicated by user input without proper sanitation. As a consequence, the application can be instructed to include a script hosted on a remote server and thus execute code controlled by an attacker. The executed scripts can be used for temporary data theft or manipulation, or for a long term takeover of the vulnerable server.

http://www.imperva.com/resources/glossary/glossary.html

2.603 INSPECCIÓN DE SEGURIDAD

2.603.1 INSPECCIÓN DE SEGURIDAD

Examen exhaustivo de un sistema de información para determinar si cumple lo requerido en materia de seguridad: política, procedimientos y operaciones.

2.603.2 (EN) SECURITY INSPECTION

Examination of an information system to determine compliance with security policy, procedures, and practices. [CNSSI_4009:2010]

2.604 INSTALACIONES

2.604.1 INSTALACIONES

Sistema, servicio o infraestructura útil para procesar información, o el lugar donde residen físicamente.

2.604.2 INSTALACIONES DE TRATAMIENTO DE INFORMACIÓN

cualquier sistema de tratamiento de la información, servicios o infraestructura, o los lugares físicos que los albergan [UNE-ISO/IEC 27000:2014]

2.604.3 (EN) INFORMATION PROCESSING FACILITIES

any information processing system, service or infrastructure, or the physical locations housing them [ISO/IEC 27000:2014]

2.604.4 (EN) FACILITY

A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.) [NERC:2014]

2.604.5 (EN) FACILITY

An installation, plant, factory, laboratory, office, university or other educational Institution, or commercial undertaking, including any associated warehouses, storage areas, utilities and components which, when related by function and location, form an operating entity. [CCN-STIC-401:2007]

2.605 INTEGRIDAD

Ver:

- *Integridad de los datos*
- *Integridad del sistema*

2.605.1 INTEGRIDAD

Propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada. [UNE-71504:2008]

2.605.2 INTEGRIDAD

(Diseño del Servicio) Un principio de seguridad que certifica que los datos y Elementos de Configuración sólo son modificados por personal y Actividades autorizados. La Integridad considera todas las posibles causas de modificación, incluyendo Fallos software y hardware, Eventos medioambientales e intervención humana. [ITIL:2007]

2.605.3 INTEGRIDAD

propiedad exactitud y completitud. [UNE-ISO/IEC 2700:2014]

2.605.4 INTEGRIDAD

Propiedad de los elementos esenciales de ser exactos y completos. [EBIOS:2005]

2.605.5 (EN) INTEGRITY

property accuracy and completeness [ISO/IEC 27000:2014]

2.605.1 (EN) INTEGRITY

Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information. [NIST-SP800-53:2013]

2.605.2 (EN) INTEGRITY

The property whereby an entity has not been modified in an unauthorized manner.

NIST 800-53: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

[CNSSI_4009:2010]

2.605.3 (EN) INTEGRITY

guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity

U.S. Code 44, Sec. 3542. Definitions, 2007

2.605.4 (EN) INTEGRITY

(Service Design) A security principle that ensures data and Configuration Items are only modified by authorised personnel and Activities. Integrity considers all possible causes of modification, including software and hardware Failure, environmental Events, and human intervention. [ITIL:2007]

2.605.5 (EN) INTEGRITY

Property defining the accuracy and completeness of the essential elements. [EBIOS:2005]

2.605.6 (EN) INTEGRITY

The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation). [NIST-SP800-27:2004]

2.605.7 (EN) INTEGRITY

the authenticity, accuracy, and completeness of an asset. [Octave:2003]

2.605.8 (EN) INTEGRITY

The security objective that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation). [NIST-SP800-33:2001]

2.605.9 (EN) INTEGRITY

Condition existing when an information system operates without unauthorized modification, alteration, impairment, or destruction of any of its components. [CIAO:2000]

2.605.10 (FR) INTÉGRITÉ

(Conception de services) Principe de sécurité qui assure que les données et les éléments de configuration ne sont modifiés que par un personnel et des activités autorisés. L'intégrité considère toutes les causes possibles de modification, y compris la défaillance logicielle et matérielle, les événements touchant à l'environnement et l'intervention humaine. [ITIL:2007]

2.605.11 (FR) INTÉGRITÉ

Propriété d'exactitude et de complétude des éléments essentiels. [EBIOS:2005]

2.606 INTEGRIDAD DE LOS DATOS

Ver:

- *Datos*
- *Integridad*

2.606.1 INTEGRIDAD

Cualidad o condición de la información que garantiza que no ha sido modificada por personas no autorizadas.

2.606.2 INTEGRIDAD

1. Prevención de la modificación no autorizada de información (ITSEC)

2. Propiedad de los datos e informaciones que son exactas y completas manteniendo además estas características. (OCDE).

Según la norma ISO/IEC ISO-7498-2, la integridad es un servicio de seguridad que se define en relación a los datos.

El mantenimiento de la integridad, junto con el de la confidencialidad y disponibilidad, constituye el objetivo de la seguridad de la información.

[Ribagorda:1997]

2.606.3 INTEGRIDAD

Servicio de seguridad que garantiza que la información no ha sido mutilada o alterada de manera no autorizada.

Como mecanismo de seguridad, incluye los procedimientos que garantizan la integridad de un campo de la información, o de todos ellos, contra desórdenes, repeticiones, inserciones, pérdidas o alteraciones, para lo que se utilizan secuencias numéricas, cadenas criptográficas o referencias horarias.

[CESID:1997]

2.606.4 (EN) INTEGRITY

The term `integrity' means guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.

Cyber Intelligence Sharing and Protection Act. H.R. 624. 2013.

2.606.1 (EN) DATA INTEGRITY

The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. [CNSSI_4009:2010]

2.606.2 (EN) DATA INTEGRITY

1. (I) The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. (See: data integrity service. Compare: correctness integrity, source integrity.)

2. (O) "The property that information has not been modified or destroyed in an unauthorized manner." [ISO-7498-2]

[RFC4949:2007]

2.606.3 (EN) DATA INTEGRITY

A property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored. [NIST-SP800-57:2007]

2.606.4 (EN) DATA INTEGRITY

The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner. [NIST-SP800-57:2007]

2.606.5 (EN) INTEGRITY

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [FIPS-200:2006] [FIPS-199:2004] [NIST-SP800-53:2013] [NIST-SP800-60V2:2004]

2.606.6 (EN) DATA INTEGRITY

The property that data has not been altered or destroyed in an unauthorized manner. [ISO-18028-2:2006]

2.606.7 (EN) DATA INTEGRITY

The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. [NIST-SP800-27:2004]

2.606.8 (EN) DATA INTEGRITY

A condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. [TDIR:2003]

2.606.9 (EN) DATA INTEGRITY

The Data Integrity Security Dimension ensures the correctness or accuracy of data. The data is protected against unauthorized modification, deletion, creation, and replication and provides an indication of these unauthorized activities. [X.805:2003]

2.606.10 (EN) DATA INTEGRITY

The data quality that exists as long as accidental or malicious destruction, alteration, or loss of data does not occur. [CRAMM:2003]

2.606.11 (EN) DATA INTEGRITY

The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. [NIST-SP800-33:2001]

2.606.12 (EN) DATA INTEGRITY

the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner. [FIPS-140-2:2001]

2.606.13 (EN) DATA INTEGRITY

A condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. [CIAO:2000]

2.606.14 (EN) DATA INTEGRITY

the prevention of the unauthorised modification of information. [ITSEC:1991]

2.606.15 (EN) DATA INTEGRITY

The property that data has not been altered or destroyed in an unauthorized manner. [ISO-7498-2:1989]

2.606.16 (EN) DATA INTEGRITY

The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction. [TCSEC:1985]

2.606.17 (EN) INFORMATION INTEGRITY

The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

http://www.ioss.gov/docs/definitions.html

2.606.18 (EN) INTEGRITY

Integrity is the need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.

http://www.sans.org/security-resources/glossary-of-terms/

2.606.19 (EN) FILE INTEGRITY CHECKER

Software that generates, stores, and compares message digests for files to detect changes to the files. [NIST-SP800-61:2004]

2.606.20 (FR) INTEGRIDAD DE LOS DATOS

Propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada. [ISO-7498-2:1989]

2.606.21 (FR) INTÉGRITÉ DE DONNÉES

Qualité de données qui n'ont pas été altérées ou détruites de manière frauduleuse. [ISO-7498-2:1989]

2.607 INTEGRIDAD DEL SISTEMA

2.607.1 INTEGRIDAD DEL SISTEMA

Dícese de un sistema cuando está perfectamente dispuesto para llevar a cabo la misión que tiene encomendada, libre de manipulaciones no autorizadas, accidentales o deliberadas.

2.607.1 (EN) INTEGRITY

The property whereby an entity has not been modified in an unauthorized manner.

NIST 800-53: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

[CNSSI_4009:2010]

2.607.2 (EN) SYSTEM INTEGRITY

Attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. [CNSSI_4009:2010]

2.607.3 (EN) SYSTEM INTEGRITY

1. (I) An attribute or quality "that a system has when it can perform its intended function in a unimpaired manner, free from deliberate or inadvertent unauthorized manipulation." [C4009, NCS04] (See: recovery, system integrity service.) [RFC4949:2007]

2.607.4 (EN) OPERATIONAL INTEGRITY

(I) Synonym for "system integrity"; this synonym emphasizes the actual performance of system functions rather than just the ability to perform them. [RFC4949:2007]

2.607.5 (EN) SYSTEM INTEGRITY

The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental. [NIST-SP800-33:2001]

2.608 INTELIGENCIA

Ver:

- *Datos*
- *Información*
- *Agregación de datos*

2.608.1 INTELIGENCIA

El producto resultante de la recolección, evaluación, análisis, integración e interpretación de toda la información disponible, y que es inmediatamente o potencialmente significativa para la planificación y las operaciones.

2.608.2 INTELIGENCIA EMPRESARIAL

La Inteligencia Empresarial (IE) se refiere a los sistemas y aplicaciones que se utilizan en forma colectiva para consolidar, almacenar y analizar datos corporativos por motivos de informes y toma de decisiones. La IE ayuda a que los negocios comprendan la salud actual de la organización, así como que sean capaces de analizar el pasado para hacer mejores decisiones.

http://www.extendb.com/esp/glossary.php

2.608.3 (EN) INTELLIGENCE.

The product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information, that concerns one or more aspects of foreign nations or of areas of foreign operations, and that is immediately or potentially significant to military planning and operations [DoD 5220:2006]

2.608.4 (EN) INTELLIGENCE

Intelligence

- the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; or
- information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. The term 'intelligence' includes foreign intelligence and counterintelligence.

[NIST-SP800-60V2:2004]

2.608.5 (EN) INTELLIGENCE

is information valued for its currency and relevance rather than its detail or accuracy in contrast with "data" which typically refers to precise or particular information, or "fact," which typically

refers to verified information. Sometimes called "active data" or "active intelligence", these typically regard the current plans, decisions, and actions of people, as these may have urgency or may otherwise be considered "valuable" from the point of view of the intelligence-gathering organization. Active intelligence is treated as a constantly mutable component, or variable, within a larger equasion of understanding the secret, covert, or otherwise private "intelligence" of an opponent, or competitor, to answer questions or obtain advance warning of events and movements deemed to be important or otherwise relevant.

As used by intelligence agencies and related services, "intelligence" refers integrally to both active data as well as the process and the result of gathering and analyzing such information, as these together form a cohesive network (cf. "hive mind"). In a sense, this usage of "intelligence" at the national level may be somewhat associated with the concept of social intelligence albeit one which is tied to localized or nationalist tradition, politics, law, and the enforcement therof.

http://en.wikipedia.org/wiki/Intelligence_%28information_gathering%29

2.608.6 (EN) INTELLIGENCE

Information about an enemy that has been studied for its importance and accuracy, and provided to warfighters and decision makers.

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.608.7 (EN) COMINT (COMMUNICATIONS INTELLIGENCE)

Technical and intelligence information gathered from foreign communications by other than the intended recipients.

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.609 INTERCAMBIO DE AUTENTICACIÓN

Ver:

- *Autenticación*

2.609.1 INTERCAMBIO DE AUTENTICACIÓN

1. Mecanismo de seguridad destinado a asegurar la identidad de una entidad mediante un intercambio de información (ISO-7498-2).

2. Sucesión de uno o más intercambios de información, con el propósito de realizar una autenticación (ISO/IEC ISO-10181-2).

[Ribagorda:1997]

2.609.2 INTERCAMBIO DE INFORMACIÓN DE AUTENTICACIÓN

Información intercambiada entre el solicitante y el verificador durante el proceso de autenticación del principal (ISO/IEC ISO-9798-1, ISO/IEC ISO-10181-2). [Ribagorda:1997]

2.609.3 INTERCAMBIO DE AUTENTICACIÓN

Mecanismo destinado a garantizar la identidad de una entidad mediante intercambio de información. [ISO-7498-2:1989]

2.609.4 (EN) AUTHENTICATION EXCHANGE

1. (I) A mechanism to verify the identity of an entity by means of information exchange.

2. (O) "A mechanism intended to ensure the identity of an entity by means of information exchange." [ISO-7498-2]

[RFC4949:2007]

2.609.5 (EN) EXCHANGE AUTHENTICATION INFORMATION

Information exchanged between a claimant and a verifier during the process of authenticating a principal. [ISO-10181-2:1996]

2.609.6 (EN) AUTHENTICATION EXCHANGE

A mechanism intended to ensure the identity of an entity by means of information exchange. [ISO-7498-2:1989]

2.609.7 (FR) ÉCHANGE D'AUTHENTIFICATION

Mécanisme destiné à garantir l'identité d'une entité par échange d'informations. [ISO-7498-2:1989]

2.610 INTERCAMBIO DE CLAVES

Ver:

- *Clave*
- *Clave criptográfica*
- *Negociación de claves*

2.610.1 INTERCAMBIO DE CLAVES

Intercambio de claves públicas para establecer un canal de comunicación seguro.

2.610.2 (EN) KEY EXCHANGE

Process of exchanging public keys (and other information) in order to establish secure communications. [CNSSI_4009:2010]

2.611 INTERCEPTACIÓN

2.611.1 INTERCEPTACIÓN

Acción de apoderarse ilegítimamente de una información, en claro o cifrada, transmitida por un canal.

Usualmente, se consigue captando las emisiones de radiofrecuencia del citado canal.

[Ribagorda:1997]

2.611.2 (EN) EAVESDROPPING ATTACK

An attack in which an Attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the Claimant. [NIST-SP800-63:2013]

2.611.3 (EN) EAVESDROPPING

(I) Passive wiretapping done secretly, i.e., without the knowledge of the originator or the intended recipients of the communication. [RFC4949:2007]

2.611.4 (EN) EAVESDROPPING

Eavesdropping is simply listening to a private conversation which may reveal information which can provide access to a facility or network.

http://www.sans.org/security-resources/glossary-of-terms/

2.612 INTERCEPTACIÓN

2.612.1 INTERCEPTAR

Apoderarse de algo antes de que llegue a su destino.

DRAE. Diccionario de la Lengua Española.

2.612.2 (EN) INTERCEPTION

(I) A type of threat action whereby an unauthorized entity directly accesses sensitive data while the data is traveling between authorized sources and destinations. (See: unauthorized disclosure.)

Usage: This type of threat action includes the following subtypes:

- "Theft": Gaining access to sensitive data by stealing a shipment of a physical medium, such as a magnetic tape or disk, that holds the data.
- "Wiretapping (passive)": Monitoring and recording data that is flowing between two points in a communication system. (See: wiretapping.)
- "Emanations analysis": Gaining direct knowledge of communicated data by monitoring and resolving a signal that is emitted by a system and that contains the data but was not intended to communicate the data. (See: emanation.)

[RFC4949:2007]

2.613 INTERCEPTACIÓN DE CONTRASEÑAS

Ver:

- *Sniffer*
- *Contraseña*

2.613.1 INTERCEPTACIÓN DE CONTRASEÑAS

Ataque de interceptación pasiva de una red. Busca descubrir las contraseñas de los usuarios.

2.613.2 (EN) PASSWORD SNIFFING

Passive wiretapping, usually on a local area network, to gain knowledge of passwords.

http://www.sans.org/security-resources/glossary-of-terms/

2.614 INTERCONEXIÓN

Ver:

- *Declaración de Requisitos de Seguridad*

2.614.1 INTERCONEXIÓN

Se produce una interconexión entre sistemas, cuando existe una conexión y se habilitan flujos de información entre los mismos, con diferentes políticas de seguridad, diferentes niveles de confianza, diferentes AOSTIC o una combinación de las anteriores. [CCN-STIC-302:2012]

2.614.2 (EN) INTERCONNECTION

Two systems are interconnected when there is an information flow between them.

2.614.3 (EN) INTERCONNECTION SECURITY AGREEMENT (ISA)

A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high-level roles and responsibilities in management of a cross-domain connection. [CNSSI_4009:2010]

2.615 INTERFERENCIA ELECTROMAGNÉTICA

2.615.1 INTERFERENCIA ELECTROMAGNÉTICA

Perturbación causada por un campo eléctrico o magnético en un sistema.

2.615.2 (EN) ELECTROMAGNETIC INTERFERENCE

electromagnetic emissions from a device, equipment, or system that interfere with the normal operation of another device, equipment, or system. [FIPS-140-2:2001]

2.616 INTERRUPCIÓN

Ver:

- *Continuidad*

2.616.1 INTERRUMPIR

Cortar la continuidad de algo en el lugar o en el tiempo.

DRAE. Diccionario de la Lengua Española.

2.616.2 INTERRUPCIÓN

Suceso no planificado que deja inutilizable un sistema o una aplicación durante un tiempo inaceptable (desmesuradamente largo).

2.616.3 (EN) DISRUPTION

An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction). [CNSSI_4009:2010]

2.616.4 (EN) DISRUPTION

(I) A circumstance or event that interrupts or prevents the correct operation of system services and functions. (See: availability, critical, system integrity, threat consequence.) [RFC4949:2007]

2.616.5 (EN) DISRUPTION

event, whether anticipated (e.g. a labour strike or hurricane) or unanticipated (e.g. a blackout or earthquake), which causes an unplanned, negative deviation from the expected delivery of products or services according to the organizations objectives. [BS25999-1:2006]

2.616.6 (EN) DISRUPTION

An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction). [NIST-SP800-34:2002]

2.616.7 (EN) DISRUPTION

A circumstance or event that interrupts or prevents the correct operation of system services and functions.

http://www.sans.org/security-resources/glossary-of-terms/

2.617 INTRANET

2.617.1 INTRANET

Red TCP/IP de uso privado dentro de una organización.

2.617.2 (EN) INTRANET

A network based on TCP/IP protocols that belongs to an organization and is accessible only by the organizations internal members, employees or others with specific authorization.

http://iab.com/

2.617.3 (EN) INTRANET

An intranet is basically an internal Internet designed to be used within the confines of a company, university, or organization. What distinguishes an intranet from the freely accessible Internet is that an intranet is private. Until recently most corporations relied on proprietary hardware and software systems to network its computers, a costly and time-consuming process made more difficult when offices are scattered around the world. Even under the best of conditions, sharing information among different hardware platforms, file formats and software is not an easy task. By using off-the-shelf Internet technology, intranets solve this problem, making internal communication and collaboration much simpler.

http://www.passwordnow.com/en/glossary/intranet.html

2.618 INTRUSIÓN

Ver:

- *Penetración*
- *Sistema de detección de intrusiones*
- *Sistema de prevención de intrusiones*

2.618.1 INTRUSO

Que se ha introducido sin derecho.

DRAE. Diccionario de la Lengua Española.

2.618.2 INTRUSARSE

Apropiarse, sin razón ni derecho, de un cargo, una autoridad, una jurisdicción, etc.

DRAE. Diccionario de la Lengua Española.

2.618.3 INTRUSIÓN

Cuando un atacante accede a un sistema informático sin autorización con el objetivo de tomar el control de la máquina o recopilar información confidencial.

Para hacerlo, suelen aprovechar alguna vulnerabilidad del sistema afectado.

http://www.inteco.es/glossary/Formacion/Glosario/

2.618.4 INTRUSIÓN

Acción de soslayar o violar los mecanismos de seguridad instalados y los procedimientos de seguridad establecidos con objeto de atacar a un sistema. [Ribagorda:1997]

2.618.5 RESISTENTE A INTRUSIONES

Dispositivo físicamente robusto, diseñado para destruir sus microcircuitos internos cuando se intenta penetrar o, en general, violar de cualquier manera. [Ribagorda:1997]

2.618.6 (EN) INTRUSION

the act of entering a place which is private or where you may not be wanted.

Oxford Advanced Learner's Dictionary.

2.618.1 (EN) INTRUSION

Unauthorized act of bypassing the security mechanisms of a system. [CNSSI_4009:2010]

2.618.2 (EN) INTRUDER

(I) An entity that gains or attempts to gain access to a system or system resource without having authorization to do so. (See: intrusion. Compare: adversary, cracker, hacker.) [RFC4949:2007]

2.618.3 (EN) INTRUSION

1. (I) A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so. (See: IDS.)

2. (I) A type of threat action whereby an unauthorized entity gains access to sensitive data by circumventing a system's security protections. (See: unauthorized disclosure.)

Usage: This type of threat action includes the following subtypes:

- "Trespass": Gaining physical access to sensitive data by circumventing a system's protections.
- "Penetration": Gaining logical access to sensitive data by circumventing a system's protections.
- "Reverse engineering": Acquiring sensitive data by disassembling and analyzing the design of a system component.
- "Cryptanalysis": Transforming encrypted data into plain text without having prior knowledge of encryption parameters or processes. (See: main entry for "cryptanalysis".)

[RFC4949:2007]

2.618.4 (EN) INTRUSION

unauthorized access to a network or a network-connected system i.e. deliberate or accidental unauthorized access to an information system, to include malicious activity against an information system, or unauthorized use of resources within an information system. [ISO-18028-1:2006]

2.618.5 (FR) INTRUSION

Une combinaison délibérée ou accidentelle d' évènements qui peuvent potentiellement causer un accès non autorisé et constituer une activité allant à l'encontre du système IT au sein même ou à l'extérieur du système. [ISO-15947:2002]

2.619 INUNDACIÓN

Ver:

- *Denegación de servicio*
- *Inundación IP*
- *Inundación ICMP*
- *SYN flood*

2.619.1 INUNDADOR

Programa que envía el mismo mensaje o texto de manera reiterada y masiva, pretendiendo así producir un efecto de saturación, colapso o inundación (de ahí su nombre, inundador) en sistemas de mensajería instantánea como MSN Messenger.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.619.1 (EN) FLOODING

An attack that attempts to cause a failure in a system by providing more input than the system can process properly. [CNSSI_4009:2010]

2.619.2 (EN) FLOODING

1. (I) An attack that attempts to cause a failure in a system by providing more input than the system can process properly. (See: denial of service, fairness. Compare: jamming.) [RFC4949:2007]

2.619.3 (EN) FLOODING

Sending large numbers of messages to a host or network at a high rate. In this publication, it specifically refers to wireless access points. [NIST-SP800-94:2007]

2.619.4 (EN) FLOODING

An attack that attempts to cause a failure in (especially, in the security of) a computer system or other data processing entity by providing more input than the entity can process properly.

http://www.sans.org/security-resources/glossary-of-terms/

2.620 INUNDACIÓN ICMP

Ver:

- *Inundación*
- *Denegación de servicio*

2.620.1 INUNDACIÓN ICMP

Ataque de denegación de servicio que actúa saturando al receptor de paquetes ICMP (ping).

2.620.2 (EN) ICMP FLOOD

(I) A denial-of-service attack that sends a host more ICMP echo request ("ping") packets than the protocol implementation can handle. (See: flooding, smurf.) [RFC4949:2007]

2.621 INUNDACIÓN IP

Ver:

- *Inundación*
- *Denegación de servicio*

2.621.1 INUNDACIÓN IP

Ataque de denegación de servicio consistente en enviar una cantidad abrumadora de paquetes IP con el ánimo de saturar y bloquear el sistema receptor.

2.621.2 (EN) IP FLOOD

A denial of service attack that sends a host more echo request ("ping") packets than the protocol implementation can handle.

http://www.sans.org/security-resources/glossary-of-terms/

2.622 INYECCIÓN DE CÓDIGO

2.622.1 ERRORES DE INYECCIÓN

Estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y que tiene como resultado una validación de entradas inapropiada, que permite a los atacantes transferir código malicioso al sistema subyacente a través de una aplicación web. En esta clase de vulnerabilidades se incluye la inyección SQL, la inyección LDAP y la inyección XPath.

http://es.pcisecuritystandards.org

2.622.2 (EN) INJECTION FLAWS

Vulnerability that is created from insecure coding techniques resulting in improper input validation, which allows attackers to relay malicious code through a web application to the underlying system. This class of vulnerabilities includes SQL injection, LDAP injection, and XPath injection.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.622.3 (EN) CODE INJECTION

This threat category includes well-known attack techniques against web applications such as SQL injection (SQLi), cross-site scripting (XSS), cross-site request forgery (CSRF), Remote File Inclusion (RFI) etc. The adversaries placing such attacks try to extract data, steal Responding to the Evolving Threat Environment credentials, take control of the targeted webserver or promote their malicious activities by exploiting vulnerabilities of web applications.

ENISA Threat Landscape [Deliverable – 2012-09-28]

2.622.4 (EN) CWE-94: IMPROPER CONTROL OF GENERATION OF CODE ('CODE INJECTION')

The software constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.

When software allows a user's input to contain code syntax, it might be possible for an attacker to craft the code in such a way that it will alter the intended control flow of the software. Such an alteration could lead to arbitrary code execution.

Injection problems encompass a wide variety of issues -- all mitigated in very different ways. For this reason, the most effective way to discuss these weaknesses is to note the distinct features which classify them as injection weaknesses. The most important issue to note is that all injection problems share one thing in common -- i.e., they allow for the injection of control plane data into the user-controlled data plane. This means that the execution of the process may be altered by sending code in through legitimate data channels, using no other mechanism. While buffer overflows, and many other flaws, involve the use of some further issue to gain execution, injection problems need only for the data to be parsed. The most classic instantiations of this category of weakness are SQL injection and format string vulnerabilities.

http://cwe.mitre.org/data/definitions/

2.622.5 (FR) DÉFAUTS D'INJECTION

Vulnérabilité qui est créée par des techniques de codage non sécurisées, ce qui provoque la validation d'une entrée incorrecte qui permet aux pirates de relayer des codes malveillants par une application Web au système sous-jacent. Cette classe de vulnérabilité comprend les injections SQL, les injections LDAP et les injections XPath.

http://fr.pcisecuritystandards.org/

2.623 INYECCIÓN SQL

Ver:

- http://en.wikipedia.org/wiki/SQL_Injection
- *XPath injection*
- *Null injection*
- *LDAP injection*
- *Meta-Character Injection*

2.623.1 INYECCIÓN SQL

Tipo de ataque a sitios web basados en bases de datos. Una persona malintencionada ejecuta comandos SQL no autorizados aprovechando códigos inseguros de un sistema conectado a Internet. Los ataques de inyección SQL se utilizan para robar información normalmente no disponible de una base de datos o para acceder a las computadoras host de una organización mediante la computadora que funciona como servidor de la base de datos.

http://es.pcisecuritystandards.org

2.623.2 INYECCIÓN SQL

Inyección SQL es un método de infiltración de código intruso que se sirve de una vulnerabilidad presente en una aplicación en el nivel de validación de entradas para la realización de consultas a una base de datos.

El origen de la vulnerabilidad radica en la incorrecta validación de las variables utilizadas en un programa que contiene o genera, código SQL.

http://www.inteco.es/glossary/Formacion/Glosario/

2.623.3 INYECCIÓN SQL

Inyección SQL es una vulnerabilidad informática en el nivel de la validación de las entradas a la base de datos de una aplicación. El origen es el filtrado incorrecto de las variables utilizadas en las partes del programa con código SQL. Es, de hecho, un error de una clase más general de vulnerabilidades que puede ocurrir en cualquier lenguaje de programación o de script que esté incrustado dentro de otro.

Una inyección SQL sucede cuando se inserta o "inyecta" un código SQL "invasor" dentro de otro código SQL para alterar su funcionamiento normal, y hacer que se ejecute maliciosamente el código "invasor" en la base de datos.

http://es.wikipedia.org/wiki/Inyecci%C3%B3n_SQL

2.623.4 (EN) SQL INJECTION

Form of attack on database-driven web site. A malicious individual executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet. SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization’s host computers through the computer that is hosting the database.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.623.5 (EN) SQL INJECTION

SQL injection is a type of input validation attack specific to database-driven applications where SQL code is inserted into application queries to manipulate the database.

http://www.sans.org/security-resources/glossary-of-terms/

2.623.6 (EN) SQL INJECTION

An attack technique used to exploit web sites by altering backend SQL statements through manipulating application input.

http://www.webappsec.org/projects/glossary/

2.623.7 (EN) SQL INJECTION

SQL injection is a type of security exploit in which the attacker adds Structured Query Language (SQL) code to a Web form input box to gain access to resources or make changes to data. An SQL query is a request for some action to be performed on a database. Typically, on a Web form for

user authentication, when a user enters their name and password into the text boxes provided for them, those values are inserted into a SELECT query. If the values entered are found as expected, the user is allowed access; if they aren't found, access is denied. However, most Web forms have no mechanisms in place to block input other than names and passwords. Unless such precautions are taken, an attacker can use the input boxes to send their own request to the database, which could allow them to download the entire database or interact with it in other illicit ways.

http://searchsoftwarequality.techtarget.com/glossary/

2.623.8 (EN) SQL INJECTION

This attack exploits target software that constructs SQL statements based on user input. An attacker crafts input strings so that when the target software constructs SQL statements based on the input, the resulting SQL statement performs actions other than those the application intended.

SQL Injection results from failure of the application to appropriately validate input. When specially crafted user-controlled input consisting of SQL syntax is used without proper validation as part of SQL queries, it is possible to glean information from the database in ways not envisaged during application design. Depending upon the database and the design of the application, it may also be possible to leverage injection to have the database execute system-related commands of the attacker's choice. SQL Injection enables an attacker to talk directly to the database, thus bypassing the application completely. Sucessful injection can cause information disclosure as well as ability to add or modify data in the database. In order to successfully inject SQL and retrieve information from a database, an attacker:

Attack Pattern 66

http://capec.mitre.org/data/index.html

2.623.9 (FR) INJECTION DE COMMANDES SQL

Type d'attaque sur un site Web depuis une base de données. Un pirate exécute des commandes SQL non autorisées en profitant d'un code non sécurisé sur un système connecté à Internet. Les attaques par injection de commandes SQL sont utilisées pour dérober des renseignements provenant d'une base de données dont les données ne seraient normalement pas disponibles, et/ou pour accéder aux ordinateurs hôtes par l'intermédiaire de l'ordinateur hébergeant la base de données.

http://fr.pcisecuritystandards.org/

2.624 IPSEC - IP SECURITY

Acrónimos: IPsec

Ver:

- *Red privada virtual*
- *AH - Authentication Header*
- *ESP - Encapsulating Security Payload*
- http://www.ietf.org/rfc/rfc4301
- *Asociación de seguridad (SA)*
- *IKE - Internet Key Exchange*
- *ISAKMP - Internet Security Association Key Management Protocol*

- *Oakley*

2.624.1 IPSEC - IP SECURITY

IPsec es una colección de mecanismos de protección que extienden los paquetes IP para proporcionar servicios de control de acceso, integridad, autenticación de origen, detección y rechazo de duplicados y confidencialidad.

2.624.2 (EN) IP SECURITY (IPSEC)

Suite of protocols for securing Internet Protocol (IP) communications at the network layer, layer 3 of the OSI model by authenticating and/or encrypting each IP packet in a data stream. IPSec also includes protocols for cryptographic key establishment. [CNSSI_4009:2010]

2.624.3 (EN) IP SECURITY PROTOCOL (IPSEC)

1a. (I) The name of the IETF working group that is specifying an architecture [R2401, R4301] and set of protocols to provide security services for IP traffic. (See: AH, ESP, IKE, SAD, SPD. Compare: IPSO.) 1b. (I) A collective name for the IP security architecture [R4301] and associated set of protocols (primarily AH, ESP, and IKE). [RFC4949:2007]

2.624.4 (EN) IPSEC - IP SECURITY

IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, detection and rejection of replays (a form of partial sequence integrity), confidentiality (via encryption), and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection in a standard fashion for all protocols that may be carried over IP (including IP itself).

2.624.5 (FR) IPSEC (IP SECURITY)

Protocole de communication sécurisé basé sur IP permettant de d'assurer de la confidentialité et l'intégrité des paquets échangés.

http://www.cases.public.lu/functions/glossaire/

2.624.6 (FR) IPSEC - INTERNET PROTOCOL SECURITY.

IPSEC est un ensemble de protocoles normalisés sous la conduite de l'IETF, afin d'améliorer la sécurité du protocole IPv4 (natif en IPv6) face aux attaques de type écoute (IP-sniffing), usurpation d'identité (IP-spoofing), prédiction de séquences de paquets, re-jeu de trafic...

IPSEC garantit l'authenticité, l'intégrité, la confidentialité et le non-re-jeu des paquets IP échangés de bout en bout entre deux entités en s'appuyant sur les techniques de cryptographie asymétrique.

IPSEC définit principalement:

- Deux protocoles d'encapsulation sécurisée: AH (Authentication Header) et ESP (Encryption Security Payload).
- Deux structures de gestion de la sécurité par les protagonistes de la communication IPSEC: SA (Security Association) et SPD (Security Policy Database).

- Des procédures d'échange et de gestion des clés: IKE (Internet Key Exchange).

http://securit.free.fr/glossaire.htm

2.625 ISAKMP - INTERNET SECURITY ASSOCIATION KEY MANAGEMENT PROTOCOL

Acrónimos: ISAKMP

Ver:

- *IPsec - IP security*
- http://www.ietf.org/rfc/rfc4306
- *Asociación de seguridad (SA)*
- *Oakley*

2.625.1 ISAKMP - INTERNET SECURITY ASSOCIATION KEY MANAGEMENT PROTOCOL

Protocolo utilizado en el marco de IPsec para autenticar entidades, así como para establecer y gestionar asociaciones de seguridad.

2.625.2 (EN) INTERNET SECURITY ASSOCIATION AND KEY MANAGEMENT PROTOCOL (ISAKMP)

(I) An Internet IPsec protocol [R2408] to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism. [RFC4949:2007]

2.625.3 (EN) ISAKMP (INTERNET SECURITY ASSOCIATION KEY MANAGEMENT PROTOCOL)

A set of specifications defined in RFC 2408 and used in close conjunction with IPSec. Defines the procedures for authenticating, creating and managing security associations, generating keys, and using digital certificates when establishing VPN connections.

http://www.watchguard.com/glossary/

2.626 ISO

Acrónimos: ISO

Ver:

- *Responsable de seguridad corporativa*
- *Responsable de seguridad de la información*
- *Responsable de seguridad del sistema*
- *Criptocustodio*

2.626.1 (EN) INFORMATION SECURITY OFFICER (ISO)

Responsible to the Information Resource Manager (IRM) for administering the information security functions within the university. The ISO is the universitys internal and external point of contact and internal resource for all information security matters. The ISO leads the Computer Incident Response Team when security incidents occur and reports to the IRM. If an ISO is not designated, the IRM serves in this capacity.

http://www.utexas.edu/its/policies/glossary.html

2.627 ITSEC - INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA

Acrónimos: ITSEC

Ver:

- *Criterios comunes*
- *TCSEC - Trusted Computer System Evaluation Criteria*

http://en.wikipedia.org/wiki/ITSEC

2.627.1 ITSEC

Ha surgido de la armonización de varios sistemas europeos de criterios de seguridad en TI. Tiene un enfoque más amplio que TCSEC.

Los criterios establecidos en ITSEC permiten seleccionar funciones de seguridad arbitrarias (objetivos de seguridad que el sistema bajo estudio debe cumplir teniendo presentes las leyes y reglamentaciones).

Se definen siete niveles de evaluación, denominados E0 a E6, que representan una confianza para alcanzar la meta u objetivo de seguridad. E0 representa una confianza inadecuada. E1, el punto de entrada por debajo del cual no cabe la confianza útil, y E6 el nivel de confianza más elevado. Por ello, los presentes criterios pueden aplicarse a una gama de posibles sistemas y productos más amplia que los del TCSEC.

El objetivo del proceso de evaluación es permitir al evaluador la preparación de un informe imparcial en el que se indique si el sistema bajo estudio satisface o no su meta de seguridad al nivel de confianza precisado por el nivel de evaluación indicado.

http://www.csi.map.es/csi/silice/Segurd21.html

(en) Information Technology Security Evaluation Criteria (ITSEC)

(N) A Standard [ITSEC] jointly developed by France, Germany, the Netherlands, and the United Kingdom for use in the European Union; accommodates a wider range of security assurance and functionality combinations than the TCSEC. Superseded by the Common Criteria.

[RFC4949:2007]

2.627.2 (EN) ITSEC

Germany, the Netherlands and the United Kingdom published the Information Technology Security Evaluation Criteria (ITSEC) based on existing work in their respective countries. Following

extensive international review, Version 1.2 was subsequently published in June 1991 by the Commission of the European Communities for operational use within evaluation and certification schemes.

The ITSEC is a structured set of criteria for evaluating computer security within products and systems. The product or system being evaluated, called the target of evaluation, is subjected to a detailed examination of its security features culminating in comprehensive and informed functional and penetration testing.

The degree of examination depends upon the level of confidence desired in the target. To provide different levels of confidence, the ITSEC defines evaluation levels, denoted E0 through E6. Higher evaluation levels involve more extensive examination and testing of the target.

Unlike earlier criteria, notably the TCSEC developed by the US defense establishment, the ITSEC did not require evaluated targets to contain specific technical features in order to achieve a particular assurance level. For example, an ITSEC target might provide authentication or integrity features without providing confidentiality or availability. A given target's security features were documented in a Security Target document, whose contents had to be evaluated and approved before the target itself was evaluated. Each ITSEC evaluation was based exclusively on verifying the security features identified in the Security Target.

Since the launch of the ITSEC in 1990, a number of other European countries have agreed to recognise the validity of ITSEC evaluations.

The ITSEC has been largely replaced by Common Criteria, which provides similarly-defined evaluation levels and implements the target of evaluation concept and the Security Target document.

http://en.wikipedia.org/wiki/ITSEC

2.628 JADE

Ver:

- *PURPLE*
- *ENIGMA*

2.628.1 JADE

Sistema de cifrado empleado por la Armada Imperial Japonesa durante la Segunda Guerra Mundial.

2.628.2 (EN) JADE

Codename for machine used by the Japanese Imperial Navy to encrypt and decrypt messages during World War II.

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.629 JAMMING

Ver:

- *Denegación de servicio*

2.629.1 JAMMING

Interferencia radio que dificulta o impide la recepción de señales radiadas.

2.629.2 (EN) JAMMING:

An activity the purpose of which is interference with the reception of broadcast communications.

The Tallinn Manual, 2013

2.629.3 (EN) JAMMING

An attack that attempts to interfere with the reception of broadcast communications. [CNSSI_4009:2010]

2.630 JERARQUÍA DE CERTIFICACIÓN

Ver:

- *Certificado X.509*

2.630.1 JERARQUÍA DE CERTIFICACIÓN

Estructura de datos en forma de árbol en la que aparecen como nodos intermedios autoridades de certificación y como hijos de cada nodo aquellas entidades que han sido certificadas por la autoridad en el nodo padre. En última instancia hay un nodo raíz ocupado por la autoridad de certificación raíz.

2.630.2 (EN) CERTIFICATION HIERARCHY

1. (I) A tree-structured (loop-free) topology of relationships between CAs and the entities to whom the CAs issue public-key certificates. (See: hierarchical PKI, hierarchy management.)

2. (I) /PEM/ A certification hierarchy for PEM has three levels of CAs [R1422]:

- The highest level is the "Internet Policy Registration Authority".
- A CA at the second-highest level is a "policy certification authority".
- A CA at the third-highest level is a "certification authority".

[RFC4949:2007]

2.631 KASUMI

Ver:

- *Cifrado en bloque*
- *Criptografía de clave secreta*
- *MISTY*
- *A5 - Cifrado de voz GSM*
- http://en.wikipedia.org/wiki/KASUMI_%28block_cipher%29

2.631.1 KASUMI

Algoritmo de cifra basado en un secreto compartido (clave). Cifra el texto en bloques de 64 bits. Utiliza claves de 128 bits.

2.631.2 (EN) KASUMI

In cryptography, KASUMI, also termed A5/3, is a block cipher used in the confidentiality (f8) and integrity algorithms (f9) for 3GPP mobile communications. A number of serious weaknesses in the cipher have been identified.

KASUMI was designed by the Security Algorithms Group of Experts (SAGE), part of the European standards body ETSI. Rather than invent a cipher from scratch, SAGE selected an existing algorithm, MISTY1, and optimised it slightly for implementation in hardware. Hence, MISTY1 and KASUMI are very similar kasumi () is the Japanese word for "mist" and the cryptanalysis of one is likely to be readily adaptable to the other. KASUMI maintains an efficient implementation in software.

http://en.wikipedia.org/wiki/KASUMI_%28block_cipher%29

2.632 KERBEROS

Ver:

- http://web.mit.edu/Kerberos/
- http://www.ietf.org/rfc/rfc4120
- *Single sign-on*

2.632.1 KERBEROS

Servicio de autenticación mutua de entidades (usuarios, estaciones de trabajo, servidores de red etc.) desarrollado en el marco del proyecto Athenea del MIT (Massachussetts Institute of Technology). La versión 5 se encuentra en estado de borrador de Norma Internet (RFC 1510). [Ribagorda:1997]

2.632.2 (EN) KERBEROS

(I) A system developed at the Massachusetts Institute of Technology that depends on passwords and symmetric cryptography (DES) to implement ticket-based, peer entity authentication service and access control service distributed in a client-server network environment. [R4120, Stei] (See: realm.) [RFC4949:2007]

2.632.3 (FR) KERBEROS

Système d'authentification réseau basé sur un tiers de confiance et l'utilisation de tickets permettant l'accès aux ressources et permettant de créer des relations de confiance transitive. Kerberos a été développé au MIT.

http://www.cases.public.lu/functions/glossaire/

2.632.4 (FR) KERBEROS

Kerberos est une méthode évoluée et extrêmement répandue d'authentification mutuelle (client et serveur), sans circulation de mot de passe sur le réseau et avec solution d'anti-rejeu.

Les principes de Kerberos reposent sur:

- La notion de "tickets" (tickets d'autorisation de tickets et ticket de session).
- Un centre de distribution des clés (Key Distribution Center), autorité approuvée dans le système Kerberos. Le tryptique KDC, serveur, client forme les trois têtes du chien Cerbère !
- Les techniques de cryptographie symétrique.

Kerberos v.4 a été développé au MIT (projet Athena) et déployé massivement en environnement Unix. La version courante, Kerberos v.5, compense certaines lacunes de sécurité mais n'est pas inter-opérable avec la version 4.

Windows 2000 implémente la méthode d'authentification Kerberos en natif.

http://securit.free.fr/glossaire.htm

2.633 KERNEL DE SEGURIDAD

2.633.1 KERNEL DE SEGURIDAD

Elementos hardware, firmware y software que conjuntamente proporcionan la funcionalidad requerida por un monitor de referencia. El kernel de seguridad debe intermediar todos los accesos, debe estar protegido frente a modificaciones no autorizadas y debe ser posible verificar que funciona correctamente.

2.633.2 (EN) SECURITY KERNEL

Hardware, firmware, and software elements of a trusted computing base implementing the reference monitor concept. Security kernel must mediate all accesses, be protected from modification, and be verifiable as correct. [CNSSI_4009:2010]

2.634 KHAFRE

Ver:

- *DES - Data Encryption Standard*
- *Khufu*
- *Cifrado en bloque*
- *Criptografía de clave secreta*
- http://en.wikipedia.org/wiki/Khufu_and_Khafre

2.634.1 KHAFRE

Algoritmo de cifra basado en un secreto compartido (clave). Cifra el texto en bloques de 64 bits. Utiliza claves de 512 bits.

Fue diseñado en Xerox Corporation por Ralph C. Merkle.

2.634.2 (EN) KHAFRE

(N) A patented, symmetric block cipher designed by Ralph C. Merkle as a plug-in replacement for DES. [Schn] [RFC4949:2007]

2.635 KHUFU

Ver:

- *DES - Data Encryption Standard*
- *Khafre*
- *Cifrado en bloque*
- *Criptografía de clave secreta*
- http://en.wikipedia.org/wiki/Khufu_and_Khafre

2.635.1 KHUFU

Algoritmo de cifra basado en un secreto compartido (clave). Cifra el texto en bloques de 64 bits. Utiliza claves de 512 bits.

Fue diseñado en Xerox Corporation por Ralph C. Merkle.

2.635.2 (EN) KHUFU

(N) A patented, symmetric block cipher designed by Ralph C. Merkle as a plug-in replacement for DES. [Schn] [RFC4949:2007]

2.636 L2TP - PROTOCOLO DE TÚNEL EN LA CAPA 2

Acrónimos: L2TP

Ver:

- http://www.ietf.org/rfc/rfc2661

2.636.1 L2TP (LAYER 2 TUNNELING PROTOCOL)

fue diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolos PPTP y L2F, creado para corregir las deficiencias de estos protocolos y establecerse como un estándar aprobado por el IETF (RFC 2661). L2TP utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado. L2TP define su propio protocolo de establecimiento de túneles, basado en L2F. El transporte de L2TP está definido para una gran variedad de tipos de paquete, incluyendo X.25, Frame Relay y ATM.

Al utilizar PPP para el establecimiento telefónico de enlaces, L2TP incluye los mecanismos de autenticación de PPP, PAP y CHAP. De forma similar a PPTP, soporta la utilización de estos protocolos de autenticación, como RADIUS.

http://es.wikipedia.org/wiki/L2TP

2.636.2 (EN) LAYER 2 TUNNELING PROTOCOL (L2TP)

(N) An Internet client-server protocol that combines aspects of PPTP and L2F and supports tunneling of PPP over an IP network or over frame relay or other switched network. (See: VPN.) [RFC4949:2007]

2.636.3 (EN) L2TP - LAYER 2 TUNNELING PROTOCOL

An extension of the Point-to-Point Tunneling Protocol used by an Internet service provider to enable the operation of a virtual private network over the Internet.

http://www.sans.org/security-resources/glossary-of-terms/

2.636.4 (FR) L2TP - LAYER 2 TUNNELING PROTOCOL

VPN de niveau 2 (couche liaison du système OSI) basé sur les propositions PPTP et L2F (RFC 2341 obsolète), L2TP permet l'établissement de tunnels de bout en bout et assure les services de sécurité suivants:

- Authentification (CHAP, PAP).
- Confidentialité (chiffrement par secret partagé, ou par clé publique en utilisant l'algorithme RC4 à 40 ou 128 bits).

L2TP encapsule des trames PPP. Les paquets L2TP ainsi formés sont ensuite encapsulés dans un protocole de transport (Frame Relay, ATM, IP/UDP).

L2TP complète PPTP en proposant une solution de transport des trames PPP sur un réseau non-IP.

http://securit.free.fr/glossaire.htm

2.637 LDAP INJECTION

Ver:

- *LDAP - Lightweight Directory Access Protocol*
- *Inyección SQL*
- *XPath injection*
- *Null injection*
- *Meta-Character Injection*

2.637.1 LDAP INJECTION

Abuso de las peticiones LDAP para alterar fraudulentamente el contenido del directorio de información de un servidor en red.

2.637.2 (EN) LDAP INJECTION

A technique for exploiting a web site by altering backend LDAP statements through manipulating application input.

http://www.webappsec.org/projects/glossary/

2.637.3 (EN) LDAP INJECTION

LDAP injection is a specific form of attack that can be employed to compromise Web sites that construct LDAP (Lightweight Directory Access Protocol) statements from data provided by users. This is done by changing LDAP statements so dynamic Web applications can run with invalid permissions, allowing the attacker to alter, add or delete content. LDAP is a protocol that facilitates the location of organizations, individuals and other resources in a network. It is a streamlined version of DAP (Directory Access Protocol), which is part of X.500, a standard for network directory services.

http://searchsoftwarequality.techtarget.com/glossary/

2.638 LDAP - LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL

Acrónimos: LDAP

Ver:

- *LDAP injection*

2.638.1 LDAP (LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL)

es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) al que pueden realizarse consultas.

Habitualmente, almacena la información de login (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc).

En conclusión, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.

http://es.wikipedia.org/wiki/LDAP

2.638.2 (EN) LDAP (LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL)

A protocol that helps manage information about authorized users on a network such as names, phone numbers, addresses, and what a user is and is not allowed to access. LDAP is vendor- and platform-neutral, working across otherwise incompatible systems.

http://www.watchguard.com/glossary/

2.639 LEAP - LIGHTWEIGHT EXTENSIBLE AUTHENTICATION PROTOCOL

Acrónimos: LEAP

Ver:

- *Extensible Authentication Protocol*

2.639.1 LEAP

Protocolo del tipo EAP patentado por Cisco basado en nombre de usuario y contraseña que se envía sin protección. Esta metodología descuida la protección de las credenciales durante la fase de autenticación del usuario con el servidor.

2.639.2 (EN) LIGHTWEIGHT EXTENSIBLE AUTHENTICATION PROTOCOL (LEAP)

is a proprietary wireless LAN authentication method developed by Cisco Systems. Important features of LEAP are dynamic WEP keys and mutual authentication (between a wireless client and a RADIUS server). LEAP allows for clients to reauthenticate frequently; upon each successful authentication, the clients acquire a new WEP key (with the hope that the WEP keys don't live long enough to be cracked).

http://en.wikipedia.org/wiki/Lightweight_Extensible_Authentication_Protocol

2.640 LEMA DE KERCKHOFFS

2.640.1 LEMA DE KERCKHOFFS

Postulado del criptógrafo holandés Kerckhoffs (Auguste Kerckhoffs von Nieuwenhof, 1835-1903, autor de uno de los libros históricos de la criptografía, La Cryptographie militaire), que establece que la seguridad de cifrado debe residir, exclusivamente, en el secreto de la clave y no en el desconocimiento del algoritmo de cifrado. Antes bien, esta última debe ser de general conocimiento por la comunidad criptográfica, para que pueda ser criptoanalizada y descubiertas sus vulnerabilidades si las hubiere.

[Ribagorda:1997]

2.640.2 (EN) KERCKHOFFS LAW

Kerckhoffs' Law also known as Kerckhoffs' principle, assumption, or axiom, states that a cryptosystem or cryptographic algorithm must be secure even if all its inner workings, and everything about it (saving only the key) is known.

Originally stated (by Auguste Kerckhoffs in the 19th century) that a system "must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience."

2.641 LEYES DE COURTNEY

2.641.1 LEYES DE COURTNEY

Principios para la gestión de la seguridad de los sistemas:

- No se puede decir nada útil respecto de la seguridad de un sistema si no es en un contexto concreto de aplicación.
- Nunca se debe gastar más dinero en proteger una vulnerabilidad que el gasto que supondría un ataque a través de la misma.
    - Corolario 1: la seguridad perfecta tiene un coste infinito.
    - Corolario 2: no existe el riesgo cero.

- No hay soluciones técnicas a los problemas de gestión; pero se pueden encontrar soluciones basadas en la gestión para problemas técnicos.

2.641.2 (EN) COURTNEY'S LAWS

(N) Principles for managing system security that were stated by Robert H. Courtney, Jr.

Tutorial: Bill Murray codified Courtney's laws as follows: [Murr]

- Courtney's first law: You cannot say anything interesting (i.e., significant) about the security of a system except in the context of a particular application and environment.
- Courtney's second law: Never spend more money eliminating a security exposure than tolerating it will cost you. (See: acceptable risk, risk analysis.)
  - First corollary: Perfect security has infinite cost.
  - Second corollary: There is no such thing as zero risk.
- Courtney's third law: There are no technical solutions to management problems, but there are management solutions to technical problems.

[RFC4949:2007]

2.642 LIBRO DE CLAVES

Ver:

- *Clave*
- *Clave criptográfica*

2.642.1 LIBRO DE CLAVES

Documento que recoge las claves criptográficas que serán usadas por un criptosistema durante un tiempo.

[Ribagorda:1997]

2.642.2 LIBRO DE CLAVES

Documento que recoge las claves que serán utilizadas por la red de cifra durante un tiempo determinado.

[CESID:1997]

2.643 LIBRO DE CÓDIGOS

Ver:

- *Código*

2.643.1 LIBRO DE CLAVES

Documento que recoge las claves que serán utilizadas por la red de cifra durante un tiempo determinado. [CESID:1997]

2.643.1 (EN) CODE BOOK

Document containing plain text and code equivalents in a systematic arrangement, or a technique of machine encryption using a word substitution technique. [CNSSI_4009:2010]

2.643.2 (EN) CODE BOOK

1. (I) Document containing a systematically arranged list of plaintext units and their ciphertext equivalents. [C4009]

2. (I) An encryption algorithm that uses a word substitution technique. [C4009] (See: code, ECB.)

[RFC4949:2007]

2.643.3 (EN) CODEBOOK

A book or other document that lists the answers (the key) to the secret code.

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.644 LISTA DE CONTROL DE ACCESO

Acrónimos: ACL

Ver:

- *Control de acceso*

2.644.1 LISTA DE CONTROL DE ACCESO (ACL)

Especificación de un conjunto de reglas representadas mediante entradas de control de acceso basadas en diferentes campos o propiedades. [CCN-STIC-401:2007]

2.644.2 LISTA DE CONTROL DE ACCESOS

Lista de entidades, junto con sus derechos de acceso, que están autorizadas para acceder a un recurso (ISO-7498-2).

Es un mecanismo de seguridad que implementan el modelo de control de accesos.

[Ribagorda:1997]

2.644.3 LISTA DE CONTROL DE ACCESO

Lista de entidades, con sus derechos de acceso, que están autorizadas a tener acceso a un recurso. [ISO-7498-2:1989]

2.644.1 (EN) ACCESS CONTROL LIST (ACL)

1. A list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.

2. A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity.

[CNSSI_4009:2010]

2.644.2 (EN) ACCESS CONTROL LIST (ACL)

(I) /information system/ A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity. (Compare: access control matrix, access list, access profile, capability list.) [RFC4949:2007]

2.644.3 (EN) ACCESS CONTROL LIST

A list of entities, together with their access rights, which are authorized to have access to a resource. [ISO-7498-2:1989]

2.644.4 (EN) ACCESS CONTROL LIST

An access control list (ACL) is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges. The most common privileges include the ability to read a file (or all the files in a directory), to write to the file or files, and to execute the file (if it is an executable file, or program). Microsoft Windows NT/2000, Novell's NetWare, Digital's OpenVMS, and Unix-based systems are among the operating systems that use access control lists. The list is implemented differently by each operating system.

http://searchsoftwarequality.techtarget.com/glossary/

2.644.5 (EN) ACCESS CONTROL LIST (ACL)

A mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted to access the resource.

http://www.sans.org/security-resources/glossary-of-terms/

2.644.6 (EN) ACCESS CONTROL LIST (ACL)

An access control list (ACL) is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges. The most common privileges include the ability to read a file (or all the files in a directory), to write to the file or files, and to execute the file (if it is an executable file, or program). Microsoft Windows NT/2000, Novell's NetWare, Digital's OpenVMS, and UNIX-based systems are among the operating systems that use access control lists. The list is implemented differently by each operating system.

http://searchsoftwarequality.techtarget.com/

2.644.7 (FR) LISTE DE CONTRÔLE D'ACCÈS

Liste des entités qui sont autorisées à accéder à une ressource, avec leurs autorisations d'accès. [ISO-7498-2:1989]

2.644.8 (FR) LISTE DE CONTRÔLE D'ACCÈS

Liste de contrôle d'accès utilisée dans de nombreuses situations et qui définit quelles ressources (utilisateurs, ordinateurs, etc.) peuvent accéder à quels services (e-mail, Internet, etc.).

http://www.cases.public.lu/functions/glossaire/

2.645 LISTA DE REVOCACIÓN DE AUTORIDAD DE ATRIBUTO

Acrónimos: AARL

Ver:

- *Certificado de atributo*
- *Lista de revocación de certificado de atributo*
- *Autoridad de atributo*

2.645.1 LISTA DE REVOCACIÓN DE AUTORIDAD DE ATRIBUTO

Relación de certificados de atributos emitidos para Autoridades de Atributos que ya no son reconocidas como válidas por la entidad emisora.

2.645.2 LISTA DE REVOCACIÓN DE AUTORIDAD DE ATRIBUTO

Lista de revocación que contiene una lista de referencias para certificados de atributo expedidos por las AA, que la autoridad expedidora ya no considera válidos. [X.509:2005]

2.645.3 (EN) ATTRIBUTE AUTHORITY REVOCATION LIST

A revocation list containing a list of references to attribute certificates issued to AAs that are no longer considered valid by the issuing authority. [X.509:2005]

2.645.4 (FR) LISTE DE REVOCATION D'AUTORITE D'ATTRIBUT

liste de révocation contenant une liste de références de certificats d'attribut concernant des autorités d'attribut qui ne sont plus considérées comme valides par l'autorité émettrice. [X.509:2005]

2.646 LISTA DE REVOCACIÓN DE AUTORIDADES DE CERTIFICACIÓN

Acrónimos: CARL

Ver:

- *Autoridad de certificación (AC)*
- *Certificado de AC*

2.646.1 LISTA DE REVOCACIÓN DE AUTORIDAD DE CERTIFICACIÓN

Lista de revocación que incluye una lista de certificados de claves públicas expedidos por autoridades de certificación, a las que el expedidor del certificado ya no considera válidos. [X.509:2005]

2.646.2 (EN) CERTIFICATION AUTHORITY REVOCATION LIST

A CARL is a revocation list containing a list of public-key certificates issued to certification authorities, that are no longer considered valid by the certificate issuer. [X.509:2005]

2.647 LISTA DE REVOCACIÓN DE CERTIFICADO DE ATRIBUTO

Acrónimos: ACRL

Ver:

- *Certificado de atributo*
- *Lista de revocación de autoridad de atributo*
- *Lista de revocación de certificados*

2.647.1 LISTA DE REVOCACIÓN DE CERTIFICADO DE ATRIBUTO

Lista de revocación que contiene una lista de referencias para certificados de atributo que la autoridad expedidora ya no considera válidos. [X.509:2005]

2.647.2 (EN) ATTRIBUTE CERTIFICATE REVOCATION LIST

A revocation list containing a list of references to attribute certificates that are no longer considered valid by the issuing authority. [X.509:2005]

2.647.3 (FR) LISTE DE REVOCATION DE CERTIFICAT D'ATTRIBUT

liste de révocation contenant une liste de références de certificats d'attribut qui ne sont plus considérés comme valides par l'autorité émettrice. [X.509:2005]

2.648 LISTA DE REVOCACIÓN DE CERTIFICADOS

Acrónimos: CRL

Ver:

- *Certificado de revocación*
- *Lista de revocación de certificado de atributo*
- *Punto de distribución de CRL*
- *CRL incremental*
- *CRL completa*
- *CRL indirecto*

2.648.1 LISTA DE REVOCACIÓN DE CERTIFICADOS

Lista firmada que indica un conjunto de certificados que el expedidor de certificados ya no considera válidos. Además del término genérico CRL, se definen algunos tipos de CRL específicos para CRL que tratan ámbitos particulares. [X.509:2005]

2.648.2 CERTIFICADO DE LISTA DE REVOCACIONES

Certificado de seguridad que contiene una lista de certificados de seguridad que han sido revocados. [X.810:1995]

2.648.3 LISTA DE REVOCACIÓN DE CERTIFICADOS

Relación de certificados emitidos por una entidad que ya no son reconocidos como válidos por dicha entidad.

2.648.1 (EN) CERTIFICATE REVOCATION LIST (CRL)

A list of revoked public key certificates created and digitally signed by a Certification Authority. [CNSSI_4009:2010]

2.648.2 (EN) X.509 CERTIFICATE REVOCATION LIST (CRL)

(N) A CRL in one of the formats defined by X.509 -- version 1 (v1) or version 2 (v2). (The v1 and v2 designations for an X.509 CRL are disjoint from the v1 and v2 designations for an X.509 public- key certificate, and from the v1 designation for an X.509 attribute certificate.) (See: certificate revocation.) [RFC4949:2007]

2.648.3 (EN) CERTIFICATE REVOCATION LIST

A CRL is a signed list indicating a set of certificates that are no longer considered valid by the certificate issuer. In addition to the generic term CRL, some specific CRL types are defined for CRLs that cover particular scopes. [X.509:2005]

2.648.4 (EN) REVOCATION LIST CERTIFICATE

A security certificate that identifies a list of security certificates that have been revoked. [X.810:1995]

2.648.5 (FR) LISTE DE REVOCATION DE CERTIFICAT

liste signée indiquant un ensemble de certificats qui ne sont plus considérés comme valides par leur émetteur. Certains types de listes CRL spécifiques sont définis en plus du type générique de liste CRL, pour couvrir des domaines particuliers. [X.509:2005]

2.648.6 (FR) CERTIFICAT DE REVOCATION DE LISTE

certificat de sécurité qui identifie une liste de certificats de sécurité qui ont été révoqués. [X.810:1995]

2.649 LISTA BLANCA

Ver

- *Lista negra*

2.649.1 LISTA BLANCA

Relación de elementos que se sabe positivamente que son aceptables en un sistema. Es lo contario de una “lista negra”.

2.649.2 (EN) WHITELISTS:

Whitelists refer to defined lists of “known good" items: users, network addresses. applications, and so on. typically for the purpose of exception-based security where any item not explicitly defined as “known good" results in a remediation action (e.g. alert and block}. Whitelists contrast blacklists. which define “known bad” items. [knapp:2014]

2.649.3 (EN) WHITE-LISTING:

Whitelisting refers to the act of comparing an item against a list of approved items for the purpose of assessing whether it is allowed or should be blocked. Typically referred to in the context of Application Whitelisting. which prevents unauthorized applications from executing on a host by comparing all applications against a whitelist of authorized applications. [knapp:2014]

2.649.4 (EN) APPLICATION WHITELISTING:

Application Whitelisting (AW) is a form of whitelisting intended to control which executable files [applications] are allowed to operate. AW systems typically work by first establishing the “white-list” of allowed applications. after which point any attempt to execute code will be compared against that list. If the application is not allowed. it will be prevented from executing. AW often operates at low levels within the kernel of the host operating system. [knapp:2014]

2.649.1 (EN) USER WHITELISTING:

The process of establishing a “whitelist” of known valid user identities and/or accounts. for the purpose of detecting and/or preventing rogue user activities. See also: Application Whitelisting. [knapp:2014]

2.649.2 (EN) WHITELIST

A list of computers, IP (Internet Protocol) addresses, user names or other identifiers to specifically allow access to a computing resource. Normally combined with a default "no-access" policy.

http://cyber.law.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas

2.650 LISTA NEGRA

Ver

- *Lista blanca*

2.650.1 LISTA NEGRA

Lista de objetos o sujetos indeseados. Su objetivo es identificarlos y detenerlos antes de que lleguen a entrar en el sistema o causar algún daño.

2.650.2 (EN) BLACKLISTING

Blacklisting refers to the technique of defining known malicious behavior, content, code, and so on. Blacklists are typically used for threat detection, comparing network traffic, files, users, or some other quantifiable metric against a relevant blacklist. For example, an intrusion prevention system (IPS) will compare the contents of network packets against blacklists of known malware, indicators of exploits, and other threats so that offending traffic (i.e. packets that match a signature within the blacklist) can be blocked. [knapp:2014]

2.650.3 (EN) BLACKLISTING

The process of the system invalidating a user ID based on the user's inappropriate actions. A blacklisted user ID cannot be used to log on to the system, even with the correct authenticator. Blacklisting and lifting of a blacklisting are both security-relevant events. Blacklisting also applies to blocks placed against IP addresses to prevent inappropriate or unauthorized use of internet resources. [CNSSI_4009:2010]

2.650.4 (EN) BLACKLIST

A list of discrete entities, such as hosts or applications, that have been previously determined to be associated with malicious activity. [NIST-SP800-94:2007]

2.650.5 (EN) BLACK LIST

List of known malicious objects (Websites, vandals, script commands, etc.) that should be blocked by default.

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.650.6 (EN) BLACKLIST

A list of computers, IP addresses, user names or other identifiers to block from access to a computing resource.

http://cyber.law.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas

2.651 LITTLE ENDIAN

Ver:

- *Big endian*

2.651.1 LITTLE ENDIAN

Ordenación de los bytes en memoria: byte menos significativo primero.

2.651.2 (EN) LITTLE ENDIAN

Byte ordering in RAM: the least significant byte is at the lowest address.

2.652 LOGIN

2.652.1 LOGIN

Procedimiento seguido por un usuario para establecer una sesión con un sistema de información.

2.652.2 (EN) LOGIN

1a. (I) An act by which a system entity establishes a session in which the entity can use system resources. (See: principal, session.)

1b. (I) An act by which a system user has its identity authenticated by the system. (See: principal, session.)

[RFC4949:2007]

2.653 MADUREZ

Acrónimos: CMM

2.653.1 MODELO DE MADUREZ DE LA CAPACIDAD (CMM)

(Mejora Continua del Servicio) El Modelo de Madurez de la Capacidad para el Software (también conocido como CMM y SW-CMM) es un modelo usado con el objeto de identificar las Mejores Prácticas para ayudar a incrementar la Madurez del Proceso. CMM fue desarrollado en el Software Engineering Institute (SEI) de la Carnegie Mellon University. En el año 2000, SW-CMM se actualizó como CMMI® (Modelo de Integración de Madurez de la Capacidad). El SEI ha dejado de mantener el modelo SW-CMM, sus métodos asociados de evaluación, y material de formación. [ITIL:2007]

2.653.2 (EN) CAPABILITY MATURITY MODEL (CMM)

(Continual Service Improvement) The Capability Maturity Model for Software (also known as the CMM and SW-CMM) is a model used to identify Best Practices to help increase Process Maturity. CMM was developed at the Software Engineering Institute (SEI) of Carnegie Mellon University. In 2000, the SW-CMM was upgraded to CMMI® (Capability Maturity Model Integration). The SEI no longer maintains the SW-CMM model, its associated appraisal methods, or training materials. [ITIL:2007]

2.653.3 (EN) CAPABILITY MATURITY MODEL FOR SOFTWARE (CMM OR SW-CMM)

A model for judging the maturity of the software processes of an organization and for identifying the key practices that are required to increase the maturity of these processes.

http://www.symantec.com/avcenter/refa.html

2.653.4 (FR) CAPABILITY MATURITY MODEL (CMM)

(Amélioration continuelle du service) Le modèle de maturité d'aptitude pour logiciel (aussi connu sous le nom de CMM et SW-CMM) est un modèle servant à identifier les meilleures pratiques,

afin d'améliorer le processus la maturité du processus. Le CMM a été développé par le SEI (Software Engineering Institute) de l'Université de Carnegie Mellon University. En 2000, le SW-CMM a fait l'objet d'une transition vers le modèle CMMI® (Capability Maturity Model Integration). Dès lors, le SEI a cessé de faire évoluer le modèle SW-CMM, ses méthodes d'évaluation associées, ni ses supports de formation. [ITIL:2007]

2.654 MAEC

2.654.1 MAEC

Lenguaje estandarizado para intercambiar información acerca de programas maliciosos. Se basa en un conjunto de atributos tales como el comportamiento, las técnicas que usa y los patrones de ataque.

http://maec.mitre.org/

2.654.2 (EN) MAEC

MAEC International in scope and free for public use, MAEC is a standardized language for encoding and communicating high-fidelity information about malware based upon attributes such as behaviors, artifacts, and attack patterns.

http://maec.mitre.org/

2.655 MANEJAR INFORMACIÓN

Ver:

- *Información*

2.655.1 MANEJAR INFORMACIÓN

Presentar, elaborar, almacenar, procesar, transportar o destruir información.

2.655.2 (EN) INFORMATION HANDLING

To show, ellaborate, store, process, transport, or destroy information.

2.656 MANIPULACIÓN

Ver:

- *Detección de manipulaciones*
- *Intrusión*

2.656.1 MANIPULAR

Intervenir con medios hábiles y, a veces, arteros, en la política, en el mercado, en la información, etc., con distorsión de la verdad o la justicia, y al servicio de intereses particulares.

http://www.getsafeonline.org/

2.656.2 (EN) TAMPERING

An intentional event resulting in modification of a system, its intended behavior, or data. [CNSSI_4009:2010]

2.656.3 (EN) TAMPER

(I) Make an unauthorized modification in a system that alters the system's functioning in a way that degrades the security services that the system was intended to provide. (See: QUADRANT. Compare: secondary definitions under "corruption" and "misuse".) [RFC4949:2007]

2.656.4 (EN) TAMPER-RESISTANT

(I) A characteristic of a system component that provides passive protection against an attack. (See: tamper.)

Usage: Usually involves physical means of protection.

[RFC4949:2007]

2.656.5 (EN) TAMPERING

(I) /threat action/ See: secondary definitions under "corruption" and "misuse". [RFC4949:2007]

2.656.6 (EN) TAMPER

To deliberately alter a system's logic, data, or control information to cause the system to perform unauthorized functions or services.

http://www.sans.org/security-resources/glossary-of-terms/

2.656.7 (EN) TAMPER RESPONSE

automatic action taken by a cryptographic module when tamper detection has occurred [ISO-19790:2006]

2.656.8 (EN) TAMPER RESPONSE

the automatic action taken by a cryptographic module when a tamper detection has occurred (the minimum response action is the zeroization of plaintext keys and CSPs). [FIPS-140-2:2001]

2.657 MARCAS DE AGUA

Ver:

- *Protección de derechos de autor*
- *Huella digital*

2.657.1 MARCAS DE AGUA DIGITALES

El watermarking o marca de agua digital es una técnica de ocultación de información que forma parte de las conocidas como esteganográficas. Su objetivo principal es poner de manifiesto el uso ilícito de un cierto servicio digital por parte de un usuario no autorizado.

Concretamente, esta técnica consiste en insertar un mensaje (oculto o no) en el interior de un objeto digital, como podrían ser imágenes, audio, vídeo, texto, software, etc. Dicho mensaje es un grupo de bits que contiene información sobre el autor o propietario intelectual del objeto digital tratado (copyright).

http://es.wikipedia.org/wiki/Marca_de_agua_digital

2.657.2 (EN) DIGITAL WATERMARKING

(I) Computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data -- text, graphics, images, video, or audio -- and for detecting or extracting the marks later. [RFC4949:2007]

2.658 MARCO DE CONTROL

2.658.1 MARCO DE CONTROL

Herramienta de gestión para los responsables de los procesos de negocio. Les permite delegar responsabilidades de forma ordenada y controlada.

2.658.2 MARCO DE CONTROL

Una herramienta para los dueños de los procesos de negocio que facilita la descarga de sus responsabilidades a través de la procuración de un modelo de control de soporte. [COBIT:2006]

2.658.3 (EN) CONTROL FRAMEWORK

A tool for business process owners that facilitates the discharge of their responsibilities through the provision of a supporting control model. [COBIT:2006]

2.659 MARS

Ver:

- *Cifrado en bloque*
- *Criptografía de clave secreta*
- *AES - Advanced Encryption Standard*
- http://en.wikipedia.org/wiki/MARS_%28cryptography%29

2.659.1 MARS

Algoritmo de cifra basado en un secreto compartido (clave). Cifra el texto en bloques de 128 bits. Utiliza claves de 128, 192 o 256 bits.

2.659.2 (EN) MARS

(O) A symmetric, 128-bit block cipher with variable key length (128 to 448 bits), developed by IBM as a candidate for the AES. [RFC4949:2007]

2.660 MÁSCARA DE UN SOLO USO

Ver:

- *Criptosistema de un solo uso*
- *Cifrado Vernam*

2.660.1 BLOC ALEATORIO

Bloc utilizado como serie cifrante que contiene caracteres o números aleatorios. Se producen sólo dos blocs, original y copia, con destino a cada extremo de un criptosistema. Cada hoja del bloc se usa una sola vez, destruyéndose a continuación. [Ribagorda:1997]

2.660.2 BLOC ALEATORIO

Procedimiento de cifrado manual presentado en forma de bloc y diseñado de manera que cada hoja, conteniendo caracteres aleatorios que sirven de clave para un mensaje, es destruida después de usada. [CESID:1997]

2.660.1 (EN) ONE-TIME PAD

Manual one-time cryptosystem produced in pad form. [CNSSI_4009:2010]

2.660.2 (EN) ONE-TIME PAD

1. (N) A manual encryption system in the form of a paper pad for one-time use.

2. (I) An encryption algorithm in which the key is a random sequence of symbols and each symbol is used for encryption only one time -- i.e., used to encrypt only one plaintext symbol and thus produce only one ciphertext symbol -- and a copy of the key is used similarly for decryption.

[RFC4949:2007]

2.660.3 (EN) PAD

In cryptography, the one-time pad is an encryption algorithm with text combined with a random key or "pad" that is as long as the plain-text and used only once. Additionally, if key is truly random, never reused, and, kept secret, the one-time pad is unbreakable.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.660.4 (EN) ONE-TIME PAD

A secret-key cipher in which the key is a truly random sequence of bits that is as long as the message itself, and encryption is performed by XORing the message with the key. This is theoretically unbreakable.

http://www.rsasecurity.com/rsalabs/faq

2.660.5 (EN) ONE-TIME PAD

In cryptography, a one-time pad is a system in which a private key generated randomly is used only once to encrypt a message that is then decrypted by the receiver using a matching one-time

pad and key. Messages encrypted with keys based on randomness have the advantage that there is theoretically no way to "break the code" by analyzing a succession of messages. Each encryption is unique and bears no relation to the next encryption so that some pattern can be detected. With a one-time pad, however, the decrypting party must have access to the same key used to encrypt the message and this raises the problem of how to get the key to the decrypting party safely or how to keep both keys secure. One-time pads have sometimes been used when the both parties started out at the same physical location and then separated, each with knowledge of the keys in the one-time pad. The key used in a one-time pad is called a secret key because if it is revealed, the messages encrypted with it can easily be deciphered. One-time pads figured prominently in secret message transmission and espionage before and during World War II and in the Cold War era. On the Internet, the difficulty of securely controlling secret keys led to the invention of public key cryptography.

http://searchsoftwarequality.techtarget.com/glossary/

2.660.6 (FR) PAD

En cryptographie, le pad ponctuel est un algorithme de cryptage avec un texte combiné à une clé aléatoire ou «pad»,aussi longue que le texte clair et utilisée une seule fois. En outre, si la clé est réellement aléatoire, jamais réutilisée et tenue secrète, le pad unique est inviolable.

http://fr.pcisecuritystandards.org/

2.661 MATERIAL DE CIFRA

Ver:

- *Cifrado*

2.661.1 MATERIAL DE CIFRA

Todo material incluyendo equipos, claves y documentos que contienen información de cifra y es esencial para el cifrado, descifrado o autenticación de las comunicaciones.

[CESID:1997]

2.661.2 (EN) CRYPTOMATERIAL

All material, including documents, devices or equipment that contains crypto information and is essential to the encryption, decryption or authentification of telecommunications.

2.662 MATRIZ DE RIESGOS

2.662.1 MATRIZ DE RIESGOS

Herramienta para presentar conjuntamente varios riesgos de forma que quede clara su importancia relativa. Por ejemplo, es frecuente emplear un diagrama bidimensional, donde un eje presenta la probabilidad y el otro las consecuencias.

2.662.2 (EN) RISK MATRIX:

tool for ranking and displaying components of risk in an array

Example: The security staff devised a risk matrix with the likelihoods of various threats to the subway system in the rows and corresponding consequences in the columns.

Annotation: A risk matrix is typically displayed in a graphical format to show the relationship between risk components.

DHS Risk Lexicon, September 2008

2.663 MAY

Ver:

- http://www.ietf.org/rfc/rfc2119
- *Obligatorio*

2.663.1 (EN) MAY

This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

2.663.2 (EN) MAY

within normative text, may indicates a course of action permissible within the limits of the document (ISO/IEC). [CC:2006]

2.664 MD2 - ALGORITMO RESUMEN

Acrónimos: MD2

Ver:

- *Función resumen*
- *Hash*
- http://www.ietf.org/rfc/rfc1319
- *MD4 - algoritmo resumen*
- *MD5 - algoritmo resumen*

2.664.1 MD2

(Acrónimo inglés de Message-Digest Algorithm 2, Algoritmo de Resumen del Mensaje 2) es una función de hash criptográfica desarrollada por Ronald Rivest en 1989. El algoritmo está optimizado para computadoras de 8 bits. El valor hash de cualquier mensaje se forma haciendo que el mensaje sea múltiplo de la longitud de bloque en el ordenador (128 bits o 16 bytes) y añadiéndole un checksum. Para el cálculo real, se utiliza un bloque auxiliar 48 bytes y una tabla de 256 bytes que contiene dígitos al azar del número pi.

http://es.wikipedia.org/wiki/MD2

2.664.2 (EN) MD2

(N) A cryptographic hash [R1319] that produces a 128-bit hash result, was designed by Ron Rivest, and is similar to MD4 and MD5 but slower. [RFC4949:2007]

2.664.3 (EN) MD2

Message Digest Algorithm 2 (MD2) is a cryptographic hash function developed by Ronald Rivest in 1989. The algorithm is optimized for 8-bit computers. MD2 is specified in RFC 1319. Although other algorithms have been proposed since, such as MD4, MD5 and SHA, even as of 2004 MD2 remains in use in public key infrastructures as part of certificates generated with MD2 and RSA.

http://en.wikipedia.org/wiki/MD2

2.665 MD4 - ALGORITMO RESUMEN

Acrónimos: MD4

Ver:

- *Función resumen*
- *Hash*
- http://www.ietf.org/rfc/rfc1320
- *MD5 - algoritmo resumen*

2.665.1 MD4 - ALGORITMO RESUMEN

Algoritmo diseñado por Ron Rivest (autor de la RC2, RC4 y RC5 y uno de los coautores del RSA). Producen un resume de 128 bits del mensaje.

El objetivo de diseño era la obtención de una función de resumen rápida, de simple diseño, compacta, optimizada para arquitecturas microprocesador (Intel en particular) y cuya seguridad fuera independiente de hipótesis no garantizadas (como la dificultad de factorización). Sin embargo, la sospecha de su posible vulnerabilidad ante ciertos ataques movió a su autor a modificar ligeramente su diseño para hacerlo más seguro, aunque ello supuso un algoritmo algo más lento. El resultado se conoce como MD5.

2.665.2 (EN) MD4

(N) A cryptographic hash [R1320] that produces a 128-bit hash result and was designed by Ron Rivest. (See: Derivation under "MD2", SHA-1.) [RFC4949:2007]

2.665.3 (EN) MD4

MD4 is a message digest algorithm (the fourth in a series) designed by Professor Ronald Rivest of MIT in 1990. It implements a cryptographic hash function for use in message integrity checks. The digest length is 128 bits. The algorithm has influenced later designs, such as the MD5, SHA and RIPEMD algorithms.

http://en.wikipedia.org/wiki/MD4

2.666 MD5 - ALGORITMO RESUMEN

Acrónimos: MD5

Ver:

- *Función resumen*
- *Hash*
- http://www.ietf.org/rfc/rfc1321
- *MD4 - algoritmo resumen*
- *SHA - Secure Hash Algorithm*

2.666.1 MD5 - ALGORITMO RESUMEN

Algoritmo diseñado por Ron Rivest (autor de la RC-2, RC-4 y RC-5 y uno de los coautores del RSA). Producen un resume de 128 bits del mensaje.

Diseñado como una mejora del algoritmo MD4, respecto del cual es más lento; pero más seguro.

Inspirador del algoritmo SHA1.

2.666.2 (EN) MD5

(N) A cryptographic hash [R1321] that produces a 128-bit hash result and was designed by Ron Rivest to be an improved version of MD4. (See: Derivation under "MD2".) [RFC4949:2007]

2.666.3 (EN) MD5

MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function with a 128-bit hash value. As an Internet standard (RFC 1321), MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files. An MD5 hash is typically a 32-character hexadecimal number. Recently, a number of projects have created MD5 "rainbow tables" which are easily accessible online, and can be used to reverse many MD5 strings into their original meanings.

http://en.wikipedia.org/wiki/MD5

2.667 MECANISMO CRÍTICO

2.667.1 MECANISMO CRÍTICO

Mecanismo de un sistema de tal relevancia que un fallo del mismo conlleva el fallo significativo del sistema.

2.667.2 (EN) CRITICAL MECHANISM

a mechanism within a Target of Evaluation whose failure would create a security weakness. [ITSEC:1991]

2.668 MECANISMO DE CONTROL DE ACCESO

Ver:

- *Control de acceso*

2.668.1 MECANISMO DE CONTROL DE ACCESO

Control de un sistema de información especializado en detectar los intentos de acceso, permitiendo el paso de las entidades autorizadas, y denegando el paso a todas las demás. Involucra medios técnicos y procedimientos operativos.

2.668.2 (EN) ACCESS CONTROL MECHANISM

Security safeguards (i.e., hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system. [CNSSI_4009:2010]

2.668.3 (EN) ACCESS CONTROL MECHANISM

Hardware or software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access in an automated system. [IRM-5239-8:1995]

2.669 MECANISMO DE SEGURIDAD

Ver:

- *Control*
- *Contra medida*
- *Salvaguarda*

2.669.1 MECANISMO DE SEGURIDAD

1. La lógica o el algoritmo que implementa una función relevante de seguridad sea en hardware o en software (ITSEC).

2. Dispositivo físico o lógico responsable de suministrar un servicio de seguridad o implementar un modelo de seguridad.

Es de destacar que un mismo modelo de seguridad puede instrumentarse en distintos mecanismos de seguridad por diferentes fabricantes.

[Ribagorda:1997]

2.669.2 MECANISMO ESPECÍFICO DE SEGURIDAD

Procedimiento que presta, de manera aislada o junto con otros, un determinado servicio de seguridad. [CESID:1997]

2.669.3 MECANISMO GENERAL DE SEGURIDAD

Es aquel mecanismo que, sin ser específico de ningún sistema de información, está relacionado con aspectos de la gestión de seguridad, variando su importancia en función del nivel de seguridad requerido por el sistema. [CESID:1997]

2.669.4 (EN) SECURITY MECHANISM

(I) A method or process (or a device incorporating it) that can be used in a system to implement a security service that is provided by or within the system. (See: Tutorial under "security policy". Compare: security doctrine.)

Usage: Usually understood to refer primarily to components of communication security, computer security, and emanation security.

[RFC4949:2007]

2.669.5 (EN) SECURITY MECHANISM

the logic or algorithm that implements a particular security enforcing or security relevenat funcion in hardware or software. [ITSEC:1991]

2.670 MEDIDA

Ver:

- *Métrica*
- *Indicador*

2.670.1 MEDIR

Comparar una cantidad con su respectiva unidad, con el fin de averiguar cuántas veces la segunda está contenida en la primera.

DRAE. Diccionario de la Lengua Española.

2.670.2 MEDIDA

variable a la que se le asigna un valor como resultado de una medición [ISO/IEC 15939:2007]

NOTA: El término "medidas" se utiliza para hacer referencia conjuntamente a medidas de base, medidas derivadas, e indicadores.

[UNE-ISO/IEC 27000:2014]

2.670.3 MEDICIÓN

proceso para determinar un valor

NOTA: En el contexto de seguridad de la información, el proceso para determinar un valor requiere información sobre la eficacia de un sistema de gestión de seguridad de la información y sus correspondientes controles utilizando un método de medición, una función de medición, un modelo analítico, y unos criterios de decisión

[UNE-ISO/IEC 27000:2014]

2.670.4 FUNCIÓN DE MEDICIÓN

algoritmo o cálculo realizado para combinar dos o más medidas básicas [ISO / IEC 15939:2007]

[UNE-ISO/IEC 27000:2014]

2.670.5 MÉTODO DE MEDICIÓN

secuencia lógica de operaciones, descritas genéricamente, utilizada en la cuantificación de un atributo con respecto a una escala especificada [ISO / IEC 15939:2007]

NOTA: El tipo de método de medición depende de la naturaleza de las operaciones utilizadas para cuantificar un atributo. Se pueden distinguir dos tipos:

- Subjetivo: la cuantificación se basa en el juicio humano;
- Objetivo: la cuantificación se basa en reglas numéricas.

[UNE-ISO/IEC 27000:2014]

2.670.6 RESULTADOS DE LAS MEDICIONES

uno o más indicadores y sus correspondientes interpretaciones que abordan una necesidad de información [UNE-ISO/IEC 27000:2014]

2.670.7 (EN) MEASURE

1. to find the size, quantity, etc. of sth in standard units

2. to be a particular size, length, amount, etc.

3. to judge the importance, value or effect of something.

Oxford Advanced Learner's Dictionary.

2.670.8 (EN) MEASUREMENT

1. the act or the process of finding the size, quantity or degree of something.

2. the size, length or amount of something

Oxford Advanced Learner's Dictionary.

2.670.9 (EN) MEASURE

variable to which a value is assigned as the result of measurement. [ISO-15939:2002]

2.670.10 (EN) MEASUREMENT

process of obtaining information about the effectiveness of ISMS, control objectives, and controls using a measurement method, a measurement function, an analytical model, and decision criteria.

NOTE. Based on the definition in ISO/Guide 99999 International Vocabulary of Basic and General Terms in Metrology, 2004-09-21.

2.670.11 (EN) MEASURE

variable to which a value is assigned as the result of measurement [ISO/IEC 15939:2007]

NOTE. The term “measures” is used to refer collectively to base measures, derived measures, and indicators.

[ISO/IEC 27000:2014]

2.670.12 (EN) MEASUREMENT

process to determine a value

NOTE: In the context of information security the process of determining a value requires information about the effectiveness of an information security management system and its associated controls using a measurement method, a measurement function, an analytical model, and decision criteria

[ISO/IEC 27000:2014]

2.670.13 (EN) MEASUREMENT FUNCTION

algorithm or calculation performed to combine two or more base measures [ISO/IEC 15939:2007]

[ISO/IEC 27000:2014]

2.670.14 (EN) MEASUREMENT METHOD

logical sequence of operations, described generically, used in quantifying an attribute with respect to a specified scale [ISO/IEC 15939:2007]

NOTE. The type of measurement method depends on the nature of the operations used to quantify an attribute. Two types can be distinguished:

- subjective: quantification involving human judgment;
- objective: quantification based on numerical rules.

[ISO/IEC 27000:2014]

2.670.15 (EN) MEASUREMENT RESULTS

one or more indicators and their associated interpretations that address an information need [ISO/IEC 27000:2014]

2.670.16 (EN) MEASUREMENT SCALE

ordered set of values, continuous or discrete, or a set of categories to which the attribute is mapped. [ISO-15939:2002]

2.670.17 (EN) UNIT OF MEASUREMENT

scalar quantity, defined and adopted by convention, with which other quantities of the same kind are compared in order to express their magnitudes.

ISO/Guide 99999 International Vocabulary of Basic and General Terms in Metrology, 2004-09-21.

2.670.18 (EN) PERFORMANCE MEASURE

A metric used to measure the extent to which a system, process, or activity fulfills its associated performance objective.

NASA Risk Management Handbook, NASA/SP-2011-3422, Version 1.0, November 2011

2.671 META-CHARACTER INJECTION

Ver:

- *Inyección SQL*
- *XPath injection*
- *Null injection*
- *LDAP injection*

2.671.1 META-CHARACTER INJECTION

Tipo de ataques contra servidores en red. Consisten en introducir caracteres extraños en las peticiones para abusar de programas poco robustos en el lado servidor. El ánimo es sortear los controles de datos de entrada para llegar a ejecutar tareas no permitidas.

2.671.2 (EN) META-CHARACTER INJECTION

An attack technique used to exploit web sites by sending in meta-characters, which have special meaning to a web application, as data input. Meta-characters are characters that have special meaning to programming languages, operating system commands, individual program procedures, database queries, etc. These special characters can adversely alter the behavior of a web application.

http://www.webappsec.org/projects/glossary/

2.672 MÉTODO ASIMÉTRICO DE AUTENTICACIÓN

Ver:

- *Método de autenticación*

2.672.1 MÉTODO ASIMÉTRICO DE AUTENTICACIÓN

Método para demostrar a una entidad que otra conoce un secreto, en el cual no toda la información necesaria para la autenticación es compartida por ambas entidades (ISO/IEC ISO-10181-2). [Ribagorda:1997]

2.672.2 (EN) ASYMMETRIC AUTHENTICATION METHOD

A method of authentication in which not all authentication information is shared by both entities. [ISO-10181-2:1996]

2.673 MÉTODO DE ATAQUE

Ver:

- *Ataque*

2.673.1 MÉTODO DE ATAQUE

Medio típico (acción o acontecimiento) con el que un elemento peligroso realiza sus ataques.

Ejemplos:

- robo de soportes informáticos o de documentos;
- alteración de programas;
- atentado contra la disponibilidad del personal;
- escucha pasiva;
- inundación;
- ...

[EBIOS:2005]

2.673.1 (EN) ATTACK METHOD

manner and means, including the weapon and delivery method, an adversary may use to cause harm on a target

Annotation: Attack method and attack mode are synonymous.

DHS Risk Lexicon, September 2008

2.673.2 (EN) ATTACK METHOD

Possible attack of a threat agent on assets.

Examples:

- a former member of the personnel with little technical ability but possibly strong motivation, deliberately damages the system software by introducing a virus, taking advantage of the ease of installing harmful programmes on the organisation's office network; this could affect, for example, the functions generating estimates or signature certificates;
- a cracker with a good level of expertise, standard equipment and paid for his actions, steals confidential files by remotely accessing the company's network;
- a developer or member of the personnel with a very good level of expertise in source codes but little ISS knowledge deliberately modifies the source code;
- a visitor steals equipment containing confidential information;
- etc.

[EBIOS:2005]

2.673.3 (EN) ATTACK METHOD

Standard means (action or event) by which a threat agent carries out an attack.

Examples:

- theft of media or documents;
- software entrapment;
- attack on availability of personnel;
- passive wiretapping;

- flood;
- etc.

[EBIOS:2005]

2.673.4 (FR) MÉTHODE D'ATTAQUE

Moyen type (action ou événement) pour un élément menaçant de réaliser une attaque.

Exemples:

- vol de supports ou de documents ;
- piégeage du logiciel ;
- atteinte à la disponibilité du personnel ;
- écoute passive ;
- crue ;
- ...

[EBIOS:2005]

2.674 MÉTODO DE AUTENTICACIÓN

Ver:

- *Método asimétrico de autenticación*
- *Método simétrico de autenticación*

2.674.1 MÉTODO DE AUTENTICACIÓN

Método empleado para demostrar la identidad de una entidad. La calidad o fortaleza del método está fuertemente ligada a la criptografía subyacente. En términos generales, se considera superior un método basado en criptografía asimétrica frente a métodos basados en secretos compartidos.

2.674.2 (EN) AUTHENTICATION METHOD

Method for demonstrating knowledge of a secret. The quality of the authentication method, its strength is determined by the cryptographic basis of the key distribution service on which it is based. A symmetric key based method, in which both entities share common authentication information, is considered to be a weaker method than an asymmetric key based method, in which not all the authentication information is shared by both entities.

http://www.opengroup.org/onlinepubs/8329799/glossary.htm

2.675 METODOLOGÍA COMÚN DE EVALUACIÓN

Acrónimos: CEM

Ver:

- *Criterios comunes*

2.675.1 METODOLOGÍA COMÚN DE EVALUACIÓN

Es la metodología que acompaña a los Criterios Comunes de evaluación. Describe las actividades que, como mínimo, debe ejecutar la entidad evaluadora durante una evaluación CC, utilizando los criterios y las evidencias requeridas en los CC.

2.675.2 (EN) COMMON EVALUATION METHODOLOGY

The Common Methodology for Information Technology Security Evaluation (CEM) is a companion document to the Common Criteria for Information Technology Security Evaluation (CC). The CEM describes the minimum actions to be performed by an evaluator in order to conduct a CC evaluation, using the criteria and evaluation evidence defined in the CC. [CEM:2006]

2.676 MÉTODO SIMÉTRICO DE AUTENTICACIÓN

Ver:

- *Método de autenticación*

2.676.1 MÉTODO SIMÉTRICO DE AUTENTICACIÓN

Método usado para demostrar a una entidad que otra conoce un secreto, en el cual no toda la información necesaria para la autenticación es compartida por ambas entidades (ISO/IEC ISO-10181-2). [Ribagorda:1997]

2.676.2 (EN) SYMMETRIC AUTHENTICATION METHOD

A method of authentication in which both entitles share common authentication information. [ISO-10181-2:1996]

2.677 MÉTRICA

Ver:

- *Medida*
- *Indicador*

2.677.1 MÉTRICA

Mecanismo normalizado para medir el grado de cumplimiento de un cierto objetivo.

2.677.2 MÉTRICA

Un estándar para medir el desempeño contra la meta. [COBIT:2006]

2.677.3 (EN) METRICS

A standard of measurement for performance against goal. [COBIT:2006]

2.677.4 (EN) METRICS

Tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. [NIST-SP800-55:2003]

2.677.5 (EN) IT SECURITY METRICS

Metrics based on IT security performance goals and objectives. [NIST-SP800-55:2003]

2.678 MISTY

Ver:

- *Cifrado en bloque*
- *Criptografía de clave secreta*
- https://www.cosic.esat.kuleuven.be/nessie/
- http://www.ietf.org/rfc/rfc2994
- *KASUMI*
- [ISO-18033-3:2005]
- http://en.wikipedia.org/wiki/MISTY1

2.678.1 MISTY

Algoritmo de cifra basado en un secreto compartido (clave). Cifra el texto en bloques de 64 bits. Utiliza claves de 128 bits.

2.678.2 (EN) MISTY

In cryptography, MISTY1 (or MISTY-1) is a block cipher designed in 1995 by Mitsuru Matsui and others for Mitsubishi Electric. MISTY1 is one of the selected algorithms in the European NESSIE project, and has been recommended for Japanese government use by the CRYPTREC project. KASUMI is a strengthened version of the MISTY1 cipher and has been adopted as the standard encryption algorithm for European mobile phones. In 2005, KASUMI was broken, but there is no practical attack against it yet; see the article for more details.

http://en.wikipedia.org/wiki/MISTY1

2.679 MOCHILA

Ver:

- *Token*

2.679.1 MOCHILA

Pequeño elemento hardware que se debe conectar a un equipo para habilitar las funciones de una cierta aplicación. La mochila actúa como autenticador del derecho a usar la aplicación.

2.679.2 (EN) DONGLE

(I) A portable, physical, usually electronic device that is required to be attached to a computer to enable a particular software program to run. (See: token.) [RFC4949:2007]

2.679.3 (EN) DONGLE

A dongle (pronounced DONG-uhl) is a mechanism for ensuring that only authorized users can copy or use specific software applications, especially very expensive programs. Common mechanisms include a hardware key that plugs into a parallel or serial port on a computer and that a software application accesses for verification before continuing to run; special key diskettes accessed in a similar manner; and registration numbers that are loaded into some form of ROM (read-only memory) at the factory or during system setup.

If more than one application requires a dongle, multiple dongles can be daisy-chained together from the same port.

http://searchsoftwarequality.techtarget.com/glossary/

2.680 MODELO DE BELL-LAPADULA

Ver:

- *Modelo de seguridad*
- *Control de acceso*
- http://en.wikipedia.org/wiki/Bell-LaPadula_model
- [BLP:1976]
- *Modelo de Biba*
- *Modelo de Brewer-Nash*

2.680.1 MODELO DE BELL-LAPADULA

Modelo de seguridad que controla el flujo de información en un sistema estableciendo unas precisas reglas de control de acceso. Las entidades se dividen en objetos y sujetos. Para determinar si un sujeto puede acceder (para leer o escribir) a un objeto se comparan la habilitación del primero con la clasificación de sensibilidad del segundo.

Este modelo preserva exclusivamente la confidencialidad de la información.

[Ribagorda:1997]

2.680.2 (EN) BELL-LAPADULA MODEL

(N) A formal, mathematical, state-transition model of confidentiality policy for multilevel-secure computer systems [Bell]. (Compare: Biba model, Brewer-Nash model.) [RFC4949:2007]

2.680.3 (EN) BELL-LAPADULA MODEL

A formal state transition model of computer security policy that describes a set of access control rules. In this formal model, the entities in a computer system are divided into abstract sets of subjects and objects. The notion of a secure state is defined and it is proven that each state transition preserves security by moving from secure state to secure state; thus, inductively proving that the system is secure. A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a specific security policy. In order to determine whether or not a specific access mode is allowed, the clearance of a subject is compared to the classification of the object and a determination is made as to whether the subject is authorized for the specific access mode. The clearance/classification scheme is expressed in terms of a lattice.

See also: Lattice, Simple Security Property, *-Property.

[TCSEC:1985]

2.681 MODELO DE BIBA

Ver:

- *Modelo de seguridad*
- *Control de acceso*
- *Modelo de Bell-LaPadula*
- *Modelo de Brewer-Nash*

2.681.1 (EN) BIBA MODEL

(N) A formal, mathematical, state-transition model of integrity policy for multilevel-secure computer systems [Biba]. (See: source integrity. Compare: Bell-LaPadula model.) [RFC4949:2007]

2.682 MODELO DE BREWER-NASH

Ver:

- *Modelo de seguridad*
- *Política tipo muralla china*
- *Modelo de Bell-LaPadula*
- *Modelo de Biba*

2.682.1 (EN) BREWER-NASH MODEL

(N) A security model [BN89] to enforce the Chinese wall policy. (Compare: Bell-LaPadula model, Clark-Wilson model.) [RFC4949:2007]

2.683 MODELO DE SEGURIDAD

Ver:

- *Modelo de Bell-LaPadula*
- *Modelo de Biba*
- *Modelo de Brewer-Nash*

2.683.1 MODELO DE SEGURIDAD

Expresión formal, matemática, de una política de seguridad.

Los modelos de seguridad se materializan en mecanismos de seguridad.

En el ITSEC se denomina: Modelo Formal de Política de Seguridad (Formal model of security policy)

[Ribagorda:1997]

2.683.2 MODELO DE SEGURIDAD

Requisitos de seguridad de un sistema de información o de sus elementos. Incluye una representación del estado inicial del sistema de información, el modo en el que el sistema cambia de estado y una definición de un estado seguro del sistema. Puede ser:

- Formal: Cuando se expresa de modo matemático, mediante conjuntos de objetos abstractos con operaciones definidas para las que se cumplen determinadas leyes.
- Informal: Cuando la especificación del modelo se efectúa con un lenguaje natural, en lugar de una notación que requiera especiales restricciones o convenciones.
- Semiformal: Cuando la especificación del modelo requiere el uso de alguna notación restringida a la que se hace referencia de manera informal.

[CESID:1997]

2.683.3 (EN) SECURITY MODEL

(I) A schematic description of a set of entities and relationships by which a specified set of security services are provided by or within a system. Example: Bell-LaPadula model, OSIRM. (See: Tutorial under "security policy".) [RFC4949:2007]

2.684 MÓDEM DE RETROLLAMADA

2.684.1 MÓDEM DE RETROLLAMADA

Módem que almacena una lista de usuarios habilitados junto con sus respectivos números telefónicos desde los que tienen autorizado el acceso al sistema informático. Cuando uno de estos usuarios intenta acceder al sistema introduce su identificación y se desconecta para que sea el módem el que, seguidamente, inicie la comunicación marcando el número telefónico correspondiente al usuario identificado. [Ribagorda:1997]

2.684.1 (EN) CALL BACK

Procedure for identifying and authenticating a remote IS terminal, whereby the host system disconnects the terminal and reestablishes contact. [CNSSI_4009:2010]

2.684.2 (EN) CALL BACK

(I) An authentication technique for terminals that remotely access a computer via telephone lines; the host system disconnects the caller and then reconnects on a telephone number that was previously authorized for that terminal. [RFC4949:2007]

2.684.3 (EN) CALL-BACK

a mechanism to place a call to a pre-defined or proposed location (and address) after receiving valid ID parameters. [ISO-18028-4:2005]

2.685 MODO COMPARTIMENTADO

Ver:

- *Modo de operación (2)*
- *Compartimento*

2.685.1 MODO COMPARTIMENTADO

Modo de operación en el cual el sistema recoge en compartimentos estancos conjuntos de información con un requisito suficiente o superior de habilitación y necesidad de conocer.

2.685.2 COMPARTIMENTADO

es aquel [modo de operación] en el que todo el personal con acceso al Sistema está autorizado para acceder al grado más elevado de clasificación de la información manejada por el Sistema, pero no todos los individuos con acceso al sistema tienen una autorización formal para acceder a toda la información manejada en el Sistema. Autorización formal implica una gestión centralizada formal para el control de accesos a diferencia de los criterios individuales de concesión. [CCN-STIC-001:2006]

2.685.1 (EN) COMPARTMENTED MODE

Mode of operation wherein each user with direct or indirect access to a system, its peripherals, remote terminals, or remote hosts has all of the following: 1) valid security clearance for the most restricted information processed in the system, 2) formal access approval and signed nondisclosure agreements for that information which a user is to have access, and 3) valid need-to-know for information which a user is to have access. [CNSSI_4009:2010]

2.685.2 (EN) COMPARTMENTED SECURITY MODE

(N) A mode of system operation wherein all users having access to the system have the necessary security clearance for the single, hierarchical classification level of all data handled by the system, but some users do not have the clearance for a non- hierarchical category of some data handled by the system. (See: category, /system operation/ under "mode", protection level, security clearance.) [RFC4949:2007]

2.686 MODO DE CIFRADO

Ver:

- *Cifrado*
- *ECB - Electronic codebook mode*
- *CBC - Cipher block chaining*
- *CFB - Cipher feedback mode*
- *OFB - Output feedback mode*
- *CTR - Cifrado modo con contador*

2.686.1 PROCEDIMIENTO DE CIFRADO

Designación que recibe cada uno de los modos específicos de cifrado dentro de un determinado método. [CESID:1997]

2.686.2 (EN) OPERATING MODE

With respect to block ciphers, a way to handle messages which are larger than the defined block size. Usually this means one of the four block cipher "applications" defined for use with DES:

- ECB or Electronic Codebook;
- CBC or Cipher Block Chaining;
- CFB or Ciphertext FeedBack; and
- OFB or Output FeedBack.

http://www.ciphersbyritter.com/GLOSSARY.HTM

2.687 MODO DEDICADO

Ver:

- *Modo de operación (2)*

2.687.1 DEDICADO

es aquel [modo seguro de operación] en el que todo el personal con acceso al Sistema está autorizado para acceder al grado más elevado de clasificación de la información manejada en el Sistema, y además posee la misma necesidad de conocer. La separación de los datos no es un requisito del Sistema. [CCN-STIC-001:2006]

2.687.2 MODO DEDICADO

El sistema se emplea por personal habilitado con el mayor grado de clasificación y teniendo en común la misma "necesidad de conocer" para toda la información contenida en el sistema; la separación de los datos no es un requisito del sistema. [CCN-STIC-103:2006]

2.687.1 (EN) DEDICATED MODE

Information systems security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following: 1) valid security clearance for all information within the system, 2) formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs), and 3) valid need-to-know for all information contained within the information system. When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time. [CNSSI_4009:2010]

2.687.2 (EN) DEDICATED SECURITY MODE

(I) A mode of system operation wherein all users having access to the system possess, for all data handled by the system, both (a) all necessary authorizations (i.e., security clearance and formal access approval) and (b) a need-to-know. (See: /system operation/ under "mode", formal access approval, need to know, protection level, security clearance.) [RFC4949:2007]

2.688 MODO DE OPERACIÓN (1)

Ver:

- *Cifrado en bloque*
- [FIPS-81:1980]
- *ECB - Electronic codebook mode*
- *CBC - Cipher block chaining*
- *CFB - Cipher feedback mode*
- *OFB - Output feedback mode*
- *CTR - Cifrado modo con contador*
- *CCM - Counter with Cipher Block Chaining-Message Authentication Code*
- *GCM - Galois / Counter Mode*

2.688.1 MODO DE OPERACIÓN (1)

Adaptación de un cifrador de bloque para una aplicación o servicio concreto.

2.688.2 (EN) MODE OF OPERATION

1. (I) /cryptographic operation/ A technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application, such as applying a block cipher to a sequence of data blocks or a data stream. (See: CBC, CCM, CMAC, CFB, CTR, ECB, OFB.) [RFC4949:2007]

2.688.3 (EN) MODES OF OPERATION

A mode of operation, or mode, for short, is an algorithm that features the use of a symmetric key block cipher algorithm to provide an information service, such as confidentiality or authentication.

http://csrc.nist.gov/CryptoToolkit/modes/

2.689 MODO DE OPERACIÓN (2)

Ver:

- *Información clasificada*
- *Modo dedicado*
- *Modo unificado al nivel superior*
- *Modo compartimentado*
- *Modo particionado*
- *Modo multinivel*

2.689.1 MODOS SEGUROS DE OPERACIÓN

Para aquellos sistemas donde se almacena, procesa o transmite información clasificada se distinguen los siguientes modos seguros de operación:

1 - Dedicado

El sistema se emplea por personal habilitado con el mayor grado de clasificación y teniendo en común la misma "necesidad de conocer" para toda la información contenida en el sistema; la separación de los datos no es un requisito del sistema.

2 - Unificado al nivel superior

El sistema maneja información con diferentes grados de clasificación. Permite el acceso selectivo y simultáneo a dicha información al personal habilitado con el mayor grado de clasificación pero con distinta "necesidad de conocer". El sistema realiza de manera fiable la separación de los datos y dispone de control de acceso selectivo a la información conforme a la diferente "necesidad de conocer".

3 – Multinivel

El sistema maneja información con diferentes grados de clasificación. Permite el acceso selectivo y simultáneo a dicha información al personal habilitado con diferentes grados de clasificación y "necesidad de conocer". El sistema realiza de manera fiable la completa separación de los datos y el control de acceso selectivo.

Para los tres modos seguros de operación, los controles físicos, del personal y de los procedimientos deben cumplir los requisitos impuestos por el mayor grado de clasificación de la información residente.

[CCN-STIC-103:2006]

2.689.2 MODO DE OPERACIÓN DE SEGURIDAD

La determinación del modo de explotación de seguridad del sistema consiste en indicar cómo el sistema permite a los usuarios de diferentes categorías procesar, transmitir o conservar datos en mayor o menor medida sensibles. Permite tomar conciencia de la problemática de la seguridad general porque el modo de explotación de seguridad define el contexto de gestión de la información de un sistema de información.

En líneas generales, el modo de explotación de seguridad del sistema pertenece a una de las siguientes categorías:

- Categoría 1: modo de explotación exclusivo
  Todas las personas que tienen acceso al sistema están autorizadas para el más alto nivel de procesamiento y tienen idéntica (o equivalente) necesidad de conocer toda la información procesada, almacenada o transmitida por el sistema.
- Categoría 2: modo de explotación dominante
  Todas las personas que tienen acceso al sistema están autorizadas para el más alto nivel de procesamiento, pero no todas tienen idéntica (o equivalente) necesidad de conocer toda la información procesada, almacenada o transmitida por el sistema.
- Categoría 3: modo de explotación multinivel
  Las personas que tienen acceso al sistema no están todas habilitadas para el más alto nivel de procesamiento y no tienen todas idéntica (o equivalente) necesidad de conocer toda la información procesada, almacenada o transmitida por el sistema.

Para elegir el modo de explotación de seguridad del sistema, es importante saber si existe o debe existir:

- una clasificación jerárquica de las informaciones (por ej.: confidencial, secreto...) y/o por compartimiento (médico, sociedad, nuclear...),
- categorías de usuarios,
- una noción de la necesidad de conocer, modificar o disponer de la información...

La elección del modo de explotación de seguridad puede reconsiderarse teniendo en cuenta los riesgos identificados en el transcurso de las etapas siguientes. Sin embargo, es importante plantearse este aspecto lo antes posible porque su implementación tiene importantes consecuencias en el diseño del SI y de la SSI.

[EBIOS:2005]

2.689.1 (EN) MODE OF OPERATION

Description of the conditions under which an information system operates based on the sensitivity of information processed and the clearance levels, formal access approvals, and need-to-know of its users. Four modes of operation are authorized for processing or transmitting information: dedicated mode, system high mode, compartmented/partitioned mode, and multilevel mode. [CNSSI_4009:2010]

2.689.2 (EN) SECURITY MODES

The mode of operation is determined by:

- The type of users who will be directly or indirectly accessing the system.
- The type of data, including classification levels, compartments, and categories, that are processed on the system.
- The type of levels of users, their need to know, and formal access approvals that the users will have.

All users must have ...

mode	signed NDA for	proper clearance for	formal access approval for	a valid need-to-know for
Dedicated	ALL	ALL	ALL	ALL
System high	ALL	ALL	ALL	SOME
Compartmented	ALL	ALL	SOME	SOME
Multilevel	ALL	SOME	SOME	SOME

http://en.wikipedia.org/wiki/Security_modes

2.689.3 (EN) MODE OF OPERATION

2. (I) /system operation/ A type of security policy that states the range of classification levels of information that a system is permitted to handle and the range of clearances and authorizations of users who are permitted to access the system. (See: compartmented security mode, controlled security mode, dedicated security mode, multilevel security mode, partitioned security mode, system-high security mode. Compare: protection level.) [RFC4949:2007]

2.689.4 (EN) MODES OF OPERATION

A description of the conditions under which an IS functions, based on the sensitivity of data processed and the clearance levels and authorizations of the users. Four modes of operation are authorized:

(1a) An IS is operating in the **dedicated mode** when the system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specific period of time.

(1b) An IS is operating in the **dedicated mode** when each user with direct or indirect individual access to the IS, its peripherals, its remote terminals, or its remote hosts has all of the following:

- a valid personnel clearance for all information on the system,
- formal access approval for, and signed nondisclosure agreements for, all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs), and
- a valid need-to-know for all information contained within the system.

(2a) An IS is operating in the **system-high m**ode when each user with direct or indirect access to the IS, its peripherals, remote terminals, or remote hosts has all of the following:

- a valid personnel clearance for all information on the IS,
- formal access approval for, and signed nondisclosure agreements for, all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs), and
- a valid need-to-know for some of the information contained within the IS.

(2b) An IS is operating in the **system-high mode** when the system hardware and software are trusted only to provide discretionary protection between users. In this mode, the entire system, to include all components electrically and/or physically connected, must operate with security measures commensurate with the highest classification and sensitivity of the information being processed and/or stored. All system users in this environment must possess clearances and authorization for all information contained in the system. All system output must be clearly marked with the highest classification and all system caveats until the information has been reviewed manually by an authorized individual to ensure appropriate classifications and that caveats have been affixed.

(3) An IS is operating in the **compartmented mode** when each user with direct or indirect access to the IS, its peripherals, remote terminals, or remote hosts has all of the following:

- a valid personnel clearance for the most restricted information processed in the IS,
- formal access approval for, and signed nondisclosure agreements for, that information to which he or she is to have access, and
- a valid need-to-know for that information to which he or she is to have access.

(4) An IS is operating in the **multilevel mode** when all the following statements are satisfied concerning users with direct or indirect access to the IS, its peripherals, remote terminals, or remote hosts:

- some do not have a valid personnel clearance for all the information processed in the IS,
- all have the proper clearance and have the appropriate formal access approval for that information to which they are to have access, and
- all have a valid need-to-know for that information to which they are to have access.

http://www.garlic.com/~lynn/secgloss.htm

2.689.5 (EN) SECURITY OPERATING MODE.

Determining the security operating mode of the system consists in indicating how the system enables various categories of users to process, send or store various types of sensitive information. This allows the general security issues to be understood since the security operating mode defines the information management context of an information system.The security operating mode of the system usually belongs to one of the following categories:

- Category 1: exclusive operating mode
  Everyone accessing the system has the highest level of authorisation and an identical need to know (or equivalent) with regard to all the information processed, stored or sent by the system.
- Category 2: dominant operating mode
  Everyone accessing the system has the highest level of authorisation but they do not have an identical need to know (or equivalent) with regard to the information processed, stored or sent by the system.
- Category 3: multilevel operating mode
  Not everyone accessing the system has the highest level of authorisation and they do not all have an identical need to know (or equivalent) with regard to the information processed, stored or sent by the system.

To choose the security operating mode of the system, it is important to know if the following exist or should exist:

- a prioritised information classification structure (e.g. confidential, secret, etc.) and/or compartmentalised structure (medical, company, nuclear, etc.),
- user categories,
- a notion of need to know, need to modify, need to have, etc.

The choice of security operating mode can be reassessed once the risks have been identified during the next stages. However, it is important to consider this aspect as early as possible, as its implementation has major consequences on the IS and ISS architecture.

[EBIOS:2005]

2.689.6 (FR) MODE D'EXPLOITATION DE SÉCURITÉ

La détermination du mode d'exploitation de sécurité du système consiste à indiquer comment le système permet aux utilisateurs de catégories différentes de traiter, transmettre ou conserver des informations de sensibilités différentes. Elle permet de prendre connaissance de la problématique sécuritaire générale car le mode d'exploitation de sécurité définit le contexte de gestion de l'information d'un système d'information.

De manière générale, le mode d'exploitation de sécurité du système appartient à l'une des catégories suivantes:

- Catégorie 1: mode d'exploitation exclusif
  Toutes les personnes ayant accès au système sont habilitées au plus haut niveau de classification et elles possèdent un besoin d'en connaître (ou équivalent) identique pour toutes les informations traitées, stockées ou transmises par le système.
- Catégorie 2: mode d'exploitation dominant
  Toutes les personnes ayant accès au système sont habilitées au plus haut niveau de

classification mais elles n'ont pas toutes un besoin d'en connaître (ou équivalent) identique pour les informations traitées, stockées ou transmises par le système.

- Catégorie 3: mode d'exploitation multiniveaux
  Les personnes ayant accès au système ne sont pas toutes habilitées au plus haut niveau de classification et elles n'ont pas toutes un besoin d'en connaître (ou équivalent) identique pour les informations traitées, stockées ou transmises par le système.

Pour choisir le mode d'exploitation de sécurité du système, il est important de savoir s'il existe ou doit exister:

- une classification des informations hiérarchique (ex: confidentiel, secret...) et/ou par compartiment (médical, société, nucléaire...),
- des catégories d'utilisateurs,
- une notion de besoin d'en connaître, d'en modifier, d'en disposer...

Le choix du mode d'exploitation de sécurité peut être reconsidéré au vu des risques identifiés lors des étapes suivantes. Il est cependant important de s'interroger sur cet aspect au plus tôt car sa mise en oeuvre a de fortes conséquences sur l'architecture du SI et de la SSI.

[EBIOS:2005]

2.690 MODO MULTINIVEL

Ver:

- *Modo de operación (2)*

2.690.1 MULTINIVEL

es aquel [modo de operación] en el que un Sistema maneja información con diferentes grados de clasificación. Permite el acceso selectivo y simultáneo a dicha información al personal autorizado con diferentes grados de clasificación y distintas necesidades de conocer. El Sistema realiza de manera fiable la completa separación de los datos y el control del acceso selectivo. [CCN-STIC-001:2006]

2.690.2 MULTINIVEL

El sistema maneja información con diferentes grados de clasificación. Permite el acceso selectivo y simultáneo a dicha información al personal habilitado con diferentes grados de clasificación y "necesidad de conocer". El sistema realiza de manera fiable la completa separación de los datos y el control de acceso selectivo. [CCN-STIC-103:2006]

2.690.1 (EN) MULTILEVEL MODE

Mode of operation wherein all the following statements are satisfied concerning the users who have direct or indirect access to the system, its peripherals, remote terminals, or remote hosts: 1) some users do not have a valid security clearance for all the information processed in the information system; 2) all users have the proper security clearance and appropriate formal access approval for that information to which they have access; and 3) all users have a valid need-to-know only for information to which they have access. [CNSSI_4009:2010]

2.690.2 (EN) MULTILEVEL SECURITY MODE

1. (N) A mode of system operation wherein (a) two or more security levels of information are allowed to be to be handled concurrently within the same system when some users having access to the system have neither a security clearance nor need-to-know for some of the data handled by the system and (b) separation of the users and the classified material on the basis, respectively, of clearance and classification level are dependent on operating system control. (See: /system operation/ under "mode", need to know, protection level, security clearance. Compare: controlled mode.)

Usage: Usually abbreviated as "multilevel mode". This term was defined in U.S. Government policy regarding system accreditation, but the term is also used outside the Government.

2. (O) A mode of system operation in which all three of the following statements are true: (a) Some authorized users do not have a security clearance for all the information handled in the system. (b) All authorized users have the proper security clearance and appropriate specific access approval for the information to which they have access. (c) All authorized users have a need-to-know only for information to which they have access. [C4009] (See: formal access approval, protection level.)

[RFC4949:2007]

2.691 MODO PARTICIONADO

Ver:

- *Modo de operación (2)*

2.691.1 MODO PARTICIONADO

Modo de operación en el que todos los usuarios con acceso al sistema disfrutan de la habilitación necesaria, aunque algunos usuarios pudieran carecer de una autorización formal o de la necesidad de conocer todos los datos que quedan accesibles.

2.691.1 (EN) PARTITIONED SECURITY MODE

Information systems security mode of operation wherein all personnel have the clearance, but not necessarily formal access approval and need-to-know, for all information handled by an information system. [CNSSI_4009:2010]

2.691.2 (EN) PARTITIONED SECURITY MODE

(N) A mode of system operation wherein all users having access to the system have the necessary security clearances for all data handled by the system, but some users might not have either formal access approval or need-to-know for all the data. (See: /system operation/ under "mode", formal access approval, need to know, protection level, security clearance.) [RFC4949:2007]

2.692 MODO UNIFICADO AL NIVEL SUPERIOR

Ver:

- *Modo de operación (2)*

2.692.1 UNIFICADO AL NIVEL SUPERIOR

es aquel [modo de operación] en el que todo el personal con acceso al Sistema está autorizado para acceder al grado más elevado de clasificación de la información manejada por el Sistema, pero no tiene la misma necesidad de conocer. Dicha necesidad de conocer se establece mediante procesos informales, o a nivel individual. El Sistema realiza de manera fiable la separación de los datos y dispone de control de acceso selectivo a la información conforme a la diferente "necesidad de conocer". [CCN-STIC-001:2006]

2.692.2 UNIFICADO AL NIVEL SUPERIOR

El sistema maneja información con diferentes grados de clasificación. Permite el acceso selectivo y simultáneo a dicha información al personal habilitado con el mayor grado de clasificación pero con distinta "necesidad de conocer". El sistema realiza de manera fiable la separación de los datos y dispone de control de acceso selectivo a la información conforme a la diferente "necesidad de conocer". [CCN-STIC-103:2006]

2.692.1 (EN) SYSTEM HIGH MODE

Information systems security mode of operation wherein each user, with direct or indirect access to the information system, its peripherals, remote terminals, or remote hosts, has all of the following: 1) valid security clearance for all information within an information system; 2) formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, sub compartments and/or special access programs); and 3) valid need-to- know for some of the information contained within the information system. [CNSSI_4009:2010]

2.692.2 (EN) SYSTEM-HIGH SECURITY MODE

(I) A mode of system operation wherein all users having access to the system possess all necessary authorizations (both security clearance and formal access approval) for all data handled by the system, but some users might not have need-to-know for all the data. (See: /system operation/ under "mode", formal access approval, protection level, security clearance.) [RFC4949:2007]

2.693 MÓDULO CRIPTOGRÁFICO

Ver:

- *Equipo criptográfico*
- *Dispositivo criptográfico*

2.693.1 MÓDULO CRIPTO

Parte de un equipo de cifra electrónico, en general con protecciones físicas y lógicas, que contiene la implementación del algoritmo y/o las memorias de claves. [CESID:1997]

2.693.2 (EN) CRYPTOGRAPHIC MODULE

(I) A set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the module's "cryptographic boundary", which is an explicitly defined contiguous perimeter that establishes the physical bounds of the module. [FP140] [RFC4949:2007]

2.693.3 (EN) CRYPTOGRAPHIC MODULE

The set of hardware, software, and/or firmware that implements Approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. [NIST-SP800-57:2007]

2.693.4 (EN) CRYPTOGRAPHIC MODULE

The set of hardware, software, and/or firmware that implements security functions and are contained within the cryptographic boundary.

cryptographic boundary. an explicitly defined continuous perimeter that establishes the physical and/or logical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.

[ISO-19790:2006]

2.693.5 (EN) CRYPTOGRAPHIC MODULE

the set of hardware, software, and/or firmware that implements Approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. [FIPS-140-2:2001]

2.694 MÓDULO DE IDENTIFICACIÓN DE USUARIO

Acrónimos: SIM

Ver:

- *Comp 128-1*
- *A5 - Cifrado de voz GSM*

2.694.1 MÓDULO DE IDENTIFICACIÓN DE USUARIO

Tarjeta inteligente instalada en los teléfonos móviles que utilizan redes GSM. Proporciona servicios de autenticación y cifrado.

2.694.2 (EN) SUBSCRIBER IDENTIFICATION MODULE

Smart card in GSM phones. It provides authentication and encryption services.

2.695 MONITOR DE REFERENCIA

Ver:

- *Criterios comunes*

2.695.1 MONITOR DE REFERENCIA

Concepto de máquina abstracta que aplica las políticas de control de acceso del TOE. [CC:2006]

2.695.2 (EN) REFERENCE MONITOR

(I) "An access control concept that refers to an abstract machine that mediates all accesses to objects by subjects." [NCS04] (See: security kernel.) [RFC4949:2007]

2.695.3 (EN) REFERENCE MONITOR

The security engineering term for IT functionality that (1) controls all access, (2) cannot be bypassed, (3) is tamper-resistant, and (4) provides confidence that the other three items are true. [NIST-SP800-33:2001]

2.695.4 (EN) REFERENCE MONITOR CONCEPT

An access control concept that refers to an abstract machine that mediates all accesses to objects by subjects. [TCSEC:1985]

2.696 MONITORIZACIÓN DE LA RED

Ver:

- *Sniffer*

2.696.1 MONITORIZACIÓN DE LA RED

Ataque de interceptación en red. El atacante accede a los paquetes que circulan por la red y los analiza para descubrir contraseñas de los usuarios.

2.696.2 (EN) NETWORK MONITORING

On some systems all messages may be read by all systems on the network. Tools are available to enable network cards to be programmed to monitor and log messages on the network including passwords. Thus any user with access to the network could potentially collect passwords for subsequent unauthorised access.

2.697 MONITORIZACIÓN DEL TECLADO

Ver:

- *Captura del teclado*

2.697.1 MONITORIZACIÓN DEL TECLADO

Dícese cuando el atacante observa el proceso de introducción de una clave por parte de un usuario legítimo. De esta observación puede inferir el conocimiento de la clave para su propio beneficio.

También se dice de programas espía que monitorizan la entrada de claves en el sistema.

2.697.2 (EN) KEY STROKE MONITORING

In the simplest case this involves covert observation by the potential attacker of authorised users' key strokes as they type in passwords. Alternatively, a malicious software (e.g. Trojan Horse, Spyware) or hardware capture device is installed on a personal computer and monitors and records key strokes as they are entered. Finally (and much less likely), compromising emissions may be picked up from the screen or from implanted keyboard bugs.

2.698 MUST

Ver:

- http://www.ietf.org/rfc/rfc2119

2.698.1 (EN) MUST

This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

2.699 MUST_NOT

Ver:

- http://www.ietf.org/rfc/rfc2119

2.699.1 (EN) MUST NOT

This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

2.700 NECESIDAD DE CONOCER

Ver:

- *Privilegio mínimo*
- http://en.wikipedia.org/wiki/Need_to_know

2.700.1 NECESIDAD DE CONOCER

Determinación positiva por la que se confirma que un posible destinatario requiere el acceso a, el conocimiento de, o la posesión de la información para desempeñar servicios, tareas o cometidos oficiales.

2.700.2 NECESIDAD DE CONOCER

Principio por el cual se toma la determinación positiva de que un receptor tenga necesidad de acceder a, conocimiento de, o posesión de información para llevar a cabo tareas o servicios oficiales. [CCN-STIC-202:2006]

2.700.3 NECESIDAD DE CONOCER

Es término sinónimo de "mínimo privilegio". [Ribagorda:1997]

2.700.4 NECESIDAD DE CONOCER

Principio de seguridad por el que, para que una persona pueda acceder a una determinada información clasificada, es necesario que ésta sea precisa para poder desarrollar su trabajo, no siendo suficiente su puesto o rango. [CESID:1997]

2.700.1 (EN) NEED-TO-KNOW

A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more. The terms 'need-to know" and "least privilege" express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes. [CNSSI_4009:2010]

2.700.1 (EN) NEED TO KNOW DETERMINATION

Decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties. [CNSSI_4009:2010]

2.700.2 (EN) NEED TO KNOW, NEED-TO-KNOW

(I) The necessity for access to, knowledge of, or possession of specific information required to carry out official duties. [RFC4949:2007]

2.700.3 (EN) NEED-TO-KNOW

A determination made by an authorized holder of classified information that a prospective recipient has a requirement for access to, knowledge, or possession of the classified information to perform tasks or services essential to the fulfillment of a classified contract or program. [DoD 5220:2006]

2.700.4 (EN) NEET-TO-KNOW

The principle according to which a positive determination is made that a prospective recipient has a requirement for access to, knowledge of, or possession of information in order to perform official tasks or services. [CCN-STIC-401:2007]

2.701 NEGOCIACIÓN DE CLAVES

Ver:

- *Clave*
- *Clave criptográfica*
- *Establecimiento de claves*
- *Secreto compartido*

2.701.1 ACUERDO DE CLAVE

Método para negociar un valor de clave en línea sin transferir la clave, incluso en forma criptada, por ejemplo, la técnica de Diffie-Hellman (para más información sobre los mecanismos de acuerdos de clave, véase ISO/IEC ISO-11770-1). [X.509:2005]

2.701.2 NEGOCIACIÓN DE CLAVES

Acuerdo entre entidades para establecer una clave secreta, tal que ninguna de ellas pueda predeterminar el valor de la citada clave (ISO/IEC ISO-11770-1).

Habitualmente se realiza mediante algún protocolo criptográfico, siendo el más común de entre ellos el de Diffie-Hellman.

[Ribagorda:1997]

2.701.3 NEGOCIACIÓN DE CLAVE

Procedimiento por el que dos equipos de cifra interconectados cambian información a fin de determinar qué claves almacena cada uno para ser usadas en el cifrado del tráfico entre ellos. [CESID:1997]

2.701.4 (EN) KEY AGREEMENT (ALGORITHM OR PROTOCOL)

1. (I) A key establishment method (especially one involving asymmetric cryptography) by which two or more entities, without prior arrangement except a public exchange of data (such as public keys), each can generate the same key value. That is, the method does not send a secret from one entity to the other; instead, both entities, without prior arrangement except a public exchange of data, can compute the same secret value, but that value cannot be computed by other, unauthorized entities. (See: Diffie-Hellman- Merkle, key establishment, KEA, MQV. Compare: key transport.)

2. (O) "A method for negotiating a key value on line without transferring the key, even in an encrypted form, e.g., the Diffie- Hellman technique." [X509] (See: Diffie-Hellman-Merkle.)

3. (O) "The procedure whereby two different parties generate shared symmetric keys such that any of the shared symmetric keys is a function of the information contributed by all legitimate participants, so that no party [alone] can predetermine the value of the key." [A9042]

[RFC4949:2007]

2.701.5 (EN) KEY AGREEMENT

A key establishment procedure where resultant keying material is a function of information contributed by two or more participants, so that no party can predetermine the value of the keying material independent of the other partys contribution. [NIST-SP800-57:2007]

2.701.6 (EN) KEY AGREEMENT

A method for negotiating a key value on-line without transferring the key, even in an encrypted form, e.g. the Diffie-Hellman technique (see ISO/IEC ISO-11770-1 for more information on key agreement mechanisms). [X.509:2005]

2.701.7 (EN) KEY AGREEMENT

the process of establishing a shared secret between entities in such a way that neither of them can predetermine the value of that key. [ISO-15946-3:2002]

2.701.8 (EN) KEY AGREEMENT

The process of establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key. [ISO-11770-3:2008]

2.701.9 (FR) AGRÉMENT DE CLÉ

méthode de négociation en ligne de la valeur d'une clé sans transfert de cette dernière, même sous forme chiffrée, par exemple en utilisant la méthode Diffie-Hellman (se référer à l'ISO/IEC ISO-11770-1 pour plus d'informations concernant les procédés d'agrément de clé). [X.509:2005]

2.702 NIVEL DE CLASIFICACIÓN

Ver:

- *Información clasificada*

2.702.1 NIVEL DE CLASIFICACIÓN

Nivel de protección (dentro de una jerarquía de niveles) que debe ser aplicado a una cierta información para controlar que no se revela sin autorización previa.

2.702.2 (EN) CLASSIFICATION LEVEL

(I) A hierarchical level of protection (against unauthorized disclosure) that is required to be applied to certain classified data. (See: classified. Compare: security level.) [RFC4949:2007]

2.703 NEGRO

Ver

- *rojo*

2.703.1 NEGRO

En seguridad de la información, se aplica a aquellos elementos que hospedan información cifrada. Es lo contrario de “negro”.

2.703.2 (EN) BLACK

Designation applied to encrypted information and the information systems, the associated areas, circuits, components, and equipment processing that information. See also RED. [CNSSI_4009:2010]

2.704 NIVEL DE GARANTÍA DE EVALUACIÓN

Acrónimos: EAL

Ver:

- *Criterios comunes*
- http://en.wikipedia.org/wiki/Evaluation_Assurance_Level

2.704.1 NIVEL DE GARANTÍA DE EVALUACIÓN

Paquete que consiste en componentes de garantía de la Parte 3 y que representa un nivel en la escala de garantía predefinida de CC. [CC:2006]

2.704.1 (EN) EVALUATION ASSURANCE LEVEL (EAL)

Set of assurance requirements that represent a point on the Common Criteria predefined assurance scale. [CNSSI_4009:2010]

2.704.2 (EN) EVALUATION ASSURANCE LEVEL (EAL)

(N) A predefined package of assurance components that represents a point on the Common Criteria's scale for rating confidence in the security of information technology products and systems.

Tutorial: The Common Criteria defines a scale of seven, hierarchically ordered EALs for rating a TOE. From highest to lowest, they are as follows:

- EAL7. Formally verified design and tested.
- EAL6. Semiformally verified design and tested.
- EAL5. Semiformally designed and tested.
- EAL4. Methodically designed, tested, and reviewed.
- EAL3. Methodically tested and checked.
- EAL2. Structurally tested.
- EAL1. Functionally tested.

[RFC4949:2007]

2.704.3 (EN) EVALUATION ASSURANCE LEVEL (EAL)

an assurance package, consisting of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale. [CC:2006]

2.705 NIVEL DE RIESGO

Ver:

- *Riesgo*

2.705.1 NIVEL DE RIESGO:

Magnitud de un riesgo o combinación de riesgos, expresados en términos de la combinación de las consecuencias y de su probabilidad.[UNE Guía 73:2010]

2.705.2 (EN) LEVEL OF RISK

magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood [ISO Guide 73:2009]

2.705.3 (FR) NIVEAU DE RISQUE

importance d'un risque ou combinaison de risques, exprimée en termes de combinaison des conséquences et de leur vraisemblance [ISO Guide 73:2009]

2.706 NMAP

2.706.1 NMAP

Software para el análisis de riesgos de seguridad encargado de delinear redes e identificar puertos abiertos en los recursos de red.

http://es.pcisecuritystandards.org

2.706.2 (EN) NMAP

Security-scanning software that maps networks and identifies open ports in network resources.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.706.3 (FR) NMAP

Logiciel d'analyse de sécurité qui mappe les réseaux et identifie les ports ouverts dans les ressources réseau.

http://fr.pcisecuritystandards.org/

2.707 NONCE

Ver:

- *Parámetro variante en el tiempo*
- *Sal*
- http://en.wikipedia.org/wiki/Nonce

2.707.1 NONCE

Valor aleatorio que no se repite nunca. Se utiliza en protocolos criptográficos para prevenir ataques de tipo 'replay'.

2.707.2 (EN) NONCE

A value used in security protocols that is never repeated with the same key. For example, nonces used as challenges in challenge-response authentication protocols must not be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement than a random challenge, because a nonce is not necessarily unpredictable. [NIST-SP800-63:2013]

2.707.3 (EN) NONCE

A random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing the transmittal of live data rather than replayed data, thus detecting and protecting against replay attacks. [CNSSI_4009:2010]

2.707.4 (EN) NONCE

(I) A random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing liveness and thus detecting and protecting against replay attacks. (See: fresh.) [RFC4949:2007]

2.707.5 (EN) NONCE

Nonce means 'for the present time' or 'for a single occasion or purpose', although the word is not often found in general use. A dictionary may note nonce words, those for which there is only a single textual instance.

In security engineering, a nonce is a 'number used once'. It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in 'replay attacks'. For instance, nonces are used in HTTP digest access authentication to calculate an MD5 digest of the password. The nonces are different each time the 401 authentication challenge response code is presented, thus making the replay attack virtually impossible. Some also refer to Initialization Vectors as nonces for the above reasons. In order to ensure that a nonce is used only once it should be time-variant (including a suitably granular timestamp in its value), or generated with enough random bits to ensure a probabilistically insignificant chance of repeating a previously generated value.

http://en.wikipedia.org/wiki/Nonce

2.707.6 (EN) NONCE

A non-repeating value, such as a counter, used in key management protocols to thwart replay and other types of attack. [x942]

A nonce is a time-variant parameter, such as a counter, random number, or time stamp, used in key management protocols to thwart message replay and other types of attacks. [X942]

http://www.garlic.com/~lynn/x9fgloss.htm

2.708 NO REPUDIO

Ver:

- *Repudio*
- *Evidencia*
- *Prueba*

2.708.1 NO REPUDIO

Capacidad para corroborar que es cierta la reivindicación de que ocurrió un cierto suceso o se realizó una cierta acción por parte de las entidades que lo originaron. [UNE-ISO/IEC 27000:2014]

2.708.2 NO REPUDIO

Con la expresión "no repudio" se hace referencia a la capacidad de afirmar la autoría de un mensaje o información, evitando que el autor niegue la existencia de su recepción o creación. Entre sus características está:

- Comprobar la creación y origen de los contenidos.
- Poseer documentos que acrediten el envío o recepción de mensajes.
- Comprobar el envío o recepción de llamadas, etc.

http://www.inteco.es/glossary/Formacion/Glosario/

2.708.3 NO REPUDIO

El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. [CCN-STIC-405:2006]

2.708.4 NO REPUDIO

Servicio de seguridad (OSI ISO-7498-2) que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

En el primer caso el no repudio se denomina en origen y en el segundo en destino.

[Ribagorda:1997]

2.708.5 NO REPUDIO EN ORIGEN (NONREPUDIATION WITH PROOF OF ORIGEN)

Servicio de seguridad que provee al receptor de los datos de una prueba del origen de los mismos, que puede usarse ante intentos del emisor de negar su remisión (ISO-7498-2) [Ribagorda:1997]

2.708.6 NO REPUDIO EN DESTINO (NOREPUDIATION WITH PROOF OF DELIVERY)

Servicio de seguridad que provee al emisor de los datos de una prueba de la recepción de los mismos, que puede usarse ante intentos del destinatario de negar su recepción (ISO-7498-2) [Ribagorda:1997]

2.708.7 NO REPUDIO

Servicio de seguridad que asegura que el origen de una información no puede rechazar su transmisión o su contenido, y/o que el receptor de una información no puede negar su recepción o su contenido. [CESID:1997]

2.708.8 (EN) NON-REPUDIATION

ability to prove the occurrence of a claimed event or action and its originating entities [ISO/IEC 27000:2014]

2.708.9 (EN) NON-REPUDIATION

Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message. [NIST-SP800-53:2013]

2.708.1 (EN) NON-REPUDIATION

Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

NIST 800-53: Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.

[CNSSI_4009:2010]

2.708.2 (EN) NON-REPUDIATION SERVICE

1. (I) A security service that provide protection against false denial of involvement in an association (especially a communication association that transfers data). (See: repudiation, time stamp.) [RFC4949:2007]

2.708.3 (EN) NON-REPUDIATION WITH PROOF OF ORIGIN

(I) A security service that provides the recipient of data with evidence that proves the origin of the data, and thus protects the recipient against an attempt by the originator to falsely deny sending the data. (See: non-repudiation service.) [RFC4949:2007]

2.708.4 (EN) NON-REPUDIATION WITH PROOF OF RECEIPT

(I) A security service that provides the originator of data with evidence that proves the data was received as addressed, and thus protects the originator against an attempt by the recipient to falsely deny receiving the data. (See: non-repudiation service.) [RFC4949:2007]

2.708.5 (EN) NON-REPUDIATION

A service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party as having originated from a specific entity in possession of the private key of the claimed signatory. [NIST-SP800-57:2007]

2.708.6 (EN) NON-REPUDIATION

Protection from denial by one of the entities involved in a communication of having participated in all or part of the communication. [H.235:2005]

2.708.7 (EN) NON-REPUDIATION

Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the senders identity, so neither can later legitimately deny having processed, stored, or transmitted the information. [NIST-SP800-60V2:2004]

2.708.8 (EN) NON-REPUDIATION EXCHANGE

A sequence of one or more transfers of non-repudiation information (NRI) for the purpose of non-repudiation. [ISO-13888-1:2004]

2.708.9 (EN) NON-REPUDIATION INFORMATION

A set of information that may consist of the information about an event or action for which evidence is to be generated and verified, the evidence itself, and the non-repudiation policy in effect. [ISO-13888-1:2004]

2.708.10 (EN) NON-REPUDIATION OF CREATION

This service is intended to protect against an entity's false denial of having created the content of a message (i.e. being responsible for the content of a message). [ISO-13888-1:2004]

2.708.11 (EN) NON-REPUDIATION WITH PROOF OF DELIVERY

security service in which the sender of data is provided with proof of delivery of data

NOTE 1. This will protect against any subsequent attempt by the recipient to falsely deny receiving the data or its contents.

NOTE 2. Adapted from ISO-7498-2 | CCIT Rec. X.800.

[ISO-18028-2:2006]

2.708.12 (EN) NON-REPUDIATION OF DELIVERY

This service is intended to protect against a recipient's false denial of having received the message and recognized the content of a message. [ISO-13888-1:2004]

2.708.13 (EN) NON-REPUDIATION OF KNOWLEDGE

This service is intended to protect against a recipient's false denial of having taken notice of the content of a received message. [ISO-13888-1:2004]

2.708.14 (EN) NON-REPUDIATION WITH PROOF OF ORIGIN

security service in which the recipient of data is provided with proof of the origin of data

NOTE 1. This will protect against any attempt by the sender to falsely deny sending the data or its contents.

NOTE 2. Adapted from ISO-7498-2 | CCIT Rec. X.800.

[ISO-18028-2:2006]

2.708.15 (EN) NON-REPUDIATION OF ORIGIN

This service is intended to protect against the originator's false denial of having created the content of a message and of having sent a message. [ISO-13888-1:2004]

2.708.16 (EN) NON-REPUDIATION OF RECEIPT

This service is intended to protect against a recipient's false denial of having received a message. [ISO-13888-1:2004]

2.708.17 (EN) NON-REPUDIATION OF SENDING

This service is intended to protect against the sender's false denial of having sent a message. [ISO-13888-1:2004]

2.708.18 (EN) NON-REPUDIATION OF SUBMISSION

This service is intended to provide evidence that a delivery authority has accepted the message for transmission. [ISO-13888-1:2004]

2.708.19 (EN) NON-REPUDIATION OF TRANSPORT

This service is intended to provide evidence for the message originator that a delivery authority has delivered the message to the intended recipient. [ISO-13888-1:2004]

2.708.20 (EN) NON-REPUDIATION POLICY

A set of criteria for the provision of non-repudiation services. More specifically, a set of rules to be applied for the generation and verification of evidence and for adjudication. [ISO-13888-1:2004]

2.708.21 (EN) NON-REPUDIATION TOKEN

A special type of security token as defined in ISO/IEC ISO-10181-1 consisting of evidence, and, optionally, of additional data. [ISO-13888-1:2004]

2.708.22 (EN) NON-REPUDIATION

This service is intended to protect against a recipient's false denial of [ISO-13888-1:2004]

2.708.23 (EN) NRD TOKEN

Non-repudiation of delivery token. A data item which allows the originator to establish non-repudiation of delivery for a message. [ISO-13888-1:2004]

2.708.24 (EN) NRO TOKEN

Non-repudiation of origin token. A data item which allows recipients to establish non-repudiation of origin for a message. [ISO-13888-1:2004]

2.708.25 (EN) NRS TOKEN

Non-repudiation of submission token. A data item which allows either the originator (sender) or the delivery authority to establish non-repudiation of submission for a message having been submitted for transmission. [ISO-13888-1:2004]

2.708.26 (EN) NRT TOKEN

Non-repudiation of transport token. A data item which allows either the originator or the delivery authority to establish non-repudiation of transport for a message. [ISO-13888-1:2004]

2.708.27 (EN) NON-REPUDIATION

the ability to prove an action or event has taken place, so that this event or action cannot be repudiated later. [ISO-13888-1:2004] [ISO-7498-2:1989]

2.708.28 (EN) NON-REPUDIATION

The Non-repudiation Security Dimension provides means for preventing an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions (such as proof of obligation, intent, or commitment; proof of data origin, proof of ownership, proof of resource use). It ensures the availability of evidence that can be presented to a third party and used to prove that some kind of event or action has taken place. [X.805:2003]

2.708.29 (EN) NON-REPUDIATION

Non-repudiation is the ability for a system to prove that a specific user and only that specific user sent a message and that it hasn't been modified.

http://www.sans.org/security-resources/glossary-of-terms/

2.708.30 (FR) NON-RÉPUDIATION

Service de sécurité dont l'objectif est de générer, récolter, maintenir, rendre disponible et valider l'évidence (information utilisée pour établir une preuve) concernant un évènement ou une action revendiquée afin de résoudre les possibles disputes sur l'occurrence ou non de l'évènement ou de l'action. [ISO-13888-1:2004]

2.709 NORMA

2.709.1 NORMA

Regla que se debe seguir o a que se deben ajustar las conductas, tareas, actividades, etc.

DRAE. Diccionario de la Lengua Española.

2.709.2 ESTÁNDAR

Una práctica de negocio o producto tecnológico que es una práctica aceptada, avalada por la empresa o por el equipo gerencial de TI. Los estándares se pueden implantar para dar soporte a una

política o a un proceso, o como respuesta a una necesidad operativa. Así como las políticas, los estándares deben incluir una descripción de la forma en que se detectará el incumplimiento. [COBIT:2006]

2.709.3 (EN) STANDARD

a business practice or technology product that is an accepted practice endorsed by the enterprise of IT management team. Standards can be put in place to support a policy or a process, or as a response to an operational need. Like policies, standards must include a description of the manner in which non-compliance will be detected. [COBIT:2006]

2.710 NOTARIZACIÓN

Ver:

- *Tercera parte de confianza*
- *No repudio*

2.710.1 NOTARIZACIÓN

Registro de datos por una Tercera Parte Fiable, quien da fe ulteriormente de la exactitud de los mismos y de algunos de sus atributos tales como contenido, origen, fecha y hora y emisor (ISO-7498-2).

Habitualmente los datos arriba citados se refieren a la clave pública (en un criptosistema asimétrico) de un usuario o entidad, en cuyo caso la notarización se realiza por la Autoridad de Certificación o Tercera Parte Fiable, que en ocasiones se denomina, informalmente, Notario Electrónico.

[Ribagorda:1997]

2.710.2 NOTARIZACIÓN

Registro de datos por un tercero de confianza que permite la ulterior seguridad de la exactitud de sus características, tales como contenido, origen, fecha, entrega. [ISO-7498-2:1989]

2.710.3 (EN) DIGITAL NOTARY

(I) An electronic functionary analogous to a notary public. Provides a trusted timestamp for a digital document, so that someone can later prove that the document existed at that point in time; verifies the signature(s) on a signed document before applying the stamp. (See: notarization.) [RFC4949:2007]

2.710.4 (EN) NOTARIZATION

(I) Registration of data under the authority or in the care of a trusted third party, thus making it possible to provide subsequent assurance of the accuracy of characteristics claimed for the data, such as content, origin, time of existence, and delivery. [ISO-7498-2] (See: digital notary.) [RFC4949:2007]

2.710.5 (EN) NOTARIZATION

The provision of evidence by a notary about the properties of the entities involved in a action or event, and of the data stored or communicated. [ISO-13888-1:2004]

2.710.6 (EN) NOTARIZATION TOKEN

A non-repudiation token generated by a notary. [ISO-13888-1:2004]

2.710.7 (EN) NOTARY (NOTARY AUTHORITY)

A trusted third party trusted to provide evidence about the properties of the entities involved and of the data stored or communicated, or to extend the lifetime of an existing token beyond its expiry or beyond subsequent revocation. [ISO-13888-1:2004]

2.710.8 (EN) NOTARIZATION

The registration of data with a trusted third party that allows the later assurance of the accuracy of its characteristics such as content, origin, time and delivery. [ISO-7498-2:1989]

2.710.9 (FR) NOTARISATION

Enregistrement de données chez un tiers de confiance permettant de s'assurer ultérieurement de leur exactitude (contenu, origine, date, remise). [ISO-7498-2:1989]

2.711 NUKE

2.711.1 NUKE

Familia de ataques en red consistente en el envío de paquetes ICMP mal construidos.

2.711.2 (EN) NUKES

Nukes are malformed or specially crafted packets.

2.711.3 (EN) WHAT IS A NUKE ATTACK?

A nuke attack consists in sending fragmented or otherwise invalid ICMP packets to the target, achieved by using a modified ping utility to repeatedly send this corrupt data, thus slowing down the affected computer until it comes to a complete stop. In online gaming, nuking is used by spamming another user, or all other users, with random repeated messages in quick succession. Such techniques are also seen in instant messaging programs as repeatedly sending text can be assigned to a macro or AppleScript. Modern operating systems are usually resistant to these techniques, and online games now have third party "Flood control."

http://en.wikipedia.org/wiki/Nuke_%28computer%29

2.712 NULL INJECTION

Ver:

- *Inyección SQL*

- *XPath injection*
- *LDAP injection*
- *Meta-Character Injection*

2.712.1 NULL INJECTION

Ataque contra servidores web consistente en inyectar caracteres 0x00 en cadenas para aprovechar que muchos programas desarrollados en C o C++ utilizan dicho carácter como 'fin de cadena' y no siguen analizando.

2.712.2 (EN) NULL INJECTION

An exploitation technique used to bypass sanity checking filters by adding URL encoded null-byte characters to user-supplied data. When developers create web applications in a variety of programming languages, these web applications often pass data to underlying lower level C-functions for further processing and functionality. If a user-supplied string contains a null character (0), the web application may stop processing the string at the point of the null. Null Injection is a form of a meta-character Injection attack.

http://www.webappsec.org/projects/glossary/

2.713 NÚMERO DE AUTENTICACIÓN DE UNA TRANSACCIÓN

Acrónimo: TAN

2.713.1 NÚMERO DE AUTENTICACIÓN DE UNA TRANSACCIÓN

Número singular que sólo se utiliza una vez para identificar una transacción y autenticarla.

2.713.2 (EN) TRANSACTION AUTHENTICATION NUMBER

A Transaction authentication number, TAN or T.A.N. is used by some online banking services as a form of single use one-time passwords to authorize financial transactions. TANs are a second layer of security above and beyond the traditional single-password authentication.

TANs are believed to provide additional security because they act as a form of two-factor authentication. Should the physical document or token containing the TANs be stolen, it will be of little use without the password; conversely, if the login data are obtained, no transactions can be performed without a valid TAN.

http://en.wikipedia.org/wiki/Transaction_authentication_number

2.714 NÚMERO DE IDENTIFICACIÓN PERSONAL

Acrónimos: PIN

2.714.1 PIN

Acrónimo de “personal identification number” (número de identificación personal). Contraseña numérica secreta que conocen solo el usuario y un sistema para autenticar al usuario en el sistema. El usuario tan solo obtiene acceso si su PIN coincide con el PIN del sistema. Los PIN más comunes

se utilizan en las transacciones de adelanto de efectivo y las ATM. Otro tipo de PIN es el que utilizan las tarjetas con chip de tipo EMV, en las que el PIN reemplaza la firma del titular de la tarjeta.

http://es.pcisecuritystandards.org

2.714.2 NÚMERO DE IDENTIFICACIÓN PERSONAL

Sucesión de dígitos decimales, entre 4 y 12, que el usuario de una tarjeta bancaria, de débito o de crédito, posee para su autenticación. Aunque las siglas PIN corresponden a la expresión en lengua inglesas son también frecuentemente usadas en castellano. [Ribagorda:1997]

2.714.3 NÚMERO DE IDENTIFICACIÓN PERSONAL

En el ámbito bancario, secuencia de dígitos decimales utilizada como contraseña para poder acceder a un terminal bancario y efectuar una operación.

Si utiliza cifras y letras se denomina Código de identificación personal (PIC).

[CESID:1997]

2.714.4 (EN) PERSONAL IDENTIFICATION NUMBER (PIN)

1a. (I) A character string used as a password to gain access to a system resource. (See: authentication information.) [RFC4949:2007]

2.714.5 (EN) PIN

Acronym for “personal identification number.” Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder’s signature.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.714.6 (EN) PIN (PERSONAL IDENTIFICATION NUMBER)

A series of numbers or code which grants a user access to a secured Web site, service, or program.

http://iab.com/

2.714.7 (EN) PERSONAL IDENTIFICATION NUMBER

an alphanumeric code or password used to authenticate an identity. [FIPS-140-2:2001]

2.714.8 (FR) PIN

Acronyme de «personal identification number», numéro d’identification personnel. Mot de passe numérique secret, connu uniquement de l’utilisateur et du système afin d’authentifier l’utilisateur. L’utilisateur n’est autorisé à accéder au système que si le code PIN qu’il fournit correspond à celui enregistré dans le système. Les codes PIN sont utilisés pour les distributeurs automatiques pour

des transactions de retrait d'espèces. Un autre type de code PIN est celui utilisé sur les cartes à puce EMV, remplaçant la signature du titulaire de carte.

http://fr.pcisecuritystandards.org/

2.715 NVD – NATIONAL VULNERABILITY DATABASE

NVD

Common Vulnerabilities and Exposures, siglas CVE, es una lista de información registrada sobre conocidas vulnerabilidades de seguridad, donde cada referencia tiene un número de identificación único.1 De esta forma provee una nomenclatura común para el conocimiento público de este tipo de problemas y así facilitar la compartición de datos sobre dichas vulnerabilidades.

Fue definido y es mantenido por The MITRE Corporation (por eso a veces a la lista se la conoce por el nombre MITRE CVE List) con fondos de la National Cyber Security Division del gobierno de los Estados Unidos de América. Forma parte del llamado Security Content Automation Protocol.

La información y nomenclatura de esta lista es usada en la National Vulnerability Database, el repositorio de los Estados Unidos de América de información sobre vulnerabilidades.

https://es.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

2.715.1 (EN) NVD

National Vulnerability Database (NVD) is a government repository of standards-based vulnerability information.

The NVD is a product of the National Institute of Standards and Technology (NIST) Computer Security Division and is used by the U.S. Government for security management and compliance as well as automatic vulnerability management.

The NVD is sponsored by the Department of Homeland Security (DHS), NCCIC and US-CERT. NVD is used as the repository for security-related content for NIST's security content automation protocol (SCAP). The National Security Agency (NSA), OSD, DHS, NIST, and DISA are all users of NVD as part of the government's information security automation program.

The automation of the systems through SCAP and NVD, for example, as well as patch management are enabled by the Federal Desktop Core Configuration (FDCC), a checklist for mandatory configuration settings on US government computers.

http://whatis.techtarget.com/definition/National-Vulnerability-Database-NVD

2.715.2 (EN) NVD

The National Vulnerability Database is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics. NVD supports the Information Security Automation Program (ISAP).

On Friday March 8, 2013, the database was taken offline after it was discovered that the system used to run multiple government sites had been compromised by a software vulnerability of Adobe ColdFusion.

In addition to providing a list of Common Vulnerabilities and Exposures (CVEs), the NVD scores CVEs to quantify the risk of vulnerabilities, calculated from a set of equations based on metrics such as access complexity and availability of a remedy.

https://en.wikipedia.org/wiki/National_Vulnerability_Database

2.716 OAKLEY

Ver:

- http://www.ietf.org/rfc/rfc2412
- *IPsec - IP security*
- *ISAKMP - Internet Security Association Key Management Protocol*

2.716.1 OAKLEY

Protocolo de establecimiento de claves propuesto para IPsec.

2.716.2 (EN) OAKLEY

(I) A key establishment protocol (proposed for IPsec but superseded by IKE) based on the Diffie-Hellman-Merkle algorithm and designed to be a compatible component of ISAKMP. [R2412] [RFC4949:2007]

2.716.3 (EN) OAKLEY

The Oakley Session Key Exchange provides a hybrid Diffie-Hellman session key exchange for use within the ISAKMP framework. Oakley provides the important property of Perfect Forward Secrecy (PFS).

http://www.watchguard.com/glossary/

2.717 OBJETIVO DE CONTROL

2.717.1 OBJETIVO DE CONTROL

Declaración formal de los resultados que se esperan de la implantación de procedimientos concretos de control en un determinado proceso.

2.717.2 OBJETIVO DE CONTROL

Un estatuto del resultado o propósito que se desea alcanzar al implantar procedimientos de control en un proceso en particular. [COBIT:2006]

2.717.3 (EN) CONTROL OBJECTIVE

A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process. [COBIT:2006]

2.718 OBJETIVO DE PUNTO DE RECUPERACIÓN

Acrónimos: RPO

Ver:

- *Continuidad*
- *Objetivo de tiempo de recuperación*

2.718.1 OBJETIVO DE PUNTO DE RECUPERACIÓN

(Operación del Servicio) La cantidad máxima de información que puede ser perdida cuando el Servicio es restaurado tras una interrupción. El Objetivo de Punto de Recuperación se expresa como una longitud de tiempo antes del Fallo. Por ejemplo, un Objetivo de Punto de Recuperación de un día debe ser soportado por Copias de Seguridad diarias, y hasta 24 horas de información pueden ser perdidas. Los Objetivos de Punto de Recuperación para cada Servicio de TI debería ser negociado, acordado y documentado, y utilizado como Requisitos para el Diseño del Servicio y los Planes de Continuidad de TI. [ITIL:2007]

2.718.2 OBJETIVO DEL PUNTO DE RECUPERACIÓN

El objetivo del punto de recuperación (RPO) es la antigüedad de los archivos que se deben recuperar del almacenamiento de copia de seguridad para reanudar las operaciones normales en caso de inactividad de un ordenador, sistema o red como resultado de una falla de hardware, programa o comunicación. El RPO se expresa en forma regresiva en el tiempo (es decir, en el pasado) desde el instante en el que ocurrió el fallo; además, se puede especificar en segundos, minutos, horas o días Es importante considerar la Planificación de Recuperación en caso de Desastre (DRP) Una vez que se ha definido el RPO para un ordenador, sistema o red en particular, se determina la frecuencia mínima en la cual se deben realizar las copias de seguridad Esto, junto con el Objetivo de Recuperación del Tiempo (RTO) ayuda a los administradores a elegir las tecnologías y procedimientos óptimos de recuperación en caso de desastre.

http://www.recall.es/why-recall/data-protection-terminology

2.718.3 (EN) RECOVERY POINT OBJECTIVE (RPO)

Determined based on the acceptable data loss in case of a disruption of operations

It indicates the earliest point in time that is acceptable to recover the data. The RPO effectively quantifies the permissible amount of data loss in case of interruption.

ISACA, Cybersecurity Glossary, 2014

2.718.4 (EN) RECOVERY POINT OBJECTIVE (RPO)

(Service Operation) The maximum amount of data that may be lost when Service is Restored after an interruption. Recovery Point Objective is expressed as a length of time before the Failure. For example a Recovery Point Objective of one day may be supported by daily Backups, and up to 24 hours of data may be lost. Recovery Point Objectives for each IT Service should be negotiated, agreed and documented, and used as Requirements for Service Design and IT Service Continuity Plans. [ITIL:2007]

2.718.5 (EN) RECOVERY POINT OBJECTIVES (RPOS)

RPOs represent the amount of data that can be lost without severely impacting the recovery of operations or the point in time in which systems and data must be recovered (e.g., the date and time of a business disruption).

http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-b-glossary.aspx

2.718.6 (FR) OBJECTIF DE POINT DE REPRISE (RPO)

(Exploitation de Services) (Service Design) La quantité maximale acceptable de données pouvant être perdues lors de la restauration d'un service après une interruption. L'objectif d'un point de reprise est exprimé sous la forme d'une durée avant la panne. Par exemple, un objectif de point de reprise d'une journée peut être attendu grâce à des copies de sauvegarde quotidiennes. Les objectifs de point de reprise de chaque service des TI doivent être négociés, acceptés et documentés ; ils doivent servir d'exigences à la Conception de services et aux plans de continuité des services des TI. [ITIL:2007]

2.719 OBJETIVO DE SEGURIDAD

Ver:

- *Criterios comunes*

2.719.1 OBJETIVO DE SEGURIDAD

Declaración de la intención de contrarrestar las amenazas identificadas y/o de cumplir las políticas e hipótesis de seguridad identificadas de la organización. [CC:2006]

2.719.2 OBJETIVO DE SEGURIDAD

La contribución a la seguridad que se pretende realice el Objeto de Evaluación (ITSEC).

Más concretamente, es la especificación de la seguridad requerida por un Objeto de Evaluación, que es usada como base para la evaluación. El Objetivo de Seguridad especificará las funciones de seguridad de Objeto de Evaluación. Puede también especificar las metas de seguridad a alcanzar, las amenazas a estas metas u cualesquiera mecanismos particulares de seguridad que sean empleados.

[Ribagorda:1997]

2.719.3 OBJETIVO DE SEGURIDAD

1. Contribución a la seguridad que se pretende conseguir con un sistema de seguridad de información (security objetives).

2. Especificación del grado de seguridad exigido a un sistema de información como base para realizar una evaluación (security target).

[CESID:1997]

2.719.4 (EN) SECURITY OBJECTIVE

Confidentiality, integrity, or availability. [FIPS-199:2004] [FIPS-200:2006]

2.719.5 (EN) SECURITY OBJECTIVE

a statement of intent to counter identified threats and/or satisfy identified organisation security policies and/or assumptions. [CC:2006]

2.719.6 (EN) SECURITY OBJECTIVE

the contribution to security which a Target of Evaluation is intended to achieve. [ITSEC:1991]

2.720 OBJETIVO DE TIEMPO DE RECUPERACIÓN

Acrónimos: RTO

Ver:

- *Continuidad*
- *Objetivo de Punto de Recuperación*

2.720.1 OBJETIVO DE TIEMPO DE RECUPERACIÓN

(Operación del Servicio) El tiempo máximo permitido para la recuperación de un Servicio de TI tras una interrupción. El Nivel de Servicio a ser provisto debe ser inferior a los Objetivos de Nivel de Servicio. Los Objetivos de Tiempo de Recuperación para cada Servicio de TI deberían ser negociados, acordados y documentados. Ver Análisis de Impacto de Negocio. [ITIL:2007]

2.720.2 OBJETIVO DE TIEMPO DE RECUPERACIÓN

El objetivo de tiempo de recuperación (Recovery Time Objective, RTO) es la máxima cantidad de tiempo tolerable que un ordenador, sistema, red o aplicación puede estar inactivo después de una fallo o un desastre. El RTO es una función del punto hasta el cual la interrupción altera las operaciones normales y la cantidad de ingresos-pérdidas por unidad de tiempo como resultado del desastre Estos factores, a su vez, dependen del equipo y de la/s aplicación/es afectada/s El RTO se mide en segundos, minutos, horas o días, y es una consideración importante en la planificación de recuperación en caso de desastre.

http://www.recall.es/why-recall/data-protection-terminology

2.720.3 (EN) RECOVERY TIME OBJECTIVE (RTO)

The amount of time allowed for the recovery of a business function or resource after a disaster occurs

ISACA, Cybersecurity Glossary, 2014

2.720.4 (EN) RECOVERY TIME OBJECTIVE (RTO)

(Service Operation) The maximum time allowed for recovery of an IT Service following an interruption. The Service Level to be provided may be less than normal Service Level Targets. Recovery Time Objectives for each IT Service should be negotiated, agreed and documented.See Business Impact Analysis. [ITIL:2007]

2.720.5 (EN) RECOVERY TIME OBJECTIVE

target time set for:

- resumption of product or service delivery after an incident; or
- resumption of performance of an activity after an incident; or
- recovery of an IT system or application after an incident.

[BS25999-1:2006]

2.720.6 (EN) WHAT IS THE RECOVERY TIME OBJECTIVE?

The balancing point between the MAO (Maximum Allowable Outage) and the cost to recover establishes the information systems RTO. Recovery strategies must be created to meet the RTO. The strategy must also address recovering information system critical components within a priority, as established by their individual RTOs. [NIST-SP800-100:2006]

2.720.7 (EN) RECOVERY TIME OBJECTIVES (RTOS)

RTOs represent the maximum allowable downtime that can occur without severely impacting the recovery of operations or the time in which systems, applications, or business functions must be recovered after an outage (e.g. the point in time that a process can no longer be inoperable).

http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-b-glossary.aspx

2.720.8 (FR) OBJECTIF DE TEMPS DE REPRISE

(Exploitation de Services) (Service Design) La durée maximale accordée à la reprise d'un service après une interruption. Le niveau de service à fournir peut être inférieur aux cibles de niveau de service normales. Les objectifs de temps de reprise de chaque service des TI doivent être négociés, convenus et documentés.

Voir Analyse d'impact sur le business (BIA).

[ITIL:2007]

2.721 OBJETO DE EVALUACIÓN

Acrónimos: TOE

Ver:

- *Criterios comunes*

2.721.1 OBJETO DE EVALUACIÓN

Sistema o producto de tecnologías de la información que se somete a una evaluación de seguridad. [Ribagorda:1997]

2.721.2 OBJETO DE EVALUACIÓN

Sistema de información al que se le efectúa una evaluación. [CESID:1997]

2.721.3 (EN) TARGET OF EVALUATION (TOE)

a set of software, firmware and/or hardware possibly accompanied by guidance. [CC:2006]

2.721.4 (EN) TARGET OF EVALUATION

an IT system or product which is subjected to security evaluation. [ITSEC:1991]

2.722 OBLIGATORIO

Ver:

- *Informativo*

2.722.1 DOCUMENTO NORMATIVO

Especificación técnica, de aplicación voluntaria, aprobada por consenso y elaborada por un Organismo de Normalización reconocido.

Los documentos normativos UNE, elaborados por AENOR son: las Normas UNE, las Normas UNE Experimentales y los Informes UNE, así como las Modificaciones y Erratum.

Guía para la Redacción de Documentos Normativos UNE, AENOR, 2006.

2.722.2 (EN) NORMATIVE

normative text describes the scope of the document, and sets out provisions. (ISO/IEC). Within normative text, the verbs shall, should, may, and can have the ISO standard meanings described in this glossary and the verb must is not used. Unless explicitly labelled informative, all CC text is normative. [CC:2006]

2.723 OCSP - ONLINE CERTIFICATE STATUS PROTOCOL

Acrónimos: OCSP

Ver:

- http://www.ietf.org/rfc/rfc2560
- *Lista de revocación de certificados*

2.723.1 OCSP - ONLINE CERTIFICATE STATUS PROTOCOL

Protocolo Internet utilizado por un cliente para obtener el estado actual de un certificado digital.

2.723.2 (EN) ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)

(I) An Internet protocol [R2560] used by a client to obtain from a server the validity status and other information about a digital certificate. (Mentioned in [X509] but not specified there.) [RFC4949:2007]

2.724 OCULTACIÓN

Ver:

- *Esteganografía*
- *Virus*

2.724.1 OCULTACIÓN

Técnica utilizada por algunos virus para no ser localizables, haciendo parecer que los ficheros infectados no lo están, interceptan peticiones de acceso a disco, por tanto cuando una aplicación antivirus intenta leer ficheros o sectores de arranque para encontrar virus, encuentra que el fichero no esta afectado, ocultando en algunos casos el tamaño real del fichero, devolviendo el tamaño anterior a la infección.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.724.2 (EN) STEALH

When a virus hides itself. Infected files look as normal files. When the virus is active, it intercepts requests of access to disc, so that when an application tries to access the file, it finds the normal contents and size. For instance, an active virus may hide itself from anti-virus applications.

2.724.3 (EN) STEALTHING

Stealthing is a term that refers to approaches used by malicious code to conceal its presence on the infected system.

http://www.sans.org/security-resources/glossary-of-terms/

2.725 OCULTAMIENTO

2.725.1 OCULTAMIENTO

En el contexto de las PCI DSS, se refiere al método para ocultar un segmento de los datos cuando se muestran o imprimen. El ocultamiento se utiliza cuando no existe un requisito por parte del negocio de ver el PAN completo. El ocultamiento se relaciona con la protección del PAN cuando se muestra o imprime.

Consulte Truncamiento para obtener información sobre la protección del PAN cuando se almacena en archivos, bases de datos, etc.

http://es.pcisecuritystandards.org

2.725.2 (EN) MASKING

In the context of PCI DSS, it is a method of concealing a segment of data when displayed or printed. Masking is used when there is no business requirement to view the entire PAN. Masking relates to protection of PAN when displayed or printed. See Truncation for protection of PAN when stored in files, databases, etc.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.725.3 (FR) MASQUAGE

Dans le cadre de la norme PCI DSS, il s'agit d'une méthode occultant un segment de données lorsque celles-ci sont affichées ou imprimées. Le masquage est utilisé lorsqu'il n'existe aucune justification professionnelle d'afficher le PAN dans son intégralité. Le masquage concerne la protection du PAN lorsque celui-ci est affiché ou imprimé. Voir Troncature pour la protection du PAN lorsqu'il est stocké dans des fichiers, bases de données, etc.

http://fr.pcisecuritystandards.org/

2.726 OFB - OUTPUT FEEDBACK MODE

Acrónimos: OFB

Ver:

- *Modo de operación (1)*
- [NIST-SP800-38A:2001]
- [FIPS-81:1980]
- *Criptografía de clave secreta*
- *Valor de inicialización*
- http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

2.726.1 OFB - OUTPUT FEEDBACK MODE

Modalidad de cifrado de flujo cuyo generador de la serie cifrante está constituido por un cifrado de bloques seguido por un selector de bits. [Ribagorda:1997]

2.726.2 (EN) OUTPUT FEEDBACK (OFB)

(N) A block cipher mode that modifies ECB mode to operate on plaintext segments of variable length less than or equal to the block length. [FP081] (See: block cipher, [SP38A].) [RFC4949:2007]

2.726.3 (EN) OFB - OUTPUT FEEDBACK MODE

The output feedback (OFB) mode makes a block cipher into a synchronous stream cipher: it generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext. Just as with other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location. This property allows many error correcting codes to function normally even when applied before encryption.

Because of the symmetry of the XOR operation, encryption and decryption are exactly the same.

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

2.727 OPCIÓN DE RECUPERACIÓN

Ver:

- *Cold standby*
- *Hot standby*

2.727.1 OPCIÓN DE RECUPERACIÓN

(Diseño del Servicio) Una Estrategia para responder a una interrupción del Servicio. Las Estrategias comunes son No Hacer Nada, Alternativa Manual, Arreglo Recíproco, Recuperación Gradual, Recuperación Rápida, Recuperación Inmediata. Las Opciones de Recuperación pueden utilizar instalaciones dedicadas, o instalaciones de Terceros compartidas por múltiples Negocios. [ITIL:2007]

2.727.2 (EN) RECOVERY OPTION

(Service Design) A Strategy for responding to an interruption to Service. Commonly used Strategies are Do Nothing, Manual Workaround, Reciprocal Arrangement, Gradual Recovery, Intermediate Recovery, Fast Recovery, Immediate Recovery. Recovery Options may make use of dedicated facilities, or Third Party facilities shared by multiple Businesses.

[ITIL:2007]

2.727.3 (FR) OPTION DE REPRISE

(Conception de service) Une stratégie permettant de répondre à une interruption de service. Les stratégies les plus couramment employées sont Ne rien faire, Solution de contournement manuelle, Arrangement réciproque, Reprise graduelle, Reprise intermédiaire, Reprise rapide, Reprise immédiate. Les options de reprise peuvent faire usage de locaux spécifiques ou de locaux tierces partagés par plusieurs métiers. [ITIL:2007]

2.728 OPENPGP - OPEN PRETTY GOOD PRIVACY

Ver:

- http://www.ietf.org/rfc/rfc2440
- *PGP - Pretty Good Privacy*
- *GPG - GNU Privacy Guard*

2.728.1 OPENPGP

La IETF se ha basado en el diseño de PGP para crear el estándar de Internet OpenPGP. Las últimas versiones de PGP son conformes o compatibles en mayor o menor medida con ese estándar.

http://es.wikipedia.org/wiki/OpenPGP

2.728.2 (EN) OPENPGP

In July 1997, PGP Inc. proposed to the IETF that there be a standard called OpenPGP. They gave the IETF permission to use the name OpenPGP to describe this new standard as well as any program that supported the standard. The IETF accepted the proposal and started the OpenPGP Working Group. OpenPGP is on the Internet Standards Track; the current specification is RFC 2440 (July 1998). OpenPGP is still under active development and a follow-on to RFC 2440 was being actively finalized by the OpenPGP working group in 2006.

http://en.wikipedia.org/wiki/OpenPGP#OpenPGP

2.728.3 (FR) OPENPGP

OpenPGP est une norme de cryptographie de l'IETF, normalisée dans la RFC 2440.

Cette norme décrit le format des messages, signatures ou clés que peuvent s'envoyer des programmes comme GnuPG. Ce n'est donc pas un programme, mais une recommandation pour l'échange sécurisé de données, qui doit son nom au programme historique PGP.

http://fr.wikipedia.org/wiki/OpenPGP

2.729 OPERACIONES EN REDES DE ORDENADORES

2.729.1 OPERACIONES EN REDES DE ORDENADORES

Un término amplio que se emplea tanto en el ámbito militar como en el ámbito civil para referirse a actividades orientadas a aprovechar y optimizar las redes de ordenadores en beneficio de los individuos o las organizaciones empresariales o gubernamentales, incluyendo escenarios de ciberguerra, buscando la superioridad propia así como reducir o eliminar las oportunidades del oponente.

Se puede hablar de tres variantes:

- CNA (Computer Network Attack): Ataques desarrollados sobre la red para interrumpir , inhabilitar, degradar o destruir la información y los servicios de la parte contraria.
- CND (Computer Network Defense): Acciones defensivas sobre la red para proteger, monitorizar, analizar, detectar y responder a ataques en red. intrusiones, disrupciones u otras actividades no autorizadas sobre nuestros sistemas y nuestras redes.
- CNE (Computer Network Exploitation): Incluye acciones oerativas y recopilación de información (inteligencia) a través de las redes que aprovechan información extraída de la parte contraria.

https://en.wikipedia.org/wiki/Computer_network_operations

2.729.2 (EN) COMPUTER NETWORK OPERATIONS (CNO)

Computer Network Operations (CNO) is a broad term that has both military and civilian application. Conventional wisdom is that information is power, and more and more of the information necessary to make decisions is digitized and conveyed over an ever expanding network of computers and other electronic devices. Computer network operations are deliberate actions taken to leverage and optimize these networks to improve human endeavor and enterprise or, in warfare, to gain information superiority and deny the enemy this enabling capability.

According to Joint Pub 3-13, CNO consists of computer network attack (CNA), computer network defense (CND) and computer network exploitation (CNE) :

- Computer Network Attack (CNA): Includes actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves.
- Computer Network Defense (CND): Includes actions taken via computer networks to protect, monitor, analyze, detect and respond to network attacks, intrusions, disruptions or other unauthorized actions that would compromise or cripple defense information systems

and networks. Joint Pub 6.0 further outlines Computer Network Defense as an aspect of NetOps:

- Computer Network Exploitation (CNE): Includes enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks.

https://en.wikipedia.org/wiki/Computer_network_operations

2.730 OPERADOR

Ver:

- *Administrador*

2.730.1 OPERADOR

Persona responsable de la operación rutinaria de los componentes de un sistema de información.

2.730.2 (EN) OPERATOR

(I) A person who has been authorized to direct selected functions of a system. (Compare: manager, user.) [RFC4949:2007]

2.730.3 (EN) OPERATOR

Person in charge of routine operation of the components of an information system.

2.731 OPT IN

Ver:

- *Opt out*
- *Spam*

2.731.1 OPT IN

El receptor de mensajes publicitarios sólo recibirá dichos mensajes previo consentimiento expreso.

2.731.2 OPT-IN

Envío de mensajes con fines comerciales a una lista de correo electrónico constituida por usuarios de Internet que han otorgado consentimiento previo a la recepción de dichos mensajes por el hecho de tener interés en recibir información publicitaria de determinados bienes, servicios o productos. Con este mecanismo el internauta notifica a una empresa, institución u organización que desea recibir vía correo electrónico información relacionada con los servicios que proporciona.

http://www.inteco.es/glossary/Formacion/Glosario/

2.731.3 (EN) OPT IN

Allowing unsolicited communication for purposes of direct marketing only with the consent of the subscriber.

http://www.enisa.europa.eu/

2.732 OPTIONAL

Ver:

- http://www.ietf.org/rfc/rfc2119

2.732.1 (EN) MAY

This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

2.733 OPT OUT

Ver:

- *Opt in*
- *Spam*

2.733.1 OPT OUT

El receptor de mensajes publicitarios recibirá dichos mensajes salvo que exprese explícitamente su deseo de ser excluido.

2.733.2 OPT-OUT

Envío de mensajes con fines comerciales a una lista de correo electrónico constituida por usuarios de Internet los cuales no han dado previa autorización o acuerdo explícito para la recepción de tales mensajes, pero que disponen de la posibilidad de retirarse de la lista de distribución en la cual están incluidos. Este proceso es utilizado también para darse de baja de forma voluntaria en foros, listas de distribución, boletines electrónicos de los que ya no se desea recibir más información y evitar que los datos de carácter personal puedan ser tratados por terceros sin consentimiento del titular de los mismos.

http://www.inteco.es/glossary/Formacion/Glosario/

2.733.3 (EN) OPT OUT

Allowing unsolicited communication for purposes of direct marketing unless the subscriber expressed the wish to not receive these communications.

http://www.enisa.europa.eu/

2.734 ORGANISMO DE CERTIFICACIÓN

Ver:

- *Certificación*

2.734.1 INSTITUCIÓN DE CERTIFICACIÓN

Organización nacional independiente e imparcial que emite las certificaciones de seguridad (ITSEC).

Realmente el ITSEC confiere más atribuciones a esta Institución, como supervisar el proceso de evaluación, otorgar las acreditaciones para realizar las evaluaciones, etc.

[Ribagorda:1997]

2.734.2 (EN) CERTIFICATION BODY

an independent and impartial national organisation that performs certification. [ITSEC:1991]

2.735 ORIGEN DE AUTORIDAD

Acrónimos: SOA

2.735.1 ORIGEN DE AUTORIDAD

A la hora de asignar una serie de privilegios, aquella fuente de información y de confianza que tiene la última palabra.

2.735.2 FUENTE DE AUTORIDAD

Autoridad de atributo en la que confía un verificador de privilegios para un recurso determinado como la autoridad última en asignar un conjunto de privilegios [X.509:2005]

2.735.3 (EN) SOURCE OF AUTHORITY

A SOA is an Attribute Authority that a privilege verifier for a particular resource trusts as the ultimate authority to assign a set of privileges. [X.509:2005]

2.735.4 (FR) SOURCE D'AUTORITÉ

autorité d'attribut auquel peut faire confiance un vérificateur de privilège pour une ressource donnée, en tant qu'autorité ultime pour l'attribution d'un ensemble de privilèges. [X.509:2005]

2.736 ORIGEN DE CONFIANZA

Ver:

- *Confianza*

2.736.1 ORIGEN DE CONFIANZA

Para validar el primer certificado de una cadena de certificados se necesita conocer una autoridad de certificación y su clave pública. A partir de esa clave pública se van validando los sucesivos certificados de la cadena. La validez del proceso descansa sobre la confianza en el primer certificado. Es frecuente que el primer certificado sea auto-firmado.

2.736.2 ANCLA DE CONFIANZA

Se trata de un conjunto de la siguiente información adicional a la clave pública: identificador de algoritmo, parámetros de clave pública (si se aplican), nombre distinguido del titular de la clave privada asociada (es decir, la autoridad de certificación sujeto) y facultativamente un periodo de validez. El ancla de confianza puede presentarse en la forma de un certificado autofirmado. Un sistema que utiliza un certificado puede confiar en un ancla de confianza y puede aplicarla para validar certificados en los trayectos de certificación. [X.509:2005]

2.736.3 (EN) TRUST ANCHOR

An established point of trust (usually based on the authority of some person, office, or organization) from which an entity begins the validation of an authorized process or authorized (signed) package. A "trust anchor" is sometimes defined as just a public key used for different purposes (e.g., validating a Certification Authority, validating a signed software package or key, validating the process (or person) loading the signed software or key). [CNSSI_4009:2010]

2.736.4 (EN) TRUST ANCHOR

A public key and the name of a certification authority that is used to validate the first certificate in a sequence of certificates. The trust anchor public key is used to verify the signature on a certificate issued by a trust anchor certification authority. The security of the validation process depends upon the authenticity and integrity of the trust anchor. Trust anchors are often distributed as self-signed certificates. [NIST-SP800-57:2007]

2.736.5 (EN) TRUST ANCHOR

trusted information, which includes a public key algorithm, a public key value, an issuer name, and optionally, other parameters.

NOTE 1. Other parameters may include but are not limited to a validity period.

NOTE 2. A trust anchor may be provided in the form of a self-signed certificate.

[ISO-19790:2006]

2.736.6 (EN) TRUST ANCHOR

A trust anchor is a set of the following information in addition to the public key: algorithm identifier, public key parameters (if applicable), distinguished name of the holder of the associated private key (i.e., the subject CA) and optionally a validity period. The trust anchor may be provided in the form of a self-signed certificate. A trust anchor is trusted by a certificate using system and used for validating certificates in certification paths. [X.509:2005]

2.736.7 (FR) ANCRE DE CONFIANCE

une ancre de confiance se compose de l'ensemble des informations dont la liste figure ci-après, outre la clé publique: identificateur d'algorithme, paramètres de clé publique (le cas échéant), nom distinctif du détenteur de la clé publique associée (c'est-à-dire autorité de certification sujet) et à titre optionnel période de validité. L'ancre de confiance peut être fournie sous la forme d'un certificat autosigné. Un système utilisant des certificats se fie à une ancre de confiance; celle-ci permet de valider des certificats sur des itinéraires de certification. [X.509:2005]

2.737 PADDING

Ver:

- *Rellenado de tráfico*

2.737.1 PADDING

Relleno de datos con bits adicionales.

2.737.2 (EN) PADDING

Appending extra bits to a data string. [ISO-10118-1:2000]

2.738 PAP - PASSWORD AUTHENTICATION PROTOCOL

Acrónimos: PAP

Ver:

- *Contraseña*
- *CHAP - Challenge-Handshake Authentication Protocol*
- http://www.ietf.org/rfc/rfc1334

2.738.1 PAP - PASSWORD AUTHENTICATION PROTOCOL

protocolo simple de autenticación para autenticar un usuario contra un servidor de acceso remoto o contra un ISP. PAP es un sub-protocolo usado por la autenticación del protocolo PPP (Point to Point Protocol), validando a un usuario que accede a ciertos recursos. PAP transmite contraseñas o password en ASCII sin cifrar, por lo que se considera inseguro. PAP se usa como último recurso cuando el servidor de acceso remoto no soporta un protocolo de autenticación más fuerte.

http://es.wikipedia.org/wiki/PAP

2.738.2 (EN) PASSWORD AUTHENTICATION PROTOCOL (PAP)

(I) A simple authentication mechanism in PPP. In PAP, a user identifier and password are transmitted in cleartext form. [R1334] (See: CHAP.) [RFC4949:2007]

2.738.3 (EN) PASSWORD AUTHENTICATION PROTOCOL - PAP

an authentication protocol provided for PPP (RFC 1334). [ISO-18028-4:2005]

2.738.4 (EN) PAP (PASSWORD AUTHENTICATION PROTOCOL)

An identity verification method used to send a user name and password over a network to a computer that compares the user name and password to a table listing authorized users. WatchGuard products do not support this authentication method because the user name and password travel as clear text that a hacker could read.

http://www.watchguard.com/glossary/

2.738.5 (EN) PAP - PASSWORD AUTHENTICATION PROTOCOL

Password Authentication Protocol is a simple, weak authentication mechanism where a user enters the password and it is then sent across the network, usually in the clear.

http://www.sans.org/security-resources/glossary-of-terms/

2.738.6 (FR) PAP - PASSWORD AUTHENTICATION PROTOCOL

PAP est un protocole élémentaire d'authentification d'un client par un serveur basée sur la connaissance d'un secret commun (ex.: le mot de passe du client). PAP se déroule en deux phases:

- Le client émet périodiquement son couple identifiant/mot de passe au serveur.
- Le serveur, une fois vérifié la conformité du couple identiant/mot de passe du client, lui émet un message de succès d'authentification.

PAP ne fournit pas de mécanisme d'anti-rejeu.

PAP véhicule l'identifiant et le mot de passe du client en clair sur le réseau de transport.

http://securit.free.fr/glossaire.htm

2.739 PARÁMETRO SECRETO

2.739.1 PARÁMETRO SECRETO

entrada aleatoria con la que se inicializa un generador de números aleatorios a fin de aumentar la entropía del sistema.

2.739.2 PARÁMETRO SECRETO

información que no es de dominio público, sino exclusivamente conocida por el aspirante.

2.739.3 (EN) SECRET PARAMETER

input to the RBG during initialisation. It provides additional entropy in the case of an entropy source failure or compromise. [ISO-18031:2005]

2.739.4 (EN) SECRET PARAMETER

number or bit string that does not appear in the public domain, only used by a claimant, e.g., a private number [ISO-9798-5:2004]

2.740 PARÁMETRO VARIANTE EN EL TIEMPO

Ver:

- *Autenticación*
- *Ataques de reproducción*
- *Nonce*
- *Sello de tiempo*

2.740.1 PARÁMETRO VARIANTE EN EL TIEMPO

Datos incluidos en la información de autenticación para prevenir la repetición ilícita de mensajes previamente emitidos. Algunos tipos permiten también detectar demoras en los mensajes forzadas por un atacante.

Los tres tipos de parámetros son estampilla de tiempo, números secuenciales y números aleatorios.

[Ribagorda:1997]

2.740.2 (EN) TIME VARIANT PARAMETER

A random or pseudorandom value that is never intentionally repeated during the cryptoperiod of the corresponding key. [x926].

http://www.garlic.com/~lynn/x9fgloss.htm

2.741 PAR ASIMÉTRICO DE CLAVES

Ver:

- *Criptografía de clave pública*
- *Par de claves*
- *Clave privada*
- *Clave pública*

2.741.1 PAR DE CLAVES ASIMÉTRICAS

Par de claves criptográficas, en cierto sentido recíprocas, en la que una de ellas, llamada pública, define el algoritmo de cifra (de uso público) y la otra, denominada privada, especifica el algoritmo de descifrado (de uso privado) (ISO/IEC ISO-11770-3). [Ribagorda:1997]

2.741.2 (EN) ASYMMETRIC KEY

(I) A cryptographic key that is used in an asymmetric cryptographic algorithm. (See: asymmetric cryptography, private key, public key.) [RFC4949:2007]

2.741.3 (EN) ASYMMETRIC KEY PAIR

pair of related keys where the private key defines the private transformation and the public key defines the public transformation [ISO/IEC ISO-9798-1:1997]. [ISO-18033-1:2005]

2.741.4 (EN) ASYMMETRIC PAIR

Two related data items, keys or numbers, where the private data item defines a private operation and the public data item defines a public operation [ISO-9798-5:2004]

2.741.5 (EN) ASYMMETRIC KEY PAIR

A pair of related keys where the private key defines the private transformation and the public key defines the public transformation. [ISO-11770-3:2008]

2.741.6 (EN) ASYMMETRIC KEY PAIR

pair of related keys where the private key defines the private transformation and the public key defines the public transformation. [ISO-9798-1:1997]

2.742 PAR DE CLAVES

Ver:

- *Clave*
- *Clave criptográfica*
- *Par asimétrico de claves*

2.742.1 PAR DE CLAVES

En criptografía pública, la pareja formada por una clave pública y su correspondiente clave privada.

2.742.1 (EN) KEY PAIR

A public key and its corresponding private key; a key pair is used with a public key algorithm. [CNSSI_4009:2010]

2.742.2 (EN) KEY PAIR

(I) A set of mathematically related keys -- a public key and a private key -- that are used for asymmetric cryptography and are generated in a way that makes it computationally infeasible to derive the private key from knowledge of the public key. (See: Diffie-Hellman-Merkle, RSA.) [RFC4949:2007]

2.742.3 (EN) KEY PAIR

A public key and its corresponding private key; a key pair is used with a public key algorithm. [NIST-SP800-57:2007]

2.742.4 (FR) BI-CLÉS

Clé publique et sa clé privée créées par et utilisées avec un système cryptographique asymétrique. [ISO-11568-4:2007]

2.742.5 (FR) BI-CLÉS

On distingue en général plusieurs natures de bi-clés:

- Bi-clés de confidentialité, utilisés pour chiffrer des messages de petite taille.
- Bi-clés de signature, dont la clé privée est utilisée pour signer les messages et la clé publique pour vérifier les signatures.
- Bi-clés de certification, utilisés par l'autorité de certification pour signer des certificats ou des messages de révocation.
- Bi-clés d'échange/transport de clés, utilisés pour le transport de clés symétriques servant à sécuriser les communications.

http://securit.free.fr/glossaire.htm

2.743 PARTE QUE SE FÍA

Ver:

- *Certificado de clave pública*

2.743.1 PARTE CONFIANTE

Usuario o agente que se fía de los datos de un certificado al tomar decisiones. [X.509:2005]

2.743.2 (EN) RELYING PARTY

An entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system. [CNSSI_4009:2010]

2.743.3 (EN) RELYING PARTY

A user or agent that relies on the data in a certificate in making decisions. [X.509:2005]

2.743.4 (FR) PARTICIPANT FAISANT CONFIANCE

utilisateur ou agent qui fait confiance aux données contenues dans un certificat pour prendre des décisions. [X.509:2005]

2.744 PASARELA

Ver:

- *Cortafuegos*
- *Proxy (agente)*

2.744.1 PASARELA

En una red, el punto de acceso a otra red.

2.744.1 (EN) GATEWAY

Interface providing a compatibility between networks by converting transmission speeds, protocols, codes, or security measures. [CNSSI_4009:2010]

2.744.2 (EN) GATEWAY

(I) An intermediate system (interface, relay) that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables either one-way or two- way communication between the networks. (See: bridge, firewall, guard, internetwork, proxy server, router, and subnetwork.) [RFC4949:2007]

2.744.3 (EN) GATEWAY

A point on a network that acts as an entrance to another network.

2.745 PASARELA DE SEGURIDAD

Ver:

- *Protección del perímetro*
- *Guardia*
- *Dispositivo de protección perimetral*
- *Cortafuegos*
- *Air gap*

2.745.1 PASARELA DE SEGURIDAD

Pasarela entre redes que implementan diferentes políticas de seguridad.

2.745.2 (EN) SECURITY GATEWAY

1. (I) An internetwork gateway that separates trusted (or relatively more trusted) hosts on one side from untrusted (or less trusted) hosts on the other side. (See: firewall and guard.)

2. (O) /IPsec/ "An intermediate system that implements IPsec protocols." [R4301]

[RFC4949:2007]

2.745.3 (EN) SECURITY GATEWAY

A security gateway is a point of connection between networks, or between subgroups within networks, or between software applications within different security domains intended to protect a network according to a given security policy. A security gateway comprises more than only firewalls; the term includes routers and switches which provide the functionality of access control and encryption. [ISO-18028-3:2005]

2.745.4 (EN) CLOUD SECURITY GATEWAYS

Cloud security gateways are on-premises or cloud-based security policy enforcement points placed between cloud service consumers and cloud service providers to interject enterprise security policies as the cloud-based resources are accessed. Cloud security gateways consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, security token mapping, encryption, tokenization, logging, alerting, API control and so on.

http://www.gartner.com/it-glossary/

2.745.5 (EN) CLOUD ENCRYPTION GATEWAY

Cloud encryption gateways provide cloud security proxy (typically at the application level), which performs encryption, tokenization or both on an item-by-item basis as data flows through the proxy. The obfuscated (encrypted or tokenized) data can then be stored in a cloud-based software-as-a-service (SaaS) application, such as salesforce.com. Cloud encryption gateways typically provide a choice of various encryption and tokenization algorithms, depending on the strength of protection required and how much format preservation is necessary (for example, to preserve sorting).

http://www.gartner.com/it-glossary/

2.746 PATRÓN DE UN ATAQUE

Ver:

- *Ataque*
- *Sistema de detección de intrusiones*

2.746.1 PATRÓN DE UN ATAQUE

Secuencia de actividades o alteraciones que utilizan los IDS para descubrir que un ataque ha ocurrido. Los datos se extraen de los registros de tráfico en la red o de los registros de actividad de los equipos.

2.746.2 (EN) ATTACK SIGNATURE

A characteristic byte pattern used in malicious code or an indicator, or set of indicators that allows the identification of malicious network activities. [CNSSI_4009:2010]

2.746.3 (EN) ATTACK SIGNATURE

A sequence of computer activities or alterations that are used to execute an attack and which are also used by an IDS to discover that an attack has occurred and often is determined by the examination of network traffic or host logs. This may also be referred to as an attack pattern. [ISO-18043:2006]

2.746.4 (EN) ATTACK SIGNATURE DETECTION

Detects patterns corresponding to know attacks. This includes both passive protocol analysis (use of sniffers in promiscuous mode) and signature analysis (interpretation of a specific series of packets or price of data contained in those packets, that represent a know pattern of attack).

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.746.5 (EN) ATTACK SIGNATURE

The features of network traffic, either in the heading of a packet or in the pattern of a group of packets, which distinguish attacks from legitimate traffic.

http://www.symantec.com/avcenter/refa.html

2.747 PCI DSS

Ver:

- https://www.pcisecuritystandards.org/index.php

2.747.1 PCI DSS

Las Normas de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y para facilitar la adopción de medidas de seguridad consistentes a nivel mundial. Las PCI DSS proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas. Las PCI DSS se aplican a todas las entidades que participan en los procesos de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios, así como también todas las demás entidades que almacenan, procesan o transmiten datos de titulares de tarjetas. Las PCI DSS constituyen un conjunto mínimo de requisitos para proteger datos de titulares de tarjetas y se pueden mejorar con el uso de controles y prácticas adicionales para mitigar otros riesgos.

https://www.pcisecuritystandards.org/index.php

2.747.2 (EN) PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

https://www.pcisecuritystandards.org/index.php

2.747.3 (EN) PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. The PCI DSS was created jointly in 2004 by four major credit-card companies: Visa, MasterCard, Discover and American Express.

http://whatis.techtarget.com/

2.747.4 (FR) PCI DSS

La norme PCI (Payment Card Industry) DSS (Data Security Standard) a été développée dans le but de renforcer la sécurité des données des titulaires de cartes et de faciliter l'adoption de mesures de sécurité uniformes à l’échelle mondiale. La norme PCI DSS sert de référence aux conditions techniques et opérationnelles conçues pour protéger les données des titulaires de cartes. La norme PCI DSS s'applique à toutes les entités impliquées dans le traitement des cartes de paiement, notamment les commerçants, les entreprises de traitement, acquéreurs, émetteurs et prestataires de service, ainsi que toutes les autres entités qui stockent, traitent ou transmettent des données de titulaires de cartes. La norme PCI DSS consiste en un ensemble de conditions minimum pour la

protection des données de titulaires de cartes et peut être renforcée de contrôles et pratiques supplémentaires pour réduire encore davantage les risques.

https://www.pcisecuritystandards.org/index.php

2.748 PEAP - PROTECTED EXTENSIBLE AUTHENTICATION PROTOCOL

Acrónimos: PEAP

Ver:

- *Extensible Authentication Protocol*

2.748.1 PEAP - PROTECTED EXTENSIBLE AUTHENTICATION PROTOCOL

Protocolo del tipo EAP desarrollado conjuntamente por Microsoft, RSA Security y Cisco para la transmisión datos autenticados, incluso claves, sobre redes inalámbricas 802.11. Autentica clientes de red wi-fi empleando sólo certificados del lado servidor creando una túnel SSL/TLS entre el cliente y el servidor de autenticación. El túnel luego protege el resto de intercambios de autenticación de usuario.

2.748.2 (EN) PEAP - PROTECTED EXTENSIBLE AUTHENTICATION PROTOCOL

a method to securely transmit authentication information, including passwords, over wired or wireless networks. It was jointly developed by Cisco Systems, Microsoft, and RSA Security. Note that PEAP is not an encryption protocol; as with other EAP types it only authenticates a client into a network.

PEAP uses only server-side public key certificates to authenticate clients by creating an encrypted SSL/TLS tunnel between the client and the authentication server. The ensuing exchange of authentication information is then encrypted and user credentials are safe from eavesdropping.

PEAP is a joint proposal by Cisco Systems, Microsoft and RSA Security as an open standard. It is already widely available in products, and provides very good security. It is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication.

http://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol

2.749 PELIGRO

Ver

- *Riesgo*

2.749.1 PELIGRO

1. m. Riesgo o contingencia inminente de que suceda algún mal.

DRAE. Diccionario de la Lengua Española.

2.749.2 (EN) HAZARD

natural or man-made source or cause of harm or difficulty

Annotation:

1) A hazard differs from a threat in that a threat is directed at an entity, asset, system, network, or geographic area, while a hazard is not directed.
2) A hazard can be actual or potential.

DHS Risk Lexicon, September 2008

2.749.3 (EN) ACCIDENTAL HAZARD

source of harm or difficulty created by negligence, error, or unintended failure

DHS Risk Lexicon, September 2008

2.749.4 (EN) INTENTIONAL HAZARD

source of harm, duress, or difficulty created by a deliberate action or a planned course of action

DHS Risk Lexicon, September 2008

2.749.5 (EN) NATURAL HAZARD

source of harm or difficulty created by a meteorological, environmental, or geological phenomenon or combination of phenomen

DHS Risk Lexicon, September 2008

2.750 PEM - PRIVACY ENHANCED MAIL

Acrónimos: PEM

Ver:

- http://www.ietf.org/rfc/rfc1421
- http://www.ietf.org/rfc/rfc1422
- http://www.ietf.org/rfc/rfc1423
- http://www.ietf.org/rfc/rfc1424
- *CMS - Cryptographic Message Syntax*
- *PGP - Pretty Good Privacy*
- *S/MIME - Secure Multipurpose Mail Extension*

2.750.1 PEM

Conjunto de protocolos estándares adoptados por el Internet Architecture Board (IAB), para proporcionar seguridad al correo electrónico sobre Internet. Los protocolos PEM se emplean para cifrado, autenticación, integridad y gestión de claves. [CESID:1997]

2.750.2 (EN) PRIVACY ENHANCED MAIL (PEM)

(I) An Internet protocol to provide data confidentiality, data integrity, and data origin authentication for electronic mail. [R1421, R1422]. (Compare: DKIM, MOSS, MSP, PGP, S/MIME.) [RFC4949:2007]

2.751 PENETRACIÓN

Ver:

- *Intrusión*
- *Pruebas de penetración*

2.751.1 PENETRACIÓN

Violación de un sistema de seguridad, lo que permite acceder a los recursos supuestamente protegidos. [Ribagorda:1997]

2.751.2 PENETRACIÓN

Violación de un sistema de información protegido. [CESID:1997]

2.751.3 (EN) PENETRATE

1a. (I) Circumvent a system's security protections. (See: attack, break, violation.)

1b. (I) Successfully and repeatedly gain unauthorized access to a protected system resource. [Huff]

[RFC4949:2007]

2.751.4 (EN) PENETRATION

Gaining unauthorized logical access to sensitive data by circumventing a system's protections.

http://www.sans.org/security-resources/glossary-of-terms/

2.752 PERFECT FORWARD SECRECY

Acrónimos: PFS

Ver:

- *Public-key forward secrecy*
- http://www.ietf.org/rfc/rfc4306

2.752.1 PERFECT FORWARD SECRECY

Propiedad de un sistema de cifra que nos garantiza que las claves usadas hoy no se verán descubiertas si el día de mañana se revela alguna información secreta relacionada con dichas claves.

2.752.2 (EN) PERFECT FORWARD SECRECY

(I) For a key agreement protocol, the property that compromises long-term keying material does not compromise session keys that were previously derived from the long-term material. (Compare: public-key forward secrecy.) [RFC4949:2007]

2.752.3 (EN) FORWARD SECRECY WITH RESPECT TO A

the property that knowledge of As long-term private key subsequent to a key agreement operation does not enable an opponent to recompute previously derived keys. [ISO-15946-3:2002]

2.752.4 (EN) FORWARD SECRECY WITH RESPECT TO BOTH A AND B INDIVIDUALLY

the property that knowledge of As long-term private key or knowledge of Bs long-term private key subsequent to a key agreement operation does not enable an opponent to recompute previously derived keys. [ISO-15946-3:2002]

2.752.5 (EN) MUTUAL FORWARD SECRECY

the property that knowledge of both As and Bs long-term private keys subsequent to a key agreement operation does not enable an opponent to recompute previously derived keys. [ISO-15946-3:2002]

2.752.6 (EN) PERFECT FORWARD SECRECY (PFS)

A cryptosystem in which, if one encryption key is compromised, only the data encrypted by that specific key is compromised. Some cryptosystems allow keys to be derived from previous keys, so that if the first key is compromised, an attacker might have enough information to figure out other keys and/or decrypt data encrypted using those keys.

http://www.watchguard.com/glossary/

2.753 PERFILADO

Ver:

- *Anonimato*

2.753.1 PERFILADO

Uso del conocimiento que se tiene de las actividades de un cliente para derivar un patrón que permita anticipar su comportamiento en el futuro.

Es interesante para centrar acciones de marketing hacia aquellos sujetos más proclives a responder positivamente.

2.753.2 (EN) INDIVIDUAL PROFILING

Refers to a site's or a service provider's use of personal data to create or build a record on the particular individual or computer for the purpose of compiling habits or personally identifiable information of that individual or computer. For example, online stores may recommend products based on the visitor's purchasing history on the specific Web site or online in general.

http://www.consumerprivacyguide.org/glossary/

2.754 PERFIL DE PROTECCIÓN

Acrónimos: PP (es), PP

Ver:

- *Criterios comunes*
- http://en.wikipedia.org/wiki/Protection_Profile

2.754.1 PERFIL DE PROTECCIÓN

Conjunto de requisitos de seguridad, independiente de la implementación, para un tipo de TOE.

TOE - Target of Evaluation

[CC:2006]

2.754.2 (EN) PROTECTION PROFILE (PP)

an implementation-independent statement of security needs for a TOE type.

TOE - Target of Evaluation

[CC:2006]

2.755 PERÍMETRO DE SEGURIDAD

Ver:

- *Personal interno*
- *Agente externo*

2.755.1 PERÍMETRO DE SEGURIDAD

Frontera física o lógica que define un dominio de seguridad o zona en la que se aplica una determinada política de seguridad o se ha implantado una determinada arquitectura de seguridad.

2.755.2 (EN) ELECTRONIC SECURITY PERIMETER (ESP)

An Electronic Security Perimeter (ESP) refers to the demarcation point between a secured enclave. such as a control system. and a less trusted network. such as a business network. The ESP typically includes those devices that secure that demarcation point. including firewalls. IDS. IPS. industrial protocol filters. application monitors. and similar devices. [knapp:2014]

2.755.3 (EN) ELECTRONIC SECURITY PERIMETER (ESP)

The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol. [NERC:2014]

2.755.4 (EN) EXTERNAL ROUTABLE CONNECTIVITY

The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection. [NERC:2014]

2.755.5 (EN) PHYSICAL SECURITY PERIMETER

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled. [NERC:2014]

2.755.6 (EN) SECURITY PERIMETER

A physical or logical boundary that is defined for a system, domain, or enclave; within which a particular security policy or security architecture is applied. [CNSSI_4009:2010]

2.755.7 (EN) SECURITY PERIMETER

(I) A physical or logical boundary that is defined for a domain or enclave and within which a particular security policy or security architecture applies. (See: insider, outsider.) [RFC4949:2007]

2.756 PERIODO DE CIFRADO

2.756.1 PERÍODO DE CIFRADO

Lapso de tiempo durante el cual se puede utilizar una clave criptográfica para su propósito definido basándose en, por ejemplo, un período de tiempo definido y/o la cantidad de texto cifrado producido, y según las mejores prácticas y directrices de la industria (por ejemplo, la Publicación especial 800-57 del NIST).

http://es.pcisecuritystandards.org/

2.756.2 (EN) CRYPTOPERIOD

The time span during which a specific cryptographic key can be used for its defined purpose based on, for example, a defined period of time and/or the amount of cipher-text that has been produced, and according to industry best practices and guidelines (for example, NIST Special Publication 800-57).

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.756.3 (FR) CRYPTOPÉRIODE

Durée pendant laquelle une clé cryptographique spécifique peut être utilisée selon l'objectif défini, par exemple, par une période définie et/ou la quantité de texte chiffré produite, conformément aux directives et aux meilleures pratiques du secteur (par exemple, la publication spéciale NIST 800-57).

http://fr.pcisecuritystandards.org/

2.757 PER - PACKET ENCODING RULES

Acrónimos: PER

Ver:

- *ASN.1 - Abstract Syntax Notation One*
- *BER - Basic Encoding Rules*
- *CER - Canonical Encoding Rules*
- *DER - Distinguished Encoding Rules*
- *XER - XML Encoding Rules*

2.757.1 PER - PACKET ENCODING RULES

Conjunto de reglas para formatear en binario datos descritos en ASN.1.

2.757.2 (EN) PER - PACKET ENCODING RULES

a set of ASN.1 encoding rules for formatting data in binary.

http://en.wikipedia.org/wiki/Packed_Encoding_Rules

2.758 PERSONAL INTERNO

Ver:

- *Perímetro de seguridad*
- *Agente externo*

2.758.1 PERSONAL INTERNO

Personas con acceso al sistema desde dentro del perímetro de seguridad. Es decir, con cierta autorización para el acceso.

2.758.2 (EN) INSIDER

1. (I) A user (usually a person) that accesses a system from a position that is inside the system's security perimeter. (Compare: authorized user, outsider, unauthorized user.)

2. (O) A person with authorized physical access to the system. Example: In this sense, an office janitor is an insider, but a burglar or casual visitor is not. [NRC98]

3. (O) A person with an organizational status that causes the system or members of the organization to view access requests as being authorized. Example: In this sense, a purchasing agent is an insider but a vendor is not. [NRC98]

[RFC4949:2007]

2.759 PGP - PRETTY GOOD PRIVACY

Acrónimos: PGP

Ver:

- http://www.pgp.com/
- *GPG - GNU Privacy Guard*
- *OpenPGP - Open Pretty Good Privacy*
- http://www.ietf.org/rfc/rfc1991
- http://www.ietf.org/rfc/rfc2440

2.759.1 PGP

Programa de seguridad para correo electrónico diseñado por P. Zimmermann. [CESID:1997]

2.759.2 PRETTY GOOD PRIVACY

Pretty Good Privacy o PGP (privacidad bastante buena) es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

PGP originalmente fue diseñado y desarrollado por Phil Zimmermann en 1991. El nombre está inspirado en el del colmado Ralph's Pretty Good Grocery de Lake Wobegon, una ciudad ficticia inventada por el locutor de radio Garrison Keillor.

http://es.wikipedia.org/wiki/PGP

2.759.3 (EN) PRETTY GOOD PRIVACY

PGP a publicly available encryption software program based on public key cryptography. The message formats are specified in RFC 1991 and RFC 2440. [ISO-18028-4:2005]

2.759.4 (EN) PGP - PRETTY GOOD PRIVACY

Computer program (and related protocols) that uses cryptography to provide data security for electronic mail and other applications on the Internet.

2.759.5 (EN) PRETTY GOOD PRIVACY

PGP Encryption (Pretty Good Privacy) is a computer program that provides cryptographic privacy and authentication. It was originally created by Philip Zimmermann in 1991. PGP and other similar products follow the OpenPGP standard (RFC 2440) for encrypting and decrypting data.

http://en.wikipedia.org/wiki/Pretty_Good_Privacy

2.759.6 (FR) PRETTY GOOD PRIVACY

Le logiciel Pretty Good Privacy (ou PGP) est un logiciel de communication électronique sécurisée utilisant la cryptographie asymétrique mais également la cryptographie symétrique. Il fait donc partie des logiciels de cryptographie hybride.

Philip Zimmermann, son développeur, a mis PGP en libre téléchargement en 1991. Violant de façon subtile les restrictions à l'exportation pour les produits cryptographiques (il avait été placé sur un site américain d'où il était possible de le charger depuis n'importe où), PGP a été très mal accueilli par le gouvernement américain qui a ouvert une enquête en 1993 -- abandonnée en 1996, sans donner de raison.

http://fr.wikipedia.org/wiki/PGP

2.760 PHARMING

Ver:

- *Envenenamiento del DNS*
- *Secuestro de DNS*
- *Suplantación de DNS*
- *Extensiones de seguridad para el DNS*

2.760.1 PHARMING

Ataque informático que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad (comúnmente una entidad bancaria) de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a otra dirección IP donde se aloja una web falsa que suplantará la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes la entidad.

http://www.inteco.es/glossary/Formacion/Glosario/

2.760.2 PHARMING

Redirecciona malintencionadamente al usuario a un sitio web falso y fraudulento, mediante la explotación del sistema DNS, se denomina secuestro o envenenamiento del DNS.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.760.3 (EN) PHARMING

An attack in which an Attacker corrupts an infrastructure service such as DNS (Domain Name Service) causing the Subscriber to be misdirected to a forged Verifier/RP, which could cause the Subscriber to reveal sensitive information, download harmful software or contribute to a fraudulent act. [NIST-SP800-63:2013]

2.760.4 (EN) PHARMING

A form of domain name spoofing that results in users believing they are on a genuine site with the correct URL only to be diverted to a scam site.

http://www.enisa.europa.eu/

2.760.5 (EN) PHARMING

An exploit in which criminals disrupt the normal functioning of DNS software which translates Internet domain names into addresses. The user enters a correct address but is redirected to a fake website.

http://www.getsafeonline.org/

2.760.6 (EN) PHARMING

This is a more sophisticated form of MITM attack. A users session is redirected to a masquerading website. This can be achieved by corrupting a DNS server on the Internet and pointing a URL to the masquerading websites IP. Almost all users use a URL like www.worldbank.com instead of the real IP (192.86.99.140) of the website. Changing the pointers on a DNS server, the URL can be redirected to send traffic to the IP of the pseudo website. At the pseudo website, transactions can be mimicked and information like login credentials can be gathered. With this the attacker can access the real www.worldbank.com site and conduct transactions using the credentials of a valid user on that website.

http://www.sans.org/security-resources/glossary-of-terms/

2.760.7 (EN) PHARMING

A type of phishing attack that involves "DNS poisoning" - malicious code that alters victims' Domain Name Server (DNS), so that they are automatically directed to a fraudulent website when they type in the address of a legitimate site. Pharming attacks are much more difficult to detect than traditional phishing attacks, since victims will still see the URL of the legitimate website when they are actually at the fraudulent site. However, it is also an extremely complicated attack technique, and security experts have noted few examples of it "in the wild."

2.760.8 (EN) PHARMING

A pharming attack occurs when the victim is fooled into entering sensitive data into supposedly trusted locations, such as an online bank site or a trading platform. An attacker can impersonate these supposedly trusted sites and have the victim be directed to his site rather than the originally intended one. Pharming does not require script injection or clicking on malicious links for the attack to succeed.

Attack Execution Flow

- Attacker sets up a system mocking the one trusted by the users. This is usually a website that requires or handles sensitive information.
- The attacker then poisons the resolver for the targeted site. This is achieved by poisoning the DNS server, or the local hosts file, that directs the user to the original website
- When the victim requests the URL for the site, the poisoned records direct the victim to the attacker's system rather than the original one.
- Because of the identical nature of the original site and the attacker controlled one, and the fact that the URL is still the original one, the victim trusts the website reached and the attacker can now "farm" sensitive information such as credentials or account numbers.

Attack Pattern 89

http://capec.mitre.org/data/index.html

2.761 PHISHING

Ver:

- http://en.wikipedia.org/wiki/Phishing

2.761.1 PHISHING

Método de ataque que busca obtener información personal o confidencial de los usuarios por medio del engaño o la picaresca, recurriendo a la suplantación de la identidad digital de una entidad de confianza en el ciberespacio.

2.761.2 PHISHING

Phishing es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc) de forma fraudulenta.

El estafador o phisher suplanta la personalidad de una persona o empresa de confianza para que el receptor de una comunicación electrónica aparentemente oficial (vía e-mail, fax, sms o telefónicamente) crea en su veracidad y facilite, de este modo, los datos privados que resultan de interés para el estafador.

http://www.inteco.es/glossary/Formacion/Glosario/

2.761.3 PHISHING

Los ataques de "phishing" usan la ingeniería social para adquirir fraudulentamente de los usuarios información personal (principalmente de acceso a servicios financieros). Para alcanzar al mayor número posible de víctimas e incrementar as sus posibilidades de éxito, utilizan el correo basura ("spam") para difundirse. Una vez que llega el correo al destinatario, intentan engañar a los usuarios para que faciliten datos de carácter personal, normalmente conduciéndolos a lugares de Internet falsificados, páginas web, aparentemente oficiales, de bancos y empresas de tarjeta de crédito que terminan de convencer al usuario a que introduzca datos personales de su cuenta bancaria, como su número de cuenta, contraseña, número de seguridad social, etc.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.761.4 (EN) PHISHING

An attack in which the Subscriber is lured (usually through an email) to interact with a counterfeit Verifier/RP and tricked into revealing information that can be used to masquerade as that Subscriber to the real Verifier/RP. [NIST-SP800-63:2013]

2.761.5 PHISHING

fraudulent process of attempting to acquire private or confidential information by masquerading as a trustworthy entity in an electronic communication

NOTE - Phishing can be accomplished by using social engineering or technical deception.

[ISO/IEC 27032:2012]

2.761.6 (EN) PHISHING

A form of Internet fraud that aims to steal valuable information such as credit card details, user IDs and passwords by tricking the user into giving the attacker the confidential information. [CSS NZ:2011]

2.761.7 (EN) PHISHING

Deceiving individuals into disclosing sensitive personal information through deceptive computer-based means. [CNSSI_4009:2010]

2.761.8 (EN) PHISHING

(D) /slang/ A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a Web site, in which the perpetrator masquerades as a legitimate business or reputable person. (See: social engineering.)

Derivation: Possibly from "phony fishing"; the solicitation usually involves some kind of lure or bait to hook unwary recipients. (Compare: phreaking.)

[RFC4949:2007]

2.761.9 (EN) PHISHING

Tricking individuals into disclosing sensitive personal information through deceptive computer-based means. [NIST-SP800-83:2005]

2.761.10 (EN) PHISHING

An attacker may create and use e-mails and websites, designed to look like e-mails and websites of legitimate organisations, in order to deceive users into disclosing personal data such as usernames and passwords.

2.761.11 (EN) PHISHING

A form of criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Phishing is typically carried out using email or an instant message, although phone contact has been used as well). Attempts to deal with the growing number of reported phishing incidents include legislation, user training, and technical measures.

http://en.wikipedia.org/wiki/Phishing

2.761.12 (EN) PHISHING

The practice of tricking a user into giving away personal information such as bank account details by pretending to be a legitimate business or organisation.

http://www.enisa.europa.eu/

2.761.13 (EN) PHISHING

Phishing is the practice of "fishing" for victims and luring these unsuspecting Internet users to a fake Web site.

This is accomplished by using authentic-looking email with the real organization's log with the purpose being to steal passwords, financial or personal information, or introduce a virus attack.

http://idtheft.about.com/od/glossaryofterms/Identity_Theft_Glossary_of_Terms.htm

2.761.14 (EN) PHISHING

An attempt at identity theft in which criminals lead users to a counterfeit website in the hope that they will disclose private information such as user names or passwords.

http://www.getsafeonline.org/

2.761.15 (EN) PHISHING

The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Typically the e-mail and the web site looks like they are part of a bank the user is doing business with.

http://www.sans.org/security-resources/glossary-of-terms/

2.762 PHREAKING

2.762.1 PHREAKING

Phreaking es un término acuñado en la subcultura informática para denominar la actividad de aquellos individuos que orientan sus estudios y ocio hacia el aprendizaje y comprensión del funcionamiento de teléfonos de diversa índole, tecnologías de telecomunicaciones, funcionamiento de compañías telefónicas, sistemas que componen una red telefónica y por último; electrónica aplicada a sistemas telefónicos.

La meta de los phreakers es generalmente superar retos intelectuales de complejidad creciente, relacionados con incidencias de seguridad o fallas en los sistemas telefónicos, que les permitan obtener privilegios no accesibles de forma legal.

El término "Phreak" es una conjunción de las palabras phone (teléfono en inglés) y freak (monstruo en inglés). También se refiere al uso de varias frecuencias de audio para manipular un sistema telefónico, ya que la palabra phreak se pronuncia de forma similar a frequency (frecuencia).

El phreak es una disciplina estrechamente vinculada con el hacking convencional. Auque a menudo es considerado y categorizado como un tipo específico de hacking informático: hacking orientado a la telefonía y estrechamente vinculado con la electrónica, en realidad el phreaking es el germen del hacking puesto que el sistema telefónico es anterior a la extensión de la informática a nivel popular, el hacking surgió del contacto de los phreakers con los primeros sistemas informáticos personales y redes de comunicaciones.

http://es.wikipedia.org/wiki/Phreaking

2.762.2 (EN) PHREAKING

(D) A contraction of "telephone breaking". An attack on or penetration of a telephone system or, by extension, any other communication or information system. [Raym] [RFC4949:2007]

2.762.3 (EN) PHREAKING

Phreaking is a slang term coined to describe the activity of a subculture of people who study, experiment with, or explore telecommunication systems, like equipment and systems connected to public telephone networks. The term "phreak" is a portmanteau of the words "phone" and "freak". It may also refer to the use of various audio frequencies to manipulate a phone system. "Phreak", "phreaker", or "phone phreak" are names used for and by individuals who participate in phreaking. Additionally, it is often associated with computer hacking. This is sometimes called the H/P culture (with H standing for Hacking and P standing for Phreaking).

http://en.wikipedia.org/wiki/Phreaking

2.762.4 (FR) PHREAKING

Technique de piratage du réseau téléphonique, dans le but notamment de profiter d'appels téléphoniques longue distance gratuits et permettant également de dissimuler la véritable origine des appels téléphoniques permettant de se connecter à un réseau comme Internet et perpétrer des actes de malveillance en restant anonyme.

http://www.cases.public.lu/functions/glossaire/

2.763 PIGGYBACK ATTACK

Ver:

- *Ataque*

2.763.1 PIGGYBACK ATTACK

Ataque de interceptación activa en el que el atacante aprovecha los periodos de pausa de un usuario legítimo para colarse.

2.763.2 (EN) PIGGYBACK ATTACK

(I) A form of active wiretapping in which the attacker gains access to a system via intervals of inactivity in another user's legitimate communication connection. Sometimes called a "between-the-lines" attack. (See: hijack attack, man-in-the-middle attack.) [RFC4949:2007]

2.764 PING MORTAL

Ver:

- *Denegación de servicio*
- *Ataque*
- *Barrido IP*
- *Teardrop*

2.764.1 PING MORTAL

Ataque a través de la red. Consiste en enviar paquetes ICMP lo bastante grandes como para causar un fallo en el sistema receptor.

2.764.2 (EN) PING OF DEATH

(D) A denial-of-service attack that sends an improperly large ICMP echo request packet (a "ping") with the intent of causing the destination system to fail. (See: ping sweep, teardrop.) [RFC4949:2007]

2.764.3 (EN) PING OF DEATH

An attack that sends an improperly large ICMP echo request packet (a "ping") with the intent of overflowing the input buffers of the destination machine and causing it to crash.

http://www.sans.org/security-resources/glossary-of-terms/

2.764.4 (EN) PING OF DEATH

On the Internet, ping of death is a denial of service (DoS) attack caused by an attacker deliberately sending an IP packet larger than the 65,536 bytes allowed by the IP protocol. One of the features of TCP/IP is fragmentation; it allows a single IP packet to be broken down into smaller segments. In 1996, attackers began to take advantage of that feature when they found that a packet broken down into fragments could add up to more than the allowed 65,536 bytes. Many operating systems didn't know what to do when they received an oversized packet, so they froze, crashed, or rebooted.

http://searchsoftwarequality.techtarget.com/glossary/

2.765 PIRATERÍA

Ver:

- *Warez*

2.765.1 PIRATERÍA

Robo o destrucción de los bienes de alguien.

DRAE. Diccionario de la Lengua Española.

2.765.2 PIRATEAR

Cometer acciones delictivas contra la propiedad, como hacer ediciones sin permiso del autor o propietario, contrabando, etc.

DRAE. Diccionario de la Lengua Española.

2.765.3 (EN) PIRACY

the act of making illegal copies of video tapes, computer programs, books, etc., in order to sell them

Oxford Advanced Learner's Dictionary.

2.765.4 (EN) PIRATE

o copy and use or sell sbs work or a product without permission and without having the right to do so

Oxford Advanced Learner's Dictionary.

2.765.5 (EN) PIRACY

Illegal use or duplication of material covered by intellectual propery laws, such as copyright.

http://www.getsafeonline.org/

2.766 PISTA DE AUDITORÍA

Ver:

- *Auditoría*

2.766.1 PISTA DE AUDITORÍA

1. Datos e informaciones históricas que están disponibles para su examen, con objeto de probar la corrección e integridad con la cual los procedimientos convenidos se seguridad, relativos a una clave o transacción(es), han sido seguidos. La pista de auditoría permite detectar las violaciones de seguridad (ISO-8732).

2. Datos acerca de la ocurrencia de acontecimientos relativos a la seguridad. Pueden usarse en la investigación de incidentes relacionados con la seguridad o para reconstruir datos dañados o destruidos.

[Ribagorda:1997]

2.766.2 REGISTRO DE AUDITORÍA DE SEGURIDAD

Proceso que proporciona a un mecanismo de análisis y valoración de la seguridad, información relevante sobre la seguridad de un sistema de información.

[CESID:1997]

2.766.3 REGISTRO DE AUDITORÍA DE SEGURIDAD

Datos recogidos que pueden usarse para efectuar una auditoría de seguridad. [ISO-7498-2:1989]

2.766.1 (EN) AUDIT TRAIL

A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result. [CNSSI_4009:2010]

2.766.2 (EN) SECURITY AUDIT TRAIL

(I) A chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results. [NCS04] (See: security audit.) [RFC4949:2007]

2.766.3 (EN) SECURITY AUDIT TRAIL

Data collected and potentially used to facilitate a security audit. [ISO-7498-2:1989]

2.766.4 (FR) JOURNAL D'AUDIT DE SÉCURITÉ

Données collectées et pouvant éventuellement être utilisées pour permettre un audit de sécurité. [ISO-7498-2:1989]

2.767 PKCS - PUBLIC KEY CRYPTOGRAPHY STANDARDS

Acrónimos: PKCS

Ver:

- http://www.rsasecurity.com/rsalabs/pkcs/

- *CAPI - Cryptographic Application Programming Interface*

2.767.1 PKCS - PUBLIC KEY CRYPTOGRAPHY STANDARDS

Serie de publicaciones de RSA Laboratories relativa a estructuras de datos y algoritmos para varias aplicaciones de criptografía asimétrica.

2.767.2 (EN) PUBLIC-KEY CRYPTOGRAPHY STANDARDS (PKCS)

(N) A series of specifications published by RSA Laboratories for data structures and algorithms used in basic applications of asymmetric cryptography. [PKCS] (See: PKCS #5 through PKCS #11.) [RFC4949:2007]

2.767.3 (EN) PKCS (PUBLIC KEY CRYPTO STANDARDS)

A set of standards published by RSA Security, developed in cooperation with an informal consortium (Apple, DEC, Lotus, Microsoft, MIT, and Sun), that includes algorithm-specific and algorithm-independent implementation standards for reliable, secure public key cryptography.

- PKCS #1: RSA Cryptography Standard
- PKCS #3: Diffie-Hellman Key Agreement Standard
- PKCS #5: Password-Based Cryptography Standard
- PKCS #6: Extended-Certificate Syntax Standard
- PKCS #7: Cryptographic Message Syntax Standard
- PKCS #8: Private-Key Information Syntax Standard
- PKCS #9: Selected Attribute Types
- PKCS #10: Certification Request Syntax Standard
- PKCS #11: Cryptographic Token Interface Standard
- PKCS #12: Personal Information Exchange Syntax Standard
- PKCS #13: Elliptic Curve Cryptography Standard
- PKCS #15: Cryptographic Token Information Format Standard

http://www.watchguard.com/glossary/

2.768 PKCS #5

Ver:

- http://www.ietf.org/rfc/rfc2898
- *PKCS - Public Key Cryptography Standards*

2.768.1 PKCS #5

Dentro de la serie PKCS, norma que define el cifrado de octetos con una clave derivada de una contraseña.

2.768.2 (EN) PKCS #5

(N) A standard [PKC05] (see: RFC 2898) from the PKCS series; defines a method for encrypting an octet string with a secret key derived from a password. [RFC4949:2007]

2.769 PKCS #7

Ver:

- http://www.ietf.org/rfc/rfc2315
- *CMS - Cryptographic Message Syntax*
- *PKCS - Public Key Cryptography Standards*

2.769.1 PKCS #7

Dentro de la serie PKCS, norma que define formatos para cifrar y firmar.

2.769.2 (EN) PKCS #7

(N) A standard [PKC07] (see: RFC 2315) from the PKCS series; defines a syntax for data that may have cryptography applied to it, such as for digital signatures and digital envelopes. (See: CMS.) [RFC4949:2007]

2.770 PKCS #10

Ver:

- http://www.ietf.org/rfc/rfc2986
- *Certificado X.509*
- *PKCS - Public Key Cryptography Standards*

2.770.1 PKCS #10

Dentro de la serie PKCS, norma que define la sintaxis para la solicitud de certificados digitales.

2.770.2 (EN) PKCS #10

(N) A standard [PKC10] (see: RFC 2986) from the PKCS series; defines a syntax for certification requests. (See: certification request.) [RFC4949:2007]

2.771 PKCS #11

Ver:

- *Cryptoki*
- *PKCS - Public Key Cryptography Standards*

2.771.1 PKCS #11

Dentro de la serie PKCS, norma que define una interfaz de programación para dispositivos criptográficos.

2.771.2 (EN) PKCS #11

(N) A standard [PKC11] from the PKCS series; defines CAPI called "Cryptoki" for devices that hold cryptographic information and perform cryptographic functions. [RFC4949:2007]

2.772 PLAINTEXT

Ver:

- *Texto en claro*

2.772.1 (EN) PLAIN TEXT

1. (I) /noun/ Data that is input to an encryption process. (See: plaintext. Compare: cipher text, clear text.) [RFC4949:2007]

2.772.2 (EN) PLAINTEXT

Intelligible data that has meaning and can be understood without the application of decryption. [NIST-SP800-57:2007]

2.772.3 (EN) PLAINTEXT

unencrypted information [ISO/IEC 10116:1997]. [ISO-18033-1:2005]

2.772.4 (EN) PLAINTEXT

unenciphered information. [ISO/IEC ISO-9797-1:1999] [ISO-18033-3:2005]

2.772.5 (EN) PLAINTEXT

A message written in regular characters readable by all without any hidden or secret meaning.

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.773 PLAN DE CONTINGENCIA

Ver:

- *Continuidad*

2.773.1 PLAN DE CONTINGENCIA

Un Plan de contingencias es un instrumento de gestión para el buen gobierno de las Tecnologías de la Información y las Comunicaciones en el dominio del soporte y el desempeño.

Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de una compañía.

http://www.inteco.es/glossary/Formacion/Glosario/

2.773.2 PLAN DE CONTINGENCIA

Definición de acciones a realizar, recursos a utilizar y personal a emplear caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos de una organización.

Es término sinónimo de "plan de recuperación de desastres" y "plan de continuidad de negocios".

[Ribagorda:1997]

2.773.3 (EN) CONTINGENCY PLAN

Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the COOP or Disaster Recovery Plan for major disruptions. [CNSSI_4009:2010]

2.773.4 (EN) CONTINGENCY PLAN

(I) A plan for emergency response, backup operations, and post- disaster recovery in a system as part of a security program to ensure availability of critical system resources and facilitate continuity of operations in a crisis. [NCS04] (See: availability.) [RFC4949:2007]

2.773.5 (EN) CONTINGENCY PLAN

A plan that is maintained for disaster response, backup operations, and post-disaster recovery to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation. [NIST-SP800-57:2007]

2.773.6 (EN) CONTINGENCY PLANNING

The development of a contingency plan. [NIST-SP800-57:2007]

2.773.7 (EN) WHAT IS IT CONTINGENCY PLANNING?

IT contingency planning is one modular piece of a larger contingency and continuity-planning program that encompasses IT, business processes, risk management, financial management, crisis communications, safety and security of personnel and property, and continuity of government. Each piece is operative in its own right, but together can create a coordinated synergy that efficiently and effectively protects the entire organization. [NIST-SP800-100:2006]

2.773.8 (EN) CONTINGENCY PLAN

Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster. [NIST-SP800-34:2002]

2.773.9 (EN) CONTINGENCY PLAN

A plan for emergency response, backup operations, and post-disaster recovery maintained by an organization as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

Synonymous with disaster plan and emergency plan.

[IRM-5239-8:1995]

2.773.10 (EN) CONTINGENCIA

In colloquial English, a contingency is something that can happen, but that generally is not anticipated. Planning for contingencies often requires a more imaginative approach, because contingencies are inherently not obvious. Large organizations, such as governments, are often criticized

for not planning for contingencies because the construction of plans to deal with contingencies often involves thinking outside the box. Beforehand, contingencies are hard to predict; this failure to appreciate contingencies ahead of time has led to the formulation of Murphy's law.

http://en.wikipedia.org/wiki/Contingency

2.773.11 (EN) CONTINGENCY PLAN (CP)

Sets out a course of action that is maintained for emergency response, backup operations, and post-disaster recovery. The purpose of the plan is to ensure availability of critical resources and facilitate the continuity of operations in an emergency. The plan includes procedures for performing backups, preparing critical facilities that can be used to facilitate continuity of critical operations in the event of an emergency and recovering from a disaster.

http://www.hipaa.yale.edu/overview/glossary.html

2.774 PLAN DE CONTINUIDAD DEL NEGOCIO (BCP)

Acrónimos: BCP

Ver:

- *Continuidad*

2.774.1 PLAN DE LA CONTINUIDAD DEL NEGOCIO (BCP)

(Diseño del Servicio) Plan que define los pasos que se requieren para el Restablecimiento de los Procesos de Negocio después de una interrupción. El Plan también identifica los disparadores para la Invocación, las personas involucradas, las comunicaciones, etc. El Plan de la Continuidad del Servicio TI es una parte importante de los Planes de Continuidad del Negocio. [ITIL:2007]

2.774.2 PLAN DE CONTINUIDAD

En Inglés BCP (Business Continuity Plan), plan cuyo objetivo es mantener la funcionalidad de una organización, a un nivel mínimo aceptable durante una contingencia.

Esto implica que un Plan de continuidad debe contemplar todas las medidas preventivas y de recuperación para cuando se produzca una contingencia que afecte al negocio.

http://www.inteco.es/glossary/Formacion/Glosario/

2.774.3 PLAN DE CONTINUIDAD DEL NEGOCIO (BCP)

Un plan de continuidad del negocio es un proceso de gestión para asegurar la continuidad de un negocio. No debe confundirse con un "plan de continuidad de operaciones" que se centra en seguir operando en caso de desastre.

La continuidad de operaciones es necesaria para mantener el negocio; pero el negocio es mucho más: cuidar la reputación, la marca, la cuota de mercado, la confianza de las partes interesadas, la cadena de suministro, proteger a empleados y clientes, ..., todos ellos aspectos muy importantes que se hallan al margen de un plan de continuidad de operaciones.

2.774.4 (EN) BUSINESS CONTINUITY PLAN (BCP)

A plan used by an enterprise to respond to disruption of critical business processes. Depends on the contingency plan for restoration of critical systems

ISACA, Cybersecurity Glossary, 2014

2.774.5 (EN) BUSINESS CONTINUITY PLAN (BCP)

The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption. [CNSSI_4009:2010]

2.774.6 (EN) BUSINESS CONTINUITY PLAN (BCP)

(Service Design) A Plan defining the steps required to Restore Business Processes following a disruption. The Plan will also identify the triggers for Invocation, people to be involved, communications etc. IT Service Continuity Plans form a significant part of Business Continuity Plans. [ITIL:2007]

2.774.7 (EN) BUSINESS CONTINUITY PLAN (BCP)

documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organization to continue to deliver its critical activities at an acceptable pre-defined level. [BS25999-1:2006]

2.774.8 (EN) BUSINESS CONTINUITY PLAN (BCP)

A comprehensive written plan to maintain or resume business in the event of a disruption. BCP includes both the technology recovery capability (often referred to as disaster recovery) and the business unit(s) recovery capability.

http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-b-glossary.aspx

2.774.9 (EN) BUSINESS CONTINUITY STRATEGY

Comprehensive strategies to recover, resume, and maintain all critical business functions.

http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-b-glossary.aspx

2.774.10 (EN) BUSINESS RECOVERY TEST / EXERCISE

An activity that tests an institution's BCP.

http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-b-glossary.aspx

2.774.11 (EN) BUSINESS CONTINUITY PLAN (BCP)

A business continuity plan (BCP) is a management process to ensure the continuity of businesses. Not to be confused with continuity of operations (COOP) where the focus is primarily a plan to ensure operations continuity after a disastrous event has already occurred. While continuity of operations is part of business continuity planning tasks, there are other issues outside of the operations that businesses will need to plan for (i.e.; brand protection, company reputation protection,

the company's market share, stockholders' confidence, supply-chain protection, customer and employee protection that may not be included in the continuity of operations plan).

http://en.wikipedia.org/wiki/Business_continuity_plan

2.774.12 (EN) BCP - BUSINESS CONTINUITY PLAN

The documentation of a predetermined set of instructions or procedures that describe how an organizations business functions will be sustained during and after a significant disruption. [NIST-SP800-34:2002]

2.774.13 (EN) BUSINESS CONTINUITY PLAN (BCP)

A Business Continuity Plan is the plan for emergency response, backup operations, and post-disaster recovery steps that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

http://www.sans.org/security-resources/glossary-of-terms/

2.774.14 (EN) BUSINESS CONTINUITY PLANNING

The development and timely execution of plans, measures, procedures and arrangements to ensure minimal or no interruption to the availability of critical services and assets.

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

2.774.15 (FR) PLAN DE CONTINUITE DU BUSINESS (BCP)

(Conception de services) Plan définissant les étapes nécessaires à la remise en fonction des processus business suite à une interruption. Ce plan doit aussi identifier les déclencheurs, les personnes impliquées, les moyens de communication, etc. Les plans de continuité des Services des TI représentent une part importante des plans de continuité du business. [ITIL:2007]

2.774.16 (FR) PLANIFICATION DE LA CONTINUITE DES ACTIVITES

Élaboration et exécution en temps opportun de plans, de mesures, de procédures et de dispositions afin d'éviter ou de minimiser toute interruption de la disponibilité des services et des biens essentiels.

http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578

2.775 PLAN DE CONTINUIDAD DE OPERACIONES

Acrónimos: COOP

Ver:

- *Continuidad*

2.775.1 PLAN DE CONTINUIDAD DE OPERACIONES

Procedimientos encaminados a garantizar que las funciones esenciales de una organización continuarán operativas, de alguna forma, en caso de desastre.

2.775.2 (EN) CONTINUITY OF OPERATIONS PLAN (COOP)

Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The COOP is the third plan needed by the enterprise risk managers and is used when the enterprise must recover (often at an alternate site) for a specified period of time. Defines the activities of individual departments and agencies and their subcomponents to ensure that their essential functions are performed. This includes plans and procedures that delineate essential functions; specifies succession to office and the emergency delegation of authority; provide for the safekeeping of vital records and databases; identify alternate operating facilities; provide for interoperable communications, and validate the capability through tests, training, and exercises. See also Disaster Recovery Plan and Contingency Plan. [CNSSI_4009:2010]

2.775.3 (EN) COOP - CONTINUITY OF OPERATIONS PLAN

A predetermined set of instructions or procedures that describe how an organizations essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations. [NIST-SP800-34:2002]

2.776 PLAN DE RECUPERACIÓN

Acrónimos: BRP

Ver:

- *Continuidad*

2.776.1 PLAN DE RECUPERACIÓN

Procedimiento definido para que se reanuden los procesos de negocio tras una interrupción significativa de los mismos.

2.776.2 (EN) BRP - BUSINESS RECOVERY / RESUMPTION PLAN

The documentation of a predetermined set of instructions or procedures that describe how business processes will be restored after a significant disruption has occurred. [NIST-SP800-34:2002]

2.777 PLAN DE RECUPERACIÓN DE DESASTRES

Acrónimos: DRP

Ver:

- *Continuidad*

2.777.1 PLAN DE RECUPERACIÓN DE DESASTRES

Un plan de recuperación de desastres se centra en los datos y el equipamiento (hardware y software) críticos para que una organización reanude sus operaciones en caso de desastre. Debería incluir planes para atajar la pérdida de personal, aunque típicamente se centra en la protección de la información.

2.777.2 (EN) DISASTER RECOVERY PLAN (DRP)

A set of human, physical, technical and procedural resources to recover, within a defined time and cost, an activity interrupted by an emergency or disaster

ISACA, Cybersecurity Glossary, 2014

2.777.3 (EN) DISASTER RECOVERY PLAN (DRP)

Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The DRP is the second plan needed by the enterprise risk managers and is used when the enterprise must recover (at its original facilities) from a loss of capability over a period of hours or days. See Continuity of Operations Plan and Contingency Plan. [CNSSI_4009:2010]

2.777.4 (EN) DRP - DISASTER RECOVERY PLAN

A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. [NIST-SP800-34:2002]

2.777.5 (EN) DISASTER RECOVERY PLAN

A plan that describes the process to recover from major processing interruptions.

http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-b-glossary.aspx

2.777.6 (EN) DISASTER RECOVERY PLAN

A Disaster recovery plan covers the data, hardware and software critical for a business to restart operations in the event of a natural or human-caused disaster. It should also include plans for coping with the unexpected or sudden loss of key personnel, although this is not covered in this article, the focus of which is data protection.

http://en.wikipedia.org/wiki/Disaster_recovery

2.777.7 (EN) DISASTER RECOVERY PLAN (DRP)

A Disaster Recovery Plan is the process of recovery of IT systems in the event of a disruption or disaster.

http://www.sans.org/security-resources/glossary-of-terms/

2.777.8 (EN) DISASTER RECOVERY PLAN (DRP)

The part of a Contingency Plan that documents the process to restore any loss of data and to recover computer systems if a disaster occurs (i.e., fire, vandalism, natural disaster, or System failure). The document defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process to attain the stated disaster recovery goals.

http://www.hipaa.yale.edu/overview/glossary.html

2.778 PLAN DE SEGURIDAD

2.778.1 PLAN DE SEGURIDAD

Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos. [Magerit:2012]

2.778.2 (EN) SYSTEM SECURITY PLAN

Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. [FIPS-200:2006] [NIST-SP800-53:2013]

2.778.3 (EN) SECURITY PLAN

The Information Security plan complements the IT Plan in so far as it documents, budgets and resources the upgrades to both hardware, software, training and procedures, in relation to Information Security.

http://www.passwordnow.com/en/glossary/information-security-plan.html

2.778.4 (EN) SYSTEM SECURITY PLAN

Provides a baseline of a system's security. A comprehensive system security plan describes the security controls that are in use, or plan to be used to protect all aspects of the system. Security plans are supported by security policy and can be essential tools that identify weaknesses in the system and document what controls will be added to combat the weaknesses.

http://www.utexas.edu/its/policies/glossary.html

2.778.5 (EN) INFORMATION SECURITY PLAN

An information security plan is a document that guides the activities of an organisation towards a more secure environment. It summarises the decisions what security barriers, security policies and training an organisation need to implement. The plan is based on the unique needs and strategies of the organisation.

http://www.itrainonline.org/itrainonline/mmtk/

2.779 PMI - PRIVILEGE MANAGEMENT INFRASTRUCTURE

Acrónimos: PMI

2.779.1 INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS

Infraestructura capaz de soportar la gestión de privilegios como soporte de un servicio de autorización completo y en relación con una infraestructura de claves públicas. [X.509:2005]

2.779.2 (EN) PRIVILEGE MANAGEMENT INFRASTRUCTURE

(O) "The infrastructure able to support the management of privileges in support of a comprehensive authorization service and in relationship with a" PKI; i.e., processes concerned with attribute certificates. [X509] [RFC4949:2007]

2.779.3 (EN) PRIVILEGE MANAGEMENT INFRASTRUCTURE (PMI)

The infrastructure able to support the management of privileges in support of a comprehensive authorization service and in relationship with a Public Key Infrastructure. [X.509:2005]

2.779.4 (FR) INFRASTRUCTURE DE GESTION DE PRIVILEGE

infrastructure qui peut prendre en charge la gestion des privilèges correspondant à un service complet d'autorisation et en relation avec une infrastructure de clé publique. [X.509:2005]

2.780 POLÍTICA

Ver:

- *Política de seguridad*

2.780.1 POLÍTICA

Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.

DRAE. Diccionario de la Lengua Española.

2.780.2 POLÍTICA

Intenciones y dirección de una organización, como las expresa formalmente su alta dirección. [ISO Anexo SL]

[UNE-ISO/IEC 27000:2014]

2.780.3 POLÍTICA

Por lo general, un documento que ofrece un principio de alto nivel o una estrategia a seguir. El propósito de una política es influenciar y guiar la toma de decisiones presente y futura, haciendo que estén de acuerdo a la filosofía, objetivos y planes estratégicos establecidos por los equipos gerenciales de la empresa. Además del contenido de la política, esta debe describir las consecuencias de la falta de cumplimiento de la misma, el mecanismo para manejo de excepciones y la manera de verificar y medir el cumplimiento de la política. [COBIT:2006]

2.780.4 POLÍTICA

Normas vigentes para toda la organización que reglamentan el uso aceptable de los recursos informáticos, las prácticas de seguridad y el desarrollo guiado de procedimientos operacionales.

http://es.pcisecuritystandards.org

2.780.5 (EN) POLICY

a plan of action agreed or chosen by a political party, a business, etc.

Oxford Advanced Learner's Dictionary.

2.780.6 (EN) POLICY

intentions and direction of an organization as formally expressed by its top management [ISO Annex SL]

[ISO-27000:2014]

2.780.7 (EN) POLICY

1a. (I) A plan or course of action that is stated for a system or organization and is intended to affect and direct the decisions and deeds of that entity's components or members. (See: security policy.) [RFC4949:2007]

2.780.8 (EN) POLICY

Generally, a document that provides a high-level principle or course of action. A policy's intended purpose is to influence and guide both present and future decision making to be in line with the philosophy, objectives and strategic plans established by the enterprise's management teams. In addition to policy content, policies need to describe the consequences of failing to comply with the policy, the means for handling exceptions, and the manner in which compliance with the policy will be checked and measured. [COBIT:2006]

2.780.9 (EN) POLICY

Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.780.10 (EN) POLICY

The method of action selected from alternatives, given specific conditions to guide and determine present and future decisions.

http://www.symantec.com/avcenter/refa.html

2.780.11 (FR) POLITIQUE

Règle à l'échelle de l'organisation régissant l'utilisation acceptable des ressources informatiques, les pratiques de sécurité, et guidant l'élaboration des procédures opérationnelles.

http://fr.pcisecuritystandards.org/

2.781 POLÍTICA DE CERTIFICACIÓN

Ver:

- *CPS - Declaración de Prácticas de Certificación*

- *Certificado X.509*

2.781.1 POLÍTICA DE CERTIFICADO

Conjunto denominado de reglas que indica la aplicabilidad de un certificado a una determinada comunidad y/o clase de aplicación con requisitos de seguridad comunes. Por ejemplo, una determinada política de certificado pudiera indicar la aplicabilidad de un tipo de certificado a la autenticación de transacciones de intercambio electrónico de datos para el comercio de bienes dentro de una gama de precios dada. [X.509:2005]

2.781.2 (EN) CERTIFICATE POLICY

A specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications. [CNSSI_4009:2010]

2.781.3 (EN) CERTIFICATION POLICY

(D) Synonym for either "certificate policy" or "certification practice statement". [RFC4949:2007]

2.781.4 (EN) CERTIFICATE POLICY

A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range. [X.509:2005]

2.781.5 (FR) POLITIQUE DE CERTIFICAT

ensemble nommé de règles indiquant la possibilité d'appliquer un certificat pour une communauté particulière et/ou une classe d'applications particulière avec des besoins de sécurité communs. Une politique de certificat particulière peut, par exemple, indiquer la possibilité d'application d'un certificat pour des transactions avec échange de données électroniques pour le commerce de biens dans une fourchette de prix donnée. [X.509:2005]

2.782 POLÍTICA DE DIVULGACIÓN

2.782.1 POLÍTICA DE DIVULGACIÓN

2.782.2 (EN) DISCLOSURE POLICY

A policy that governs the disclosure to clients and other stakeholder by a provider of a computer program or system of defects discovered in those products.

http://cyber.law.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas

2.783 POLÍTICA DE FIRMA ELECTRÓNICA

Ver:

- *Firma electrónica*
- *Política de certificación*

2.783.1 POLÍTICA DE FIRMA ELECTRÓNICA.

Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma. [ENS:2010]

2.783.2 (EN) ELECTRONIC SIGNATURE POLICY

Set of security standards, organizational, technical and legal to determine how to generate, verify and manage electronic signatures, including the characteristics required of signing certificates. [ENS:2010]

2.784 POLÍTICA DE PRIVILEGIOS

Ver:

- *Privilegio*

2.784.1 POLÍTICA DE PRIVILEGIOS

Política que destaca condiciones para los verificadores de privilegios con el fin de proporcionar o realizar servicios relacionados con asertores de privilegios cualificados. La política de privilegios relaciona atributos asociados con el servicio, así como atributos asociados con asertores de privilegios. [X.509:2005]

2.784.2 (EN) PRIVILEGE POLICY

The policy that outlines conditions for privilege verifiers to provide/perform sensitive services to/for qualified privilege asserters. Privilege policy relates attributes associated with the service as well as attributes associated with privilege asserters. [X.509:2005]

2.784.3 (FR) POLITIQUE DE PRIVILÈGE

politique qui définit dans ses grandes lignes les conditions sous lesquelles les vérificateurs de privilège peuvent fournir ou effectuer des services sensibles au profit ou pour le compte de déclarants de privilège qualifiés. La politique de privilège est liée à des attributs associés au service, ainsi qu'à des attributs associés aux déclarants de privilège. [X.509:2005]

2.785 POLÍTICA DE SEGURIDAD

Ver:

- *Política*
- *Dominio de seguridad*

2.785.1 POLÍTICA DE SEGURIDAD.

Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos. [ENS:2010]

2.785.2 POLÍTICA DE SEGURIDAD

Conjunto de leyes, reglamentos y prácticas que regulan el modo en una organización administra, protege y distribuye información confidencial.

http://es.pcisecuritystandards.org

2.785.3 POLÍTICA DE SEGURIDAD

Son las decisiones o medidas de seguridad que una empresa a decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos. También puede referirse al documento de nivel ejecutivo mediante el cual una empresa establece sus directrices de seguridad de la información.

http://www.inteco.es/glossary/Formacion/Glosario/

2.785.4 POLÍTICA DE SEGURIDAD

(Diseño del Servicio) Política que gobierna la visión de la Organización a la Gestión de la Información de Seguridad. [ITIL:2007]

2.785.5 POLÍTICA DE SEGURIDAD

Conjunto de leyes, normas y prácticas, que regulan la gestión, la protección y la distribución de los bienes, información sensible incluida, de un organismo, en el seno de éste. [CCN-STIC-207:2006]

2.785.6 POLÍTICA DE SEGURIDAD

Documento de alto nivel que sirve como marco para reflejar las intenciones y requisitos de seguridad de la información de una Organización. [CCN-STIC-401:2007]

2.785.7 POLÍTICA DE SEGURIDAD

Conjunto de reglas establecidas por la autoridad de seguridad que rigen la utilización y prestación de servicios y facilidades de seguridad. [X.509:2005]

2.785.8 POLÍTICA CORPORATIVA DE SEGURIDAD

1. Conjunto de leyes, reglas y prácticas, que regulan el modo en que los bienes que contienen información sensible son gestionados, protegidos y distribuidos dentro de una organización (ITSEC).

2. Conjunto de principios y normas que regulan la forma propia de cada organización, de proteger las informaciones que maneja y los productos y sistemas de tratamiento de dichas informaciones.

[Ribagorda:1997]

2.785.9 POLÍTICA DE SEGURIDAD

1. Conjunto de reglas para el establecimiento de servicios de seguridad (ISO-7498-2).

2. Conjunto de reglas establecidas por la Autoridad de seguridad, que gobiernan el uso y suministro de servicios de seguridad e instalaciones seguras (ISO/IEC 9594-8, ITU-T X.509)

[Ribagorda:1997]

2.785.10 POLÍTICA DE SEGURIDAD

Conjunto de criterios para la prestación de servicios de seguridad (véanse también «política de seguridad basada en la identidad» y «política de seguridad basada en reglas»). [ISO-7498-2:1989]

2.785.11 POLÍTICA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Conjunto, formalizado en un documento aplicable, de elementos estratégicos, directivas, procedimientos, códigos de conducta, normas organizacionales y técnicas, que tiene por objetivo la protección del (o de los) sistema(s) de información del organismo. [PSSI] [EBIOS:2005]

2.785.1 (EN) INFORMATION SECURITY POLICY

Aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information. [CNSSI_4009:2010]

2.785.2 (EN) SECURITY POLICY

1. (I) A definite goal, course, or method of action to guide and determine present and future decisions concerning security in a system. [NCS03, R3198] (Compare: certificate policy.)

2a. (I) A set of policy rules (or principles) that direct how a system (or an organization) provides security services to protect sensitive and critical system resources. (See: identity-based security policy, policy rule, rule-based security policy, rules of behavior. Compare: security architecture, security doctrine, security mechanism, security model, [R1281].)

2b. (O) A set of rules to administer, manage, and control access to network resources. [R3060, R3198]

2c. (O) /X.509/ A set of rules laid down by an authority to govern the use and provision of security services and facilities.

2d. (O) /Common Criteria/ A set of rules that regulate how assets are managed, protected, and distributed within a TOE.

[RFC4949:2007]

2.785.3 (EN) SECURITY POLICY

within the context of this document; rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its systems, particularly those which impact the systems and associated elements. [ISO-21827:2007]

2.785.4 (EN) INFORMATION SECURITY POLICY

(Service Design) The Policy that governs the Organisation's approach to Information Security Management. [ITIL:2007]

2.785.5 (EN) ORGANISATIONAL SECURITY POLICY (OSP)

a set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organisation in the operational environment. [CC:2006]

2.785.6 (EN) SECURITY POLICY

The set of rules laid down by the security authority governing the use and provision of security services and facilities. [X.509:2005]

2.785.1 (EN) INFORMATION SYSTEMS SECURITY POLICY

Set of strategic information, directives, procedures, codes of conduct, organisational and technical rules formalised in an applicable document whose objective is to protect the organisation's information system(s). [EBIOS:2005]

2.785.2 (EN) ORGANISATIONAL SECURITY POLICY

Security rule, procedure, code of conduct or guideline that an organisation imposes for its operation. [ISO 15408] [EBIOS:2005]

2.785.3 (EN) SECURITY POLICY

The statement of required protection of the information objects. [NIST-SP800-27:2004]

2.785.4 (EN) SECURITY POLICY

The statement of required protection of the information objects. [NIST-SP800-33:2001]

2.785.5 (EN) CORPORATE SECURITY POLICY

the set of laws, rules and practices that regulate how assets including sensitive information are managed, protected and distributed within a user organisation. [ITSEC:1991]

2.785.6 (EN) SYSTEM SECURITY POLICY

the set of laws, rules and practices that regulate how sensitive information and other information are managed, protected and distributed within a specific system.. [ITSEC:1991]

2.785.7 (EN) TECHNICAL SECURITY POLICY

the set of laws, rules and practices regulating the processing of sensitive information and the use of resources by the hardware and software of an IT system or product. [ITSEC:1991]

2.785.8 (EN) SECURITY POLICY

The set of criteria for the provision of security services. [ISO-7498-2:1989]

2.785.9 (EN) IDENTITY-BASED SECURITY POLICY

A security policy based on the identities and/or attributes of users, a group of users, or entities acting on behalf of the users and the resources/objects being accessed. [ISO-7498-2:1989]

2.785.10 (EN) SECURITY POLICY

The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. [TCSEC:1985]

2.785.11 (EN) SECURITY POLICY

Set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.785.12 (EN) SECURITY POLICY

In business, a security policy is a document that states in writing how a company plans to protect the company's physical and information technology (IT) assets. A security policy is often considered to be a "living document", meaning that the document is never finished, but is continuously updated as technology and employee requirements change. A company's security policy may include an acceptable use policy, a description of how the company plans to educate its employees about protecting the company's assets, an explanation of how security measurements will be carried out and enforced, and a procedure for evaluating the effectiveness of the security policy to ensure that necessary corrections will be made.

http://searchsecurity.techtarget.com/

2.785.13 (EN) SECURITY POLICY

A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

http://www.sans.org/security-resources/glossary-of-terms/

2.785.14 (EN) SECURITY POLICY

A Security Policy is a set of objectives, rules of behaviour for users and administrators, and requirements for system configuration and management that collectively are designed to ensure Security of computer systems in an organization.

A Security Policy might include sections on:

- Virus detection and prevention.
- Firewall use and configuration.
- Password strength and management.
- Host System administration practices.

- Access Control rules.
- Use of Access Logs.
- Use of screen locking software.
- Logging out of unattended workstations.
- Physical security.
- Account termination.
- Procedures for granting and revoking system access.

http://hitachi-id.com/concepts/security_policy.html

2.785.15 (FR) POLITIQUE DE SÉCURITÉ

Ensemble de lois, de règles et de pratiques régissant la manière dont une organisation gère, protège et distribue des informations sensibles.

http://fr.pcisecuritystandards.org/

2.785.16 (FR) POLITIQUE DE SÉCURITÉ INFORMATIQUE

(Conception de services) La politique qui gouverne l'approche que peut avoir une organisation en termes de Gestion de la Sécurité de l'Information. [ITIL:2007]

2.785.17 (FR) POLITIQUE DE SÉCURITÉ

ensemble de règles fixées par l'autorité de sécurité qui régit l'utilisation et la fourniture de services et de fonctionnalités de sécurité. [X.509:2005]

2.785.18 (FR) POLITIQUE DE SÉCURITÉ

Ensemble des critères permettant de fournir des services de sécurité [voir aussi «politique de sécurité fondée sur l'identité» (§ 3.3.30) et «politique de sécurité fondée sur des règles» [ISO-7498-2:1989]

2.785.19 (FR) POLITIQUE DE SECURITE DE SYSTEME D'INFORMATION

Ensemble, formalisé dans un document applicable, des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d'information de l'organisme. [PSSI] [EBIOS:2005]

2.785.20 (FR) POLITIQUE (DE SÉCURITÉ)

Ensemble de règles et de mesures décrivant les objectifs et exigences de sécurité d'une organisation. La politique fait suite à une analyse des risques et fait appel à des procédures particulières. La direction de l'organisation doit s'engager à faire respecter la politique de sécurité auprès de ses employés, collaborateurs et intervenants.

http://www.cases.public.lu/functions/glossaire/

2.786 POLÍTICA DE SEGURIDAD BASADA EN LA IDENTIDAD

Ver:

- *Política de seguridad basada en reglas*
- *Control de acceso por roles*

2.786.1 POLÍTICA DE SEGURIDAD BASADA EN LA IDENTIDAD

Política de seguridad basada en las identidades y/o atributos de los usuarios, de un grupo de usuarios o entidades que actúan en nombre de los usuarios y en los recursos/objetos a que se accede. [ISO-7498-2:1989]

2.786.2 (EN) IDENTITY-BASED SECURITY POLICY

(I) "A security policy based on the identities and/or attributes of users, a group of users, or entities acting on behalf of the users and the resources/objects being accessed." [ISO-7498-2] (See: rule-based security policy.) [RFC4949:2007]

2.786.3 (EN) IDENTITY-BASED SECURITY POLICY

A security policy based on the identities and/or attributes of the object (system resource) being accessed and of the subject (user, group of users, process, or device) requesting access. [NIST-SP800-33:2001]

2.786.4 (EN) IDENTITY-BASED SECURITY POLICY

A security policy based on the identities and/or attributes of users, a group of users, or entities acting on behalf of the users and the resources/objects being accessed. [ISO-7498-2:1989]

2.786.5 (FR) POLITIQUE DE SECURITE FONDEE SUR L'IDENTITE

Politique de sécurité fondée sur les identités et/ou les attributs des utilisateurs, d'un groupe d'utilisateurs ou d'entités agissant au nom d'utilisateurs et sur les identités et/ou attributs des ressources/objets auxquels on doit accéder. [ISO-7498-2:1989]

2.787 POLÍTICA DE SEGURIDAD BASADA EN REGLAS

Ver:

- *Política de seguridad basada en la identidad*
- *Control de acceso basado en reglas*

2.787.1 POLÍTICA DE SEGURIDAD BASADA EN REGLAS

Política de seguridad basada en reglas globales impuestas a todos los usuarios. Estas reglas suelen depender de una comparación de la sensibilidad de los recursos a los que se accede con los atributos correspondientes de los usuarios, de un grupo de usuarios o de entidades que actúan en nombre de los usuarios. [ISO-7498-2:1989]

2.787.2 (EN) RULE-BASED SECURITY POLICY

A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding

attributes by the subjects requesting access. Also known as discretionary access control (DAC). [CNSSI_4009:2010]

2.787.3 (EN) RULE-BASED SECURITY POLICY

(I) "A security policy based on global rules [i.e., policy rules] imposed for all users. These rules usually rely on comparison of the sensitivity of the resource being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users." [ISO-7498-2] (Compare: identity- based security policy, policy rule, RBAC.) [RFC4949:2007]

2.787.4 (EN) RULE-BASED SECURITY POLICY

A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes by the subjects requesting access. [NIST-SP800-33:2001]

2.787.1 (EN) RULE-BASED SECURITY POLICY

A security policy based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users. [ISO-7498-2:1989]

2.787.2 (FR) POLITIQUE DE SECURITE FONDEE SUR DES REGLES

Politique de sécurité fondée sur des règles globales imposées à tous les utilisateurs. Ces règles s'appuient généralement sur une comparaison de la sensibilité des ressources auxquelles on doit accéder avec les attributs correspondants d'utilisateurs, d'un groupe d'utilisateurs ou d'entités agissant au nom d'utilisateurs. [ISO-7498-2:1989]

2.788 POLÍTICA DE SELLOS DE TIEMPO

Ver:

- *Sello de tiempo*

2.788.1 POLÍTICA DE SELLOS DE TIEMPO

conjunto formal de reglas que indican la aplicabilidad de unos sellos de tiempo a una comunidad de usuarios o un conjunto de aplicaciones con unos criterios de seguridad compartidos [traducción de ISO/IEC 18014-1]

2.788.2 (EN) TIME-STAMPING POLICY

a named set of rules that indicates the applicability of a time-stamp token to a particular community or class of application with common security requirements [ISO-18014-2:2002]

2.789 POLÍTICA DE USO DEL E-MAIL

Ver:

- *Política*

2.789.1 POLÍTICA DE USO DEL E-MAIL

Normativa referente al uso corporativo de la mensajería electrónica.

2.789.2 (EN) EMAIL POLICY

Policies that address issues, such as:

- Which users are entitled to send or receive email.
- What files and text can be included in email.
- To and from what addresses.
- How HTML formatted mail is handled.
- Content inspection of attachments to prevent vandals and viruses from infecting the network.

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.790 POLÍTICA TIPO MURALLA CHINA

Ver:

- *Modelo de Brewer-Nash*

2.790.1 POLÍTICA TIPO MURALLA CHINA

Política de seguridad que enfoca el problema de una organización que interactúa con otras organizaciones que son competencia comercial de la primera.

2.790.2 (EN) CHINESE WALL POLICY

(I) A security policy to prevent conflict of interest caused by an entity (e.g., a consultant) interacting with competing firms. (See: Brewer-Nash model.) [RFC4949:2007]

2.791 POTENCIAL DE ATAQUE

Ver:

- *Ataque*

2.791.1 POTENCIAL DE ATAQUE

Percepción de las posibilidades de éxito de un ataque. Se expresa en función de la capacidad del atacante (experiencia y recursos disponibles) así como de su motivación para atacar.

2.791.2 (EN) ATTACK POTENTIAL

(I) The perceived likelihood of success should an attack be launched, expressed in terms of the attacker's ability (i.e., expertise and resources) and motivation. (Compare: threat, risk.) [RFC4949:2007]

2.791.3 (EN) ATTACK POTENTIAL

a measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation.

TOE - Target of Evaluation

[CC:2006]

2.791.4 (EN) ATTACK POTENTIAL

The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation. [CC:2006]

2.792 PPP - POINT-TO-POINT PROTOCOL

Acrónimos: PPP

Ver:

- http://www.ietf.org/rfc/rfc1661
- *CHAP - Challenge-Handshake Authentication Protocol*
- *Extensible Authentication Protocol*
- *PAP - Password Authentication Protocol*

2.792.1 PPP - POINT-TO-POINT PROTOCOL

El protocolo PPP permite establecer una comunicación a nivel de enlace entre dos computadoras. Generalmente, se utiliza para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un módem telefónico. Ocasionalmente también es utilizado sobre conexiones de banda ancha (como PPPoE o PPPoA). Además del simple transporte de datos, PPP facilita dos funciones importantes:

- Autenticación. Generalmente mediante una clave de acceso.
- Asignación dinámica de IP.

http://es.wikipedia.org/wiki/Point-to-Point_Protocol

2.792.2 (EN) POINT-TO-POINT PROTOCOL (PPP)

(I) An Internet Standard protocol (RFC 1661) for encapsulation and full-duplex transportation of protocol data packets in OSIRM Layer 3 over an OSIRM Layer 2 link between two peers, and for multiplexing different Layer 3 protocols over the same link. Includes optional negotiation to select and use a peer entity authentication protocol to authenticate the peers to each other before they exchange Layer 3 data. (See: CHAP, EAP, PAP.) [RFC4949:2007]

2.793 PPTP - POINT-TO-POINT TUNNELING PROTOCOL

Acrónimos: PPTP

Ver:

- http://www.ietf.org/rfc/rfc2637
- *L2TP - protocolo de túnel en la capa 2*

- *IPsec - IP security*
- *Red privada virtual*
- *PPP - Point-to-Point Protocol*

2.793.1 PPTP - POINT-TO-POINT TUNNELING PROTOCOL

protocolo desarrollado por Microsoft, U.S. Robotics, Ascend Communications, 3Com/Primary Access, ECI Telematics conocidas colectivamente como PPTP Forum, para implementar redes privadas virtuales o VPN.

http://es.wikipedia.org/wiki/PPTP

2.793.2 (EN) POINT-TO-POINT TUNNELING PROTOCOL (PPTP)

(I) An Internet client-server protocol (RFC 2637) (originally developed by Ascend and Microsoft) that enables a dial-up user to create a virtual extension of the dial-up link across a network by tunneling PPP over IP. (See: L2TP.) [RFC4949:2007]

2.793.3 (EN) PPTP (POINT-TO-POINT TUNNELING PROTOCOL)

A VPN tunneling protocol with encryption. It uses one TCP port (for negotiation and authentication of a VPN connection) and one IP protocol (for data transfer) to connect the two nodes in a VPN. Though favored by Microsoft, many experts feel PPTP offers weaker confidentiality of data than a competing standard, IPSec.

http://www.watchguard.com/glossary/

2.793.4 (EN) PPTP - POINT-TO-POINT TUNNELING PROTOCOL

A protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet.

2.793.5 (EN) POINT-TO-POINT TUNNELING PROTOCOL (PPTP)

A protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet.

http://www.sans.org/security-resources/glossary-of-terms/

2.793.6 (FR) PPTP - POINT TO POINT TUNNELING PROTOCOL

Développé initialement par Microsoft, 3COM et Ascend, puis normalisé par l'IETF, PPTP est un protocole de tunneling de niveau 2 (couche liaison du système OSI), à l'image de L2TP, assurant les services de sécurité suivants:

- Authentification (CHAP, PAP).
- Confidentialité (chiffrement par secret partagé, ou par clé publique en utilisant l'algorithme RC4 à 40 ou 128 bits).

PPTP encapsule des trames PPP dans des paquets IP uniquement, pour un transport sur le réseau Internet ou tout réseau IP, IPX , NetBEUI.

PPTP permet de prolonger l'encapsulation PPP et d'utiliser ses fonctionnalités pour gérer la sécurité de bout en bout (authentification et chiffrement).

PPTP utilise le port TCP 1723 et l'identifiant (proto) 47 au niveau IP.

http://securit.free.fr/glossaire.htm

2.794 PRACTICA DE CONTROL

2.794.1 PRACTICA DE CONTROL

Mecanismo esencial de control. Es la base para garantizar que los objetivos de control se alcanzarán con los recursos disponibles, una gestión adecuada y un alineamiento de los sistemas de información al negocio.

2.794.2 PRÁCTICA DE CONTROL

Mecanismo clave de control que apoya el logro de los objetivos de control por medio del uso responsable de recursos, la administración apropiada de los riesgos y la alineación de TI con el negocio. [COBIT:2006]

2.794.3 (EN) CONTROL PRACTICE

Key control mechanism that supports the achievement of control objectives through responsible use of resources, appropriate management of risk and alignment of IT with business. [COBIT:2006]

2.795 PREGUNTA-RESPUESTA

Ver:

- *Reto*
- *Método de autenticación*
- http://en.wikipedia.org/wiki/Challenge-response_authentication
- *CAPTCHA*

2.795.1 PREGUNTA-RESPUESTA

Procedimiento de autenticación en el cual un ordenador lanza a un supuesto usuario un mensaje que debe ser operado por éste según una transformación específica, y sólo conocida por ambos, y devuelto al ordenador.

Habitualmente, la forma de operar es como sigue: Usuarios y ordenador comparten un único algoritmo de cifra y una criptografía, distinta para cada usuario.

En el proceso de autenticación, el usuario, primero, se identifica, lo que sirve al ordenador para extraer la clave criptográfica correspondiente. Seguidamente, éste lanza al usuario una pregunta (a menudo denominada reto) constituida por un número aleatorio distinto cada vez. El usuario responde devolviendo el resultado de cifrar este número con su clave de usuario. Al tiempo, el ordenador cifra el número y lo compara con la respuesta recibida, para verificar su coincidencia (el usuario será quien alega ser) o no.

En otros modelos, el usuario se limita a cifrar con su clave el tiempo de un reloj sincronizado con el ordenador, devolviendo a éste el resultado.

[Ribagorda:1997]

2.795.2 PROTOCOLO PREGUNTA-RESPUESTA

Protocolo de autenticación en el que una entidad prueba su identidad a otra demostrando el conocimiento de un secreto asociado a dicha entidad pero sin revelarle el secreto. [CESID:1997]

2.795.1 (EN) CHALLENGE AND REPLY AUTHENTICATION

Prearranged procedure in which a subject requests authentication authentication of another and the latter establishes validity with a correct reply. [CNSSI_4009:2010]

2.795.2 (EN) CHALLENGE-RESPONSE

(I) An authentication process that verifies an identity by requiring correct authentication information to be provided in response to a challenge. In a computer system, the authentication information is usually a value that is required to be computed in response to an unpredictable challenge value, but it might be just a password. [RFC4949:2007]

2.795.3 (EN) CHALLENGE RESPONSE

A method to authenticate another party using either a shared secret (symmetric key) that is used to encrypt a random challenge, or by using asymmetric cryptography i.e. signing a challenge whereas the other side verifies the signature.

2.795.4 (EN) CHALLENGE-RESPONSE

In computer security, challenge-response authentication is a family of protocols in which one party presents a question ("challenge") and another party must provide a valid answer ("response") to be authenticated.

http://en.wikipedia.org/wiki/Challenge-response_authentication

2.795.5 (FR) STIMULATION/RÉPONSE

Est un procédé d'authentification basé sur un défi émis par un serveur. Le client ne peut relever ce défi que s'il possède un secret particulier. Le succès du défi prouve l'identité du client.

http://securit.free.fr/glossaire.htm

2.796 PREVENCIÓN DE PÉRDIDA DE DATOS

Acrónimos: DLP

2.796.1 PREVENCIÓN DE PÉRDIDA DE DATOS

Data leakage protection (DLP) son aquellas medidas de seguridad que tratan de evitar que la información confidencial o valiosa sea copiada o transladada fuera del entorno de seguridad.

http://www.inteco.es/glossary/Formacion/Glosario/

2.796.2 (EN) DATA LOSS PREVENTION

Data loss prevention (DLP) is the identification and safeguarding of information that should have controlled or limited distribution, that is, data that should not be in the public domain. Example data types that should be covered by data loss prevention efforts include (but are not limited to)

- Information formally classified by the U.S. Government as confidential, secret, or top secret;
- Information not formally classified, but which has been labeled for limited distribution (For Official Use Only, Sensitive But Unclassified, and similar terms);
- Information covered by the Privacy Act of 1974 or other Personally Identifiable Information (PII) designated as not for public release;
- Proprietary vendor information—information released by contractors and other entities to the Federal government for its internal use only.

DLP is the umbrella term used for efforts to ensure that limited distribution data is only available as authorized. Controls on limited distribution data include both data at rest (data temporarily or permanently stored in any way, including but not limited to physical drives and non-volatile or volatile memory), data in motion (data being transmitted within a device or between devices by any means),and data in processing (data being acted on by a process).

Mobile Security Reference Architecture, May 23, 2013

2.797 PRINCIPAL

2.797.1 PRINCIPAL

Identidad que singulariza al usuario que accede al sistema.

2.797.2 (EN) PRINCIPAL

(I) A specific identity claimed by a user when accessing a system.

(I) /Kerberos/ A uniquely identified (i.e., uniquely named) client or server instance that participates in a network communication.

[RFC4949:2007]

2.798 PRIVACIDAD

Ver:

- *Evaluación de respeto a la privacidad*

2.798.1 PRIVACIDAD

1. Derecho de los individuos a controlar e influir en la recogida y almacenamiento de datos referentes a los mismos, así como por quien y a quien pueden ser dados a conocer estos datos (ISO-7498-2).

2. Derecho de los individuos de mantener su vida privada libre de intromisiones de otros individuos u organizaciones o de la obtención y uso de datos por estos individuos u organizaciones.

[Ribagorda:1997]

2.798.2 PRIVACIDAD

Derecho de los individuos de controlar qué datos relativos a ellos pueden ser recopilados y almacenados y quién y para qué puede tener acceso a ellos. [CESID:1997]

2.798.3 PRIVACIDAD

Derecho de las personas a controlar o influir sobre la información relacionada con ellos que puede recogerse o almacenarse y las personas a las cuales o por las cuales esta información puede ser revelada.

NOTA. Como este término se relaciona con el derecho de las personas, no puede ser muy preciso y su uso debe evitarse, salvo como un motivo para exigir seguridad.

[ISO-7498-2:1989]

2.798.4 (EN) PRIVACY

1. (I) The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others. (See: HIPAA, personal information, Privacy Act of 1974. Compare: anonymity, data confidentiality.) [FP041]

2. (O) "The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed." [ISO-7498-2]

[RFC4949:2007]

2.798.5 (EN) PRIVACY

the right of every individual that his/her private and family life, home and correspondence are treated in confidence. There shall be no interference by an authority with the exercise of this right except where it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, the protection of health or morals, or for the protection of the rights and freedoms of others. [ISO-18028-1:2006]

2.798.6 (EN) PRIVACY

right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. [ISO-18028-2:2006]

2.798.7 (EN) PRIVACY

A mode of communication in which only the explicitly enabled parties can interpret the communication. This is typically achieved by encryption and shared key(s) for the cipher. [H.235:2005]

2.798.8 (EN) PRIVACY

The Privacy Security Dimension provides for the protection of information that might be derived from the observation of network activities. Examples of this information include web-sites that a user has visited, a user's geographic location, and the IP addresses and DNS names of devices in a Service Provider network. [X.805:2003]

2.798.9 (EN) PRIVACY

The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

NOTE. Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security.

[ISO-7498-2:1989]

2.798.10 (FR) RESPECT DE LA VIE PRIVEE

Droit des individus de contrôler ou d'agir sur des informations les concernant, qui peuvent être collectées et stockées, et sur les personnes par lesquelles et auxquelles ces informations peuvent être divulguées.

Remarque. Ce terme étant lié au droit privé, il ne peut pas être très précis et son utilisation devrait être évitée sauf pour des besoins de sécurité.

[ISO-7498-2:1989]

2.799 PRIVILEGIO

Ver:

- *Control de acceso*

2.799.1 PRIVILEGIO

Atributo o propiedad asignado a una entidad por una autoridad. [X.509:2005]

2.799.2 PRIVILEGIO

Capacidad de usar un servicio controlado o restringido. [Ribagorda:1997]

2.799.3 PRIVILEGIO TEMPORAL

Práctica de permitir un privilegio sólo durante el período de tiempo para el que se necesita con objeto de concluir una función específica. [Ribagorda:1997]

2.799.4 (EN) PRIVILEGE

A right granted to an individual, a program, or a process. [CNSSI_4009:2010]

2.799.5 (EN) PRIVILEGED ACCOUNT

An information system account with approved authorizations of a privileged user. [CNSSI_4009:2010]

2.799.6 (EN) PRIVILEGED COMMAND

A human-initiated command executed on an information system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information. [CNSSI_4009:2010]

2.799.7 (EN) PRIVILEGED PROCESS

A computer process that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary processes are not authorized to perform. [CNSSI_4009:2010]

2.799.8 (EN) PRIVILEGED USER

A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. [CNSSI_4009:2010]

2.799.9 (EN) PRIVILEGE

1a. (I) /access control/ A synonym for "authorization". (See authorization. Compare: permission.)

1b. (I) /computer platform/ An authorization to perform a security-relevant function in the context of a computer's operating system.

[RFC4949:2007]

2.799.10 (EN) PRIVILEGE

An attribute or property assigned to an entity by an authority. [X.509:2005]

2.799.11 (FR) PRIVILÈGE

attribut ou propriété attribué par une autorité à un utilisateur. [X.509:2005]

2.800 PRIVILEGIO MÍNIMO

Ver:

- *Necesidad de conocer*
- http://en.wikipedia.org/wiki/Least_privilege

2.800.1 MÍNIMO PRIVILEGIO

Principio según el cual los sujetos deben acceder exclusivamente a aquellos objetos que precisen inexcusablemente para ejecutar sus trabajos o procesos.

Es término sinónimo de "necesidad de saber".

[Ribagorda:1997]

2.800.2 PRINCIPIO DE MÍNIMO PRIVILEGIO

Postulado que requiere que los sujetos de un sistema tengan habilitado, exclusivamente, el derecho de acceso (escritura, lectura, etc.) a los objetos que ineludiblemente requieran para cumplir las funciones del puesto que ocupan.

Es término sinónimo de "necesidad de saber".

[Ribagorda:1997]

2.800.1 (EN) LEAST PRIVILEGE

The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. [CNSSI_4009:2010]

2.800.2 (EN) LEAST PRIVILEGE

(I) The principle that a security architecture should be designed so that each system entity is granted the minimum system resources and authorizations that the entity needs to do its work.

(Compare: economy of mechanism, least trust.)

[RFC4949:2007]

2.800.3 (EN) LEAST PRIVILEGE

This principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use. [TCSEC:1985]

2.800.4 (EN) LEAST PRIVILEGE

Least Privilege is the principle of allowing users or applications the least amount of permissions necessary to perform their intended function.

http://www.sans.org/security-resources/glossary-of-terms/

2.801 PRIVILEGIOS DE ACCESO

Ver:

- *Derecho de acceso*
- *Acceso*
- *Control de acceso*
- *Privilegio*

2.801.1 DERECHOS DE ACCESO

Privilegios de acceso de sujeto a un objeto. Por ejemplo, los derechos pueden ser: escritura, lectura, ejecución, borrado, etc. [Ribagorda:1997]

2.801.2 (EN) ACCESS PRIVILEGES

The ability of users to read, change or delete files.

http://www.getsafeonline.org/

2.802 PROBABILIDAD DE OCURRENCIA

2.802.1 PROBABILIDAD

En análisis de riesgos, estimación de la posibilidad de que ocurra un cierto suceso. Puede ser cuantitativa (un valor numérico) o cualitativa (una escala ordenada de valores relativos).

2.802.2 PROBABILIDAD

Cálculo matemático que permite determinar hasta qué punto se puede esperar que ocurra un suceso.

Diccionario Manual de la Lengua Española Vox. © 2007 Larousse Editorial, S.L.

2.802.3 (EN) LIKELIHOOD OF OCCURRENCE

In Information Assurance risk analysis, a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability. [CNSSI_4009:2010]

2.802.4 (EN) PROBABILITY OF OCCURRENCE

See likelihood of occurrence. [CNSSI_4009:2010]

2.802.5 (EN) LIKELIHOOD

estimate of the potential of an incident or event's occurrence

Annotation:

1. Qualitative and semi-quantitative risk assessments can use qualitative estimates of likelihood such as high, medium, or low, which may be represented numerically but not mathematically. Quantitative assessments use mathematically derived values to represent likelihood.
2. The likelihood of a successful attack occurring is typically broken into two related quantities: the likelihood that an attack occurs (which is a common mathematical representation of threat), and the likelihood that the attack succeeds, given that it is attempted (which is a common mathematical representation of vulnerability). In the context of natural hazards, likelihood of occurrence is typically informed by the frequency of past incidents or occurrences.
3. The intelligence community typically estimates likelihood in bins or ranges such as "remote," "unlikely," "even chance," "probable/likely," or "almost certain."
4. Probability is a specific type of likelihood. Likelihood can be communicated using numbers (e.g. 0-100, 1-5) or phrases (e.g. low, medium, high), while probabilities must meet more stringent conditions.

See Also: Probability (Mathematical)

DHS Risk Lexicon, September 2008

2.802.6 (EN) PROBABILITY (MATHEMATICAL):

likelihood that is expressed as a number between 0 and 1, where 0 indicates that the occurrence is impossible and 1 indicates definite knowledge that the occurrence has happened or will happen, where the ratios between numbers reflect and maintain quantitative relationships

Example: The probability of a coin landing on "heads" is 1/2.

Annotation:

1) Probability (mathematical) is a specific type of likelihood estimate that obeys the laws of probability theory.

2) Probability is used colloquially as a synonym for likelihood.

DHS Risk Lexicon, September 2008

2.802.7 (FR) VRAISEMBLANCE

possibilité que quelque chose se produise

NOTE 1 Dans la terminologie du management du risque, le mot «vraisemblance» est utilisé pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminée de façon objective ou subjective, qualitative ou quantitative, et qu'elle soit décrite au moyen de termes généraux ou mathématiques [telles une probabilité ou une fréquence sur une période donnée].

NOTE 2 Le terme anglais «likelihood» (vraisemblance) n'a pas d'équivalent direct dans certaines langues et c'est souvent l'équivalent du terme «probability» (probabilité) qui est utilisé à la place. En anglais, cependant, le terme «probability» (probabilité) est souvent limité à son interprétation mathématique. Par conséquent, dans la terminologie du management du risque, le terme «vraisemblance » est utilisé avec l'intention qu'il fasse l'objet d'une interprétation aussi large que celle dont bénéficie le terme «probability» (probabilité) dans de nombreuses langues autres que l'anglais.

[ISO Guide 73 2009]

2.802.8 (FR) VRAISEMBLANCE

Estimation de la possibilité qu'un scénario de menace ou un risque, se produise. Elle représente sa force d'occurrence.

[EBIOS:2010]

2.803 PROCEDIMIENTO

Ver:

- *Procedimientos Operativos de Seguridad (POS)*
- *SECOPS - Security Operating Procedures*
- *Procedimiento operativo*

2.803.1 PROCEDIMIENTO

Método de ejecutar algunas cosas.

DRAE. Diccionario de la Lengua Española.

2.803.2 PROCEDIMIENTO

Una descripción de una manera particular de lograr algo; una forma establecida de hacer las cosas; una serie de pasos que se siguen en un orden regular definido, garantizando un enfoque consistente y repetitivo hacia las actividades. [COBIT:2006]

2.803.3 PROCEDIMIENTO

forma especificada para llevar a cabo una actividad o un proceso [ISO-9000_es:2000]

2.803.4 PROCEDIMIENTO

Narración descriptiva de una política. El procedimiento equivale a los pasos de una política y describe cómo debe implementarse una determinada política.

http://es.pcisecuritystandards.org

2.803.5 (EN) PROCEDURE

a way of doing sth, especially the usual or correct way

Oxford Advanced Learner's Dictionary.

2.803.6 (EN) PROCEDURE

a written description of a course of action to be taken to perform a given task [IEEE-STD-610].

2.803.7 (EN) PROCEDURE

A description of a particular way of accomplishing something; an established way of doing things; a series of steps followed in a definite regular order ensuring the consistent and repetitive approach to actions. [COBIT:2006]

2.803.8 (EN) PROCEDURE

Descriptive narrative for a policy. Procedure is the “how to” for a policy and describes how the policy is to be implemented.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.803.9 (FR) PROCÉDURE

Commentaire descriptif d’une politique. La procédure indique «comment utiliser» une politique et décrit la manière dont celle-ci est mise en œuvre.

http://fr.pcisecuritystandards.org/

2.804 PROCEDIMIENTO OPERATIVO

Ver:

- *Procedimiento*
- *SECOPS - Security Operating Procedures*
- *Procedimientos Operativos de Seguridad (POS)*

2.804.1 PROCEDIMIENTO OPERATIVO

Reglas que determinan el uso correcto del objeto sujeto a evaluación (TOE).

2.804.2 (EN) OPERATING PROCEDURE

a set of rules defining correct use of a Target of Evaluation (TOE). [ITSEC:1991]

2.805 PROCEDIMIENTOS OPERATIVOS DE SEGURIDAD (POS)

Acrónimos: POS (es)

Ver:

- *SECOPS - Security Operating Procedures*

2.805.1 PROCEDIMIENTOS OPERATIVOS DE SEGURIDAD (POS)

Los POS definen los principios que deberán adoptarse en materia de seguridad, los procedimientos operativos que deberán seguirse y las responsabilidades del personal. Los POS se elaborarán bajo la responsabilidad del Responsable del Sistema.

Adaptada de 2001/264/CE.

2.805.2 PROCEDIMIENTOS OPERATIVOS DE SEGURIDAD (POS)

Descripción precisa de la aplicación de los requisitos de seguridad, detallando las responsabilidades y todas las acciones y procedimientos de seguridad a seguir, con el objetivo de garantizar y mantener la seguridad del Sistema.

2.805.3 PROCEDIMIENTOS OPERATIVOS DE SEGURIDAD (POS)

Documento que describe las condiciones de seguridad en la operación de un sistema. Se basa en los requisitos de seguridad que se impusieron para éste. Mostrará la arquitectura del sistema, el personal autorizado a operar, los servicios que proporciona así como su modo seguro de operación.

2.806 PROCESO

2.806.1 PROCESO

Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en elementos de salida. [UNE-ISO/IEC 27000:2014]

2.806.2 (EN) PROCESS

set of interrelated or interacting activities which transforms inputs into outputs [ISO/IEC 27000:2014]

2.807 PRODUCTO DE SEGURIDAD TIC

2.807.1 PRODUCTO DE SEGURIDAD TIC

Conjunto de componentes software, firmware y/o hardware, que proporcionan funcionalidad de seguridad, diseñado para su uso o para su incorporación en un sistema o en un entorno operativo definido específicamente y con una utilidad particular.

2.807.2 (EN) IT SECURITY PRODUCT

A package of IT software, firmware and/or hardware, providing security functionality designed for use or incorporation within a multiplicity of systems or within a specifically defined operational environment and with a particular purpose.

2.808 PROPIEDAD DE LA ESTRELLA (*)

Ver:

- *Modelo de Bell-LaPadula*

2.808.1 PROPIEDAD DE LA ESTRELLA (*)

En el modelo de seguridad de Bell-LaPadula, se define una regla de control de acceso consistente en que un usuario no puede escribir información en un nivel inferior a aquel en el que se encuentra. Sí puede escribir en niveles superiores. De esta forma, la información que se maneja en un cierto nivel de clasificación puede ascender; pero no puede descender de nivel.

2.808.2 (EN) *-PROPERTY

A Bell-LaPadula security model rule allowing a subject write access to an object only if the security level of the subject is dominated by the security level of the object. Also known as the Confinement Property. [TCSEC:1985]

2.808.3 (EN) STAR PROPERTY

In Star Property, a user cannot write data to a lower classification level without logging in at that lower classification level.

http://www.sans.org/security-resources/glossary-of-terms/

2.808.4 (EN) STRONG STAR PROPERTY

In Strong Star Property, a user cannot write data to higher or lower classifications levels than their own.

http://www.sans.org/security-resources/glossary-of-terms/

2.809 PROPIETARIO DE LA INFORMACIÓN

Ver:

- *Datos*
- *Custodio*
- *Responsable de la información*

2.809.1 PROPIETARIO DE LA INFORMACIÓN

Persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información. Debe tener autoridad para especificar y exigir las medidas de seguridad necesarias para cumplir con sus responsabilidades, pudiendo delegar los aspectos operacionales en responsables de seguridad.

2.809.2 RESPONSABLE DEL FICHERO

Persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento.

LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. (Vigente hasta el 14 de enero de 2000)

2.809.3 (EN) DATA OWNER

(N) The organization that has the final statutory and operational authority for specified information. [RFC4949:2007]

2.809.4 (EN) PROPIETARIOS DE DATOS

Individuos, por lo general gerentes o directores, que tienen la responsabilidad de la integridad, el uso y el reporte preciso de los datos computarizados. [COBIT:2006]

2.809.5 (EN) DATA OWNERS

Individuals, normally managers or directors, who have responsibility for the integrity, accurate reporting and use of computarised data. [COBIT:2006]

2.809.6 (EN) OWNER

The authoritative head of the respective college, school, or unit. The owner is responsible for the function that is supported by the resource or for carrying out the program that uses the resources. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments. The owner or his designated representatives are responsible for and authorized to:

- Approve access and formally assign custody of an information resources asset.
- Determine the asset's value.

- Specify and establish data control requirements that provide security, and convey them to users and custodians.
- Specify appropriate controls, based on risk assessment, to protect the state's information resources from unauthorized modification, deletion, or disclosure. Controls shall extend to information resources outsourced by the university.
- Confirm that controls are in place to ensure the accuracy, authenticity, and integrity of data.
- Confirm compliance with applicable controls.
- Assign custody of information resources assets and provide appropriate authority to implement security controls and procedures.
- Review access lists based on documented security risk management decisions.

http://www.utexas.edu/its/policies/glossary.html

2.809.7 (EN) DATA OWNER

A Data Owner is the entity having responsibility and authority for the data.

http://www.sans.org/security-resources/glossary-of-terms/

2.810 PROPIETARIO DEL RIESGO

Ver:

- *Riesgo*

2.810.1 DUEÑO DEL RIESGO

Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo. [UNE-ISO GUÍA 73:2010]

[UNE-ISO/IEC 27000:2014]

2.810.1 DUEÑO DEL RIESGO

Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo. [UNE Guía 73:2010]

2.810.2 (EN) RISK OWNER

person or entity with the accountability and authority to manage a risk [ISO Guide 73:2009]

[ISO/IEC 27000:2014]

2.810.3 (EN) RISK OWNER

person or entity with the accountability and authority to manage a risk. [ISO Guide 73:2009]

2.810.4 (FR) PROPRIÉTAIRE DU RISQUE

personne ou entité ayant la responsabilité du risque et ayant autorité pour le gérer [ISO Guide 73:2009]

2.811 PROTECCIÓN DE DERECHOS DE AUTOR

Acrónimos: DRM

Ver:

- *Marcas de agua*
- *Huella digital*

2.811.1 PROTECCIÓN DE DERECHOS DE AUTOR

Soporte tecnológico para proteger los derechos de autor sobre información digital o digitalizada.

2.811.2 DRM

DRM, Digital rights management, son aquellas tecnologías de control de acceso que pueden ser usadas por fabricantes de hardware y autores para evitar un uso indebido de contenidos y dispositivos digitales.

http://www.inteco.es/glossary/Formacion/Glosario/

2.811.3 (EN) DIGITAL RIGHTS MANAGEMENT (DRM)

Any technology used to protect the interests of copyright holders of commercial digital information products and services.

2.812 PROTECCIÓN DEL PERÍMETRO

Acrónimos: BPC, BPS

Ver:

- *Pasarela de seguridad*
- *Dispositivo de protección perimetral*
- *Guardia*
- *Cortafuegos*
- *Air gap*

2.812.1 SISTEMA DE PROTECCIÓN DE PERÍMETRO

Combinación de hardware y/o software, denominado Dispositivo de Protección de Perímetro, cuya finalidad es mediar en el tráfico de entrada y salida en los puntos de interconexión de los sistemas. [CCN-STIC-301:2006] [CCN-STIC-302:2012]

2.812.2 (EN) BOUNDARY

Physical or logical perimeter of a system.

2.812.3 (EN) LOGICAL PERIMETER

A conceptual perimeter that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system. without a reliable human review by an appropriate

authority. The location of such a review is commonly referred to as an "air gap." [CNSSI_4009:2010]

2.812.4 (EN) BOUNDARY PROTECTION

Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).

2.812.5 (EN) BOUNDARY PROTECTION DEVICE

A device with appropriate mechanisms that facilitates the adjudication of different security policies for interconnected systems.

NIST SP 800.53: A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection.

[CNSSI_4009:2010]

2.812.6 (EN) BOUNDARY PROTECTION

Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels). [NIST-SP800-53:2013]

2.812.7 (EN) BOUNDARY PROTECTION COMPONENT (BPC)

A component of a system that provides a Boundary Protection Service.

Note: a combination of multiple BPC may be required to implement a particular BPS; a single BPC may contribute to implement more than one BPS (e.g., the Unified Threat Management concept). Traditionally BPC were found at the security boundary providing network level BPS, but BPC may be distributed throughout the CIS, to include BPC at the desktop. Examples: content checking software (e.g. anti-virus, antispam), firewall, data diode, backup components, guard, filtering router, access router, proxy servers, network and host level intrusion prevention/detection, encryptor.

2.812.8 (EN) BOUNDARY PROTECTION SERVICE (BPS)

A service that mediates information flows and/or mitigates security risk introduced by an interconnection. Examples: Entity authentication, access control, data integrity, system integrity.

2.813 PROTOCOLO DE SEÑALES DE TRÁFICO

Acrónimos: TLP

2.813.1 PROTOCOLO DE SEÑALES DE TRÁFICO

Protocolo creado para promover la compartición de información clasificada. Permite que el originatario de una información le indique al receptor las condiciones en que le llega la información a efectos de su posible compartición con terceros.

Se definen 4 colores, pensando en las luces de un semáforo:

- ROJO - sólo puede llegar a manos de personas identificadas nominalmente

  Normalmente esta información se transfiere personalmente al receptor.

- NARANJA - distribución limitada

  El receptor puede conpartir la información recibida con otros miembros de su organización, aunque siempre respetando el principio de 'necesidad de conocer'. El receptor puede verse requerido para especificar a quién se lo hace llegar.

- VERDE - restringido a la comunidad

  La información puede circular libremente dentro de una cierta comunidad. Eso no implica que sea información pública, ni que pueda ser proporcionada a terceras partes fuera de la comunidad identificada.

- BLANCO - sin límites

  La información se puede transmitor sin más restricciones que las derivadas de las condicones de derechos de autor (copyright).

2.813.2 (EN) TRAFFIC LIGHT PROTOCOL

The Traffic Light Protocol (TLP) was created in order to encourage greater sharing of information. In order to encourage the sharing of sensitive information, however, the originator needs to signal how widely they want their information to be circulated beyond the immediate recipient, if at all.

The TLP provides a simple method to achieve this. It is designed to improve the flow of information between individuals, organisations or communities in a controlled and trusted way. It is important that everyone understands and obeys the rules of the protocol. Only then can trust be established and the benefits of information sharing realised. The TLP is based on the concept of the originator labeling information with one of four colours to indicate what further dissemination, if any, can be undertaken by the recipient. The recipient must consult the originator if wider dissemination is required.

There are four colours (or traffic lights):

- RED - personal for named recipients only

  In the context of a meeting, for example, RED information is limited to those present at the meeting. In most circumstances, RED information will be passed verbally or in person.

- AMBER - limited distribution

  The recipient may share AMBER information with others within their organisation, but only on a 'need-to-know' basis. The originator may be expected to specify the intended limits of that sharing.

- GREEN - community wide

Information in this category can be circulated widely within a particular community. However, the information may not be published or posted publicly on the Internet, nor released outside of the community.

- WHITE – unlimited

  Subject to standard copyright rules, WHITE information may be distributed freely, without restriction.

http://en.wikipedia.org/wiki/Traffic_Light_Protocol

2.814 PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN

Ver:

- *Firma electrónica*
- *Autoridad de certificación (AC)*

2.814.1 PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica. [Ley-59:2003]

2.814.2 (EN) CERTIFICATION SERVICE PROVIDER

means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.

[Directive-1999/93/EC:1999]

2.815 PROXY (AGENTE)

Ver:

- *Cortafuegos*
- *Pasarela*

2.815.1 PROXY

Programa o dispositivo que realiza una acción en representación de otro. [CCN-STIC-641:2006]

2.815.2 PROXY (AGENTE)

Dispositivo pasarela que implementa la funcionalidad cliente/servidor de uno o más protocolos o aplicaciones, según los RFC o estándares correspondientes, con el objetivo de servir peticiones a servidores en nombre de los clientes que lo utilizan. [CCN-STIC-401:2007]

2.815.3 PROXY INVERSO

Dispositivo "proxy" con el objetivo de servir peticiones de clientes externos de nuestra red protegiendo el acceso a un servicio externo. [CCN-STIC-401:2007]

2.815.4 PROXY TRANSPARENTE

Dispositivo "proxy" con la capacidad de interceptar el tráfico a nivel de red sin que sea percibido por parte de los clientes. [CCN-STIC-401:2007]

2.815.5 PROXY (AGENTE)

Servidor de comunicaciones, responsable de canalizar el tráfico entre una red privada e Internet, que contiene un cortafuegos a nivel físico. [Ribagorda:1997]

2.815.1 (EN) PROXY

An application that “breaks” the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it.

Note: This effectively closes the straight path between the internal and external networks making it more difficult for an attacker to obtain internal addresses and other details of the organization’s internal network. Proxy servers are available for common Internet services; for example, a Hyper Text Transfer Protocol (HTTP) proxy used for Web access, and a Simple Mail Transfer Protocol (SMTP) proxy used for e-mail. [CNSSI_4009:2010]

2.815.2 (EN) PROXY AGENT

A software application running on a firewall or on a dedicated proxy server that is capable of filtering a protocol and routing it between the interfaces of the device. [CNSSI_4009:2010]

2.815.3 (EN) PROXY SERVER

A server that services the requests of its clients by forwarding those requests to other servers. [CNSSI_4009:2010]

2.815.4 (EN) PROXY

1. (I) A computer process that acts on behalf of a user or client.

2. (I) A computer process --often used as, or as part of, a firewall-- that relays application transactions or a protocol between client and server computer systems, by appearing to the client to be the server and appearing to the server to be the client. (See: SOCKS.)

[RFC4949:2007]

2.815.5 (EN) PROXY SERVERS

A server that acts as an intermediary between users and the Internet to enable security, caching, administrative control, and policy enforcements.

http://iab.com/

2.815.6 (EN) PROXY

A software agent, often a firewall mechanism, which performs a function or operation on behalf of another application or system while hiding the details involved.

http://www.symantec.com/avcenter/refa.html

2.815.7 (FR) PROXY

Service qui sépare la communication entre un réseau local et un réseau externe. Le proxy sert de filtre et de protection d'adressage direct de communication permettant de cacher la topologie du réseau local aux utilisateurs du réseau externe et interdisant ces derniers à entrer en communication directe avec des machines du réseau local. Le proxy permet également de concentrer les accès en provenance de plusieurs machines du réseau local vers différents services sur des machines du réseau externe, on garantie ainsi une facilité dans la gestion de la sécurité des communications sortantes en n'autorisant grâce au firewall qu'une seule machine à accéder au réseau externe et non pas individuellement chaque machine du réseau local.

http://www.cases.public.lu/functions/glossaire/

2.816 PROYECTO ABIERTO DE SEGURIDAD DE APLICACIONES WEB

2.816.1 PROYECTO ABIERTO DE SEGURIDAD DE APLICACIONES WEB

OWASP (acrónimo de Open Web Application Security Project, en inglés ‘Proyecto abierto de seguridad de aplicaciones web’) es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP. La comunidad OWASP está formada por empresas, organizaciones educativas y particulares de todo mundo. Juntos constituyen una comunidad de seguridad informática que trabaja para crear artículos, metodologías, documentación, herramientas y tecnologías que se liberan y pueden ser usadas gratuitamente por cualquiera.

http://es.wikipedia.org/wiki/Open_Web_Application_Security_Project

2.816.2 (EN) OWASP

The Open Web Application Security Project (OWASP) is an online community dedicated to web application security. The OWASP community includes corporations, educational organizations, and individuals from around the world. This community works to create freely-available articles, methodologies, documentation, tools, and technologies. The OWASP Foundation is a 501(c)(3) charitable organization that supports and manages OWASP projects and infrastructure. It is also a registered non profit in Europe since June 2011.

http://en.wikipedia.org/wiki/OWASP

2.816.3 (EN) OPEN WEB APPLICATION SECURITY PROJECT

An open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted Security Project (OWASP) maintain applications that can be trusted

ISACA, Cybersecurity Glossary, 2014

2.817 PRUEBA

Ver:

- *Evidencia*
- *Criterios comunes*

2.817.1 PRUEBA

Razón, argumento, instrumento u otro medio con que se pretende mostrar y hacer patente la verdad o falsedad de algo.

DRAE. Diccionario de la Lengua Española.

2.817.2 (EN) PROOF

information, documents, etc. that show that sth is true

Oxford Advanced Learner's Dictionary.

2.817.3 (EN) PROOF

The corroboration that evidence is valid in accordance with the non-repudiation policy in force.

NOTE. Proof is evidence that serves to prove truth or existence of something.

[ISO-13888-1:2004]

2.817.4 (EN) PROVE

this term refers to a formal analysis in its mathematical sense. It is completely rigorous in all ways. Typically, prove is used when there is a desire to show correspondence between two TSF representations at a high level of rigour.

TSF - TOE Security Functionality

TOE - Target of Evaluation

[CC:2006]

2.818 PRUEBA DE POSESIÓN

Acrónimos: POP

Ver:

- *Clave*
- *Clave criptográfica*

2.818.1 PRUEBA DE POSESIÓN

Protocolo para que una entidad demuestre a otra que conoce un cierto secreto.

2.818.2 (EN) PROOF-OF-POSSESSION PROTOCOL

(I) A protocol whereby a system entity proves to another that it possesses and controls a cryptographic key or other secret information. (See: zero-knowledge proof.) [RFC4949:2007]

2.818.3 (EN) PROOF OF POSSESSION (POP)

A verification process whereby it is proven that the owner of a key pair actually has the private key associated with the public key. The owner demonstrates possession by using the private key in its intended manner. [NIST-SP800-57:2007]

2.819 PRUEBAS DE PENETRACIÓN

Ver:

- *Penetración*
- http://en.wikipedia.org/wiki/Penetration_test
- *Ataque controlado*
- *Escáner de vulnerabilidades*

A veces denominado “pen testing” o “pentesting”.

2.819.1 PRUEBA DE PENETRACIÓN

Las pruebas de penetración tienen como finalidad intentar identificar maneras de aprovechar las vulnerabilidades para evitar o rechazar las características de seguridad de los componentes del sistema. Las pruebas de penetración incluyen pruebas de aplicaciones y de redes, y controles y procesos de redes y aplicaciones. Se realizan tanto desde el exterior del entorno (pruebas externas) como en el sentido contrario.

http://es.pcisecuritystandards.org

2.819.2 PENTEST

Una prueba de penetración (pentest) es un método de evaluación de la seguridad de un sistema informático o red mediante la simulación de un ataque de una fuente malicioso realizado por un hacker ético. El proceso implica un análisis activo de cualquier vulnerabilidad potencial, configuraciones deficientes o inadecuadas, tanto de hardware como de software ,o deficiencias operativas en las medidas de seguridad.

Este análisis se realiza desde la posición de un atacante potencial y puede implicar la explotación activa de vulnerabilidades de seguridad. Cualquier problema de seguridad que se encuentran se presentará al propietario del sistema, junto con una evaluación de su impacto, y a menudo con una propuesta de mitigación o una solución técnica. La intención de una prueba de penetración es determinar la viabilidad de un ataque y el impacto en el negocio de un ataque exitoso.

http://www.inteco.es/glossary/Formacion/Glosario/

2.819.3 PRUEBAS DE PENETRACIÓN

Pruebas de auditoria para comprobar la correcta aplicación y configuración de contramedidas de seguridad en los dispositivos de información y comunicaciones según lo especificado en la política de seguridad y así alertar de posibles desviaciones detectadas. [CCN-STIC-401:2007]

2.819.4 PRUEBAS DE PENETRACIÓN

1. Prueba realizada por el evaluador sobre el Objeto de Evaluación para comprobar si sus vulnerabilidades son, o no, explotables en la práctica (ITSEC).

2. Etapa del proceso de verificación de la seguridad de un sistema en la que los evaluadores tratan de soslayar o violar los controles de seguridad del mismo.

[Ribagorda:1997]

2.819.5 (EN) PEN TEST:

A Penetration Test. A method for determining the risk to a network by attempting to penetrate its defenses. Pentesting combines vulnerability assessment techniques with evasion techniques and other attack methods to simulate a “real attack.” [knapp:2014]

2.819.6 (EN) PENETRATION TESTING

A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system. [NIST-SP800-53:2013]

2.819.1 (EN) PENETRATION TESTING

A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system. [CNSSI_4009:2010]

2.819.2 (EN) PENETRATION TEST

(I) A system test, often part of system certification, in which evaluators attempt to circumvent the security features of a system. [NCS04, SP42] (See: tiger team.) [RFC4949:2007]

2.819.3 (EN) PENETRATION TESTING

tests performed by an evaluator on the Target of Evaluation in order to confirm whether or not known vulnerabilities are actually exploitable in practice. [ITSEC:1991]

2.819.4 (EN) PENETRATION TESTING

The portion of security testing in which the penetrators attempt to circumvent the security features of a system. The penetrators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The penetrators work under no constraints other than those that would be applied to ordinary users. [TCSEC:1985]

2.819.5 (EN) PENETRATION TEST

Penetration tests attempt to exploit vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application testing as well as controls and processes around the networks and applications, and occurs from both outside the network trying to come in (external testing) and from inside the network.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.819.6 (EN) PENETRATION TESTING

When trusted hackers simulate an attack on a computer system in the hope of revealing vulnerabilities and finding opportunities for improving its security.

http://www.getsafeonline.org/

2.819.7 (EN) PENETRATION TESTING

Penetration testing is the security-oriented probing of a computer system or network to seek out vulnerabilities that an attacker could exploit. The testing process involves an exploration of the all security features of the system in question, followed by an attempt to breech security and penetrate the system. The tester, sometimes known as an ethical hacker, generally uses the same methods and tools as a real attacker. Afterwards, the penetration testers report on the vulnerabilities and suggest steps that should be taken to make the system more secure.

http://searchsoftwarequality.techtarget.com/glossary/

2.819.8 (EN) PENETRATION TESTING

Penetration testing is used to test the external perimeter security of a network or facility.

http://www.sans.org/security-resources/glossary-of-terms/

2.819.9 (EN) PENETRATION TESTING

Penetration testing goes beyond vulnerability scanning to use multistep and multivector attack scenarios that first find vulnerabilities and then attempt to exploit them to move deeper into the enterprise infrastructure. Since this is how advanced targeted attacks work, penetration testing provides visibility into aggregations of misconfigurations or vulnerabilities that could lead to an attack that could cause serious business impact. As a minimum, penetration testing provides a means for prioritizing the highest risk vulnerabilities.

http://www.gartner.com/it-glossary/

2.819.10 (EN) PEN TEST (PENETRATION TESTING)

Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents.

Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in.

Pen test strategies include:

Targeted testing

Targeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights-turned-on" approach because everyone can see the test being carried out.

External testing

This type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.

Internal testing

This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

Blind testing

A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.

Double blind testing

Double blind testing takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is being conducted. Double-blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures.

http://searchsoftwarequality.techtarget.com/

2.819.11 (FR) TEST DE PÉNÉTRATION

Les tests de pénétration essayent d'identifier les manières d'exploiter les vulnérabilités pour contourner ou vaincre les fonctions sécuritaires des composants du système. Le test d'intrusion doit inclure le test du réseau et de l'application, ainsi que des contrôles et processus relatifs aux réseaux et aux applications. Il doit être mis en œuvre aussi depuis l'extérieur de l'environnement (test externe) que de l'intérieur.

http://fr.pcisecuritystandards.org/

2.820 PRUEBAS DE SEGURIDAD

2.820.1 PRUEBAS DE SEGURIDAD

Proceso que permite determinar si las funciones de seguridad de un sistema están acordes con lo establecido para un cierto escenario de aplicación. El proceso incluye pruebas funcionales, pruebas de penetración y técnicas de verificación.

2.820.2 (EN) SECURITY TESTING

A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed application environment. This process includes hands-on functional testing, penetration testing, and verification.

See also: Functional Testing, Penetration Testing, Verification.

[TCSEC:1985]

2.821 PRUEBAS FUNCIONALES

2.821.1 PRUEBAS FUNCIONALES

Dentro de las pruebas de seguridad, aquellas en las que las medidas de protección se ponen a prueba en condiciones operativas.

2.821.2 (EN) FUNCTIONAL TESTING

Segment of security testing in which advertised security mechanisms of an information system are tested under operational conditions. [CNSSI_4009:2010]

2.822 PUBLIC-KEY FORWARD SECRECY

Acrónimos: PFS

Ver:

- *Perfect forward secrecy*
- http://www.ietf.org/rfc/rfc4306

2.822.1 PUBLIC-KEY FORWARD SECRECY

Propiedad del sistema de generación de claves que nos asegura que una clave de sesión que estamos usando hoy no se vería comprometida si en el futuro se revelaran partes secretas utilizados para generar la clave actual.

2.822.2 (EN) PUBLIC-KEY FORWARD SECRECY (PFS)

(I) For a key-agreement protocol based on asymmetric cryptography, the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future. (See: Usage note and other discussion under "perfect forward secrecy".) [RFC4949:2007]

2.822.3 (EN) PUBLIC-KEY FORWARD SECRECY (PFS)

For a key agreement protocol based on asymmetric cryptography, the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future.

http://www.sans.org/security-resources/glossary-of-terms/

2.823 PUERTA ENCUBIERTA

Ver:

- *Puerta trasera*

2.823.1 PUERTA ENCUBIERTA

Mecanismo oculto que permite acceder a un sistema obviando los mecanismos autorizados de acceso. Algunos programadores introducen estas vías de acceso, no especificadas en el producto, para posteriormente poder acceder directamente al sistema.

2.823.2 (EN) TRAP DOOR

1. A means of reading cryptographically protected information by the use of private knowledge of weaknesses in the cryptographic algorithm used to protect the data. See also back door.

2. In cryptography, one-to-one function that is easy to compute in one direction, yet believed to be difficult to invert without special information.

[CNSSI_4009:2010]

2.823.3 (EN) TRAP DOOR

A hidden software or hardware mechanism that can be triggered to permit system protection mechanisms to be circumvented in some innocent-appearing manner; e.g., a special "random" key sequence at a keyboard. Software developers often introduce trap doors in their code to enable them to reenter the system and perform certain functions.

Synonymous with back door.

[IRM-5239-8:1995]

2.823.4 (EN) TRAP DOOR

A hidden software or hardware mechanism that permits system protection mechanisms to be circumvented. It is activated in some non-apparent manner (e.g., special "random" key sequence at a terminal). [TCSEC:1985]

2.824 PUERTA TRASERA

Ver:

- *Puerta encubierta*

2.824.1 BACKDOOR

Se denomina backdoor o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema.

Las puertas traseras pueden ser errores o fallos, o pueden haber sido creadas a propósito, por los propios autores pero al ser descubiertas por terceros, pueden ser utilizadas con fines ilícitos.

Por otro lado, también se consideran puertas traseras a los programas que, una vez instalados en el ordenador de la víctima, dan el control de éste de forma remota al ordenador del atacante.

Por lo tanto aunque no son específicamente virus, pueden llegar a ser un tipo de malware que funcionan como herramientas de control rmoto. Cuentan con una códificación propia y usan cualquier servicio de Internet: correo, mensajería instantánea,Http, ftp, telnet o chat. Chat.

http://www.inteco.es/glossary/Formacion/Glosario/

2.824.2 PUERTA TRASERA

Código de entrada, no documentado y secreto, a un programa o dispositivo físico, que se usa para acceder a dicho programa o dispositivo soslayando los controles establecidos para ello.

Con frecuencia adopta la forma de un canal oculto.

Es el principal problema en el desarrollo seguro de programas. Los controles de seguridad que se recomienda establecer son los habituales de la ingeniería del software: modularidad, encapsulación, revisiones cruzadas y pruebas independientes.

[Ribagorda:1997]

2.824.3 PUERTA TRASERA

Tipo de software de control remoto que permite ingresar en un sistema operativo, página web o aplicación a una determinada parte de los mismos que usualmente está restringida a un usuario ajeno, evitando los métodos de autentificación usuales. Estos programas suelen ser troyanos para la entrada de "hackers" y "crackers" pero también pueden ser una entrada secreta de los programadores o "webmasters" con diversos fines.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.824.1 (EN) BACK DOOR

Typically unauthorized hidden software or hardware mechanism used to circumvent security controls. [CNSSI_4009:2010]

2.824.2 (EN) BACK DOOR

1. (I) /COMPUSEC/ A computer system feature -- which may be (a) an unintentional flaw, (b) a mechanism deliberately installed by the system's creator, or (c) a mechanism surreptitiously installed by an intruder -- that provides access to a system resource by other than the usual procedure and usually is hidden or otherwise not well-known. (See: maintenance hook. Compare: Trojan Horse.)

2. (I) /cryptography/ A feature of a cryptographic system that makes it easily possible to break or circumvent the protection that the system is designed to provide.

[RFC4949:2007]

2.824.3 (EN) BACKDOOR

A malicious program that listens for commands on a certain Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port. [NIST-SP800-83:2005]

2.824.4 (EN) BACKDOOR

A backdoor is a point of access to a computer that does not require authentication. An unlocked house back door gives access to an otherwise secure home; a computer backdoor allows access to your PC without your knowledge or permission.

PC Security Handbook, Rich Robinson

2.824.5 (EN) BACKDOOR

A design fault, planned or accidental, that allows the apparent strength of the design to be easily avoided by those who know the trick.

http://www.watchguard.com/glossary/

2.824.6 (EN) BACKDOOR

A way into a network that a hacker has planted to circumvent a network's security policy. For example, a modem connection that is not secure can serve as a back door.

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.824.7 (EN) BACK DOOR

A back door is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a back door so that the program can be accessed for trouble-shooting or other purposes. However, attackers often use back doors that they detect or install themselves, as part of an exploit. In some cases, a worm is designed to take advantage of a back door created by an earlier attack. For example, Nimda gained entrance through a back door left by Code Red.

Whether installed as an administrative tool or a means of attack, a back door is a security risk, because there are always crackers out there looking for any vulnerability to exploit. In her article "Who gets your trust?" security consultant Carole Fennelly uses an analogy to illustrate the situation: "Think of approaching a building with an elaborate security system that does bio scans, background checks, the works. Someone who doesn't have time to go through all that might just rig up a back exit so they can step out for a smoke -- and then hope no one finds out about it."

http://searchsoftwarequality.techtarget.com/glossary/

2.824.8 (EN) BACKDOOR

A backdoor is a tool installed after a compromise to give an attacker easier access to the compromised system around any security mechanisms that are in place.

http://www.sans.org/security-resources/glossary-of-terms/

2.824.9 (FR) PORTE DÉROBÉE OU BRÈCHE

Mécanisme non documenté et qui peut-être caché ou volontairement créé dans un système d'information pour contourner les mécanismes de protection. Les portes dérobées permettent par exemple à des pirates de maintenir un accès sur un système pour revenir ultérieurement sur le système.

http://www.cases.public.lu/functions/glossaire/

2.824.10 (FR) PORTE DÉROBÉE, TRAPPE ARRIÈRE

Moyen non documenté permettant d'obtenir des droits privilégiés dans une application ou un ordinateur. Dans le cas d'une application, la backdoor est souvent un bout de code ajouté par les développeurs pour contourner toute procédure de sécurité et faciliter ainsi les tests ou le dépannage: présente dans la version finale du programme, elle permet à qui en a connaissance d'exécuter l'application sans autorisation voire de s'introduire dans le système. Dans le cas d'un ordinateur, la backdoor est un petit programme installé automatiquement par un virus ou manuellement par une personne malveillante: à l'insu des utilisateurs, elle permet de prendre le contrôle à distance du système, ou lors d'une intrusion de revenir ultérieurement sans avoir à en forcer à nouveau la sécurité. Les antivirus pouvant assez facilement être pris en défaut par les backdoors, le meilleur moyen pour s'en prémunir reste de ne pas exécuter les logiciels ou fichiers joints douteux et d'installer un pare-feu afin de surveiller les entrées/sorties.

http://www.secuser.com/glossaire/

2.825 PUESTA A CEROS

2.825.1 PUESTA A CERO

Borrado de claves que se produce por acceso no autorizado a un equipo o por la pulsación de un botón o secuencia de teclas. [CESID:1997]

2.825.2 (EN) ZEROIZE

Overwrite a memory location with data consisting entirely of bits with the value zero so that the data is destroyed and not recoverable. This is often contrasted with deletion methods that merely destroy reference to data within a file system rather than the data itself. [NIST-SP800-63:2013]

2.825.3 (EN) ZERO FILL

To fill unused storage locations in an information system with the representation of the character denoting "0." [CNSSI_4009:2010]

2.825.4 (EN) ZEROIZATION

A method of erasing electronically stored data, cryptographic keys, and Credentials Service Providers (CSPs) by altering or deleting the contents of the data storage to prevent recovery of the data. [CNSSI_4009:2010]

2.825.5 (EN) ZEROIZE

To remove or eliminate the key from a cryptographic equipment or fill device. [CNSSI_4009:2010]

2.825.6 (EN) ZEROIZE

1. (I) Synonym for "erase". (See: sanitize.) Usage: Particularly with regard to erasing keys that are stored in a cryptographic module.

2. (O) Erase electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FP140]

3. (O) "To remove or eliminate the key from a cryptoequipment or fill device." [C4009]

[RFC4949:2007]

2.825.7 (EN) ZEROIZATION

method of destruction of stored data and CSPs to prevent retrieval and reuse [ISO-19790:2006]

2.825.8 (EN) ZEROISATION

Method of destruction of stored data and CSPs to prevent retrieval and reuse. [ISO-19790:2006]

2.825.9 (EN) ZEROIZATION

a method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data. [FIPS-140-2:2001]

2.826 PUNTO DE ACCESO

Acrónimos: AP

2.826.1 PUNTO DE ACCESO

En una red local inalámbrica, el punto donde se conecta a la red terrestre o cableada.

2.826.2 (EN) ACCESS POINT

the system providing access from a wireless network to a terrestrial network.

2.827 PUNTO DE ACCESO INALÁMBRICO

Acrónimos: WAP

2.827.1 PUNTO DE ACCESO INALÁMBRICO

Dispositivo que interconecta equipos inalámbricos entre sí y con la red fija, creando una red inalámbrica.

2.827.2 (EN) WIRELESS ACCESS POINT (WAP)

A device that acts as a conduit to connect wireless communication devices together to allow them to communicate and create a wireless network. [CNSSI_4009:2010]

2.828 PUNTO DE DISTRIBUCIÓN DE CRL

Ver:

- *Lista de revocación de certificados*

2.828.1 PUNTO DE DISTRIBUCIÓN DE LISTA DE REVOCACIÓN DE CERTIFICADOS

Asiento de directorio u otra fuente de distribución para las CRL; una CRL distribuida a través de un punto de distribución de CRL puede contener asientos de revocación sólo para un subconjunto del conjunto total de certificados expedidos por una autoridad de certificación o puede contener asientos de revocación para múltiples autoridades de certificación. [X.509:2005]

2.828.2 (EN) DISTRIBUTION POINT

(I) An X.500 Directory entry or other information source that is named in a v3 X.509 public-key certificate extension as a location from which to obtain a CRL that may list the certificate. [RFC4949:2007]

2.828.3 (EN) CRL DISTRIBUTION POINT

A directory entry or other distribution source for CRLs; a CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs. [X.509:2005]

2.828.4 (FR) POINT DE REPARTITION DE LISTE CRL

élément de dictionnaire ou autre source de distribution de listes CRL; une telle liste distribuée par le biais d'un point de répartition de liste CRL peut contenir des éléments révoquant uniquement un sous-ensemble de la totalité des certificats émis par une autorité de certification ou peut contenir des éléments révoquant plusieurs autorités de certification. [X.509:2005]

2.829 PURPLE

Ver:

- *JADE*
- *ENIGMA*

2.829.1 PURPLE

Sistema de cifra utilizado por el servicio diplomático japonés durante la Segunda Guerra Mundial.

2.829.2 (EN) PURPLE

Codename for the Japanese system of encrypting diplomatic messages during World War II.

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.830 RACF - RESOURCE ACCESS CONTROL FACILITY

Acrónimos: RACF

2.830.1 RACF - RESOURCE ACCESS CONTROL FACILITY

Producto de IBM que proporciona control de acceso y funciones de auditoría.

2.830.2 (EN) RACF

RACF, short for Resource Access Control Facility, is an IBM software product. It is a security system that provides access control and auditing functionality for the z/OS and z/VM operating systems. Its primary market competitors have been ACF2 and TopSecret, both now produced by Computer Associates.

In addition to being one of the most mature and scalable security monitors in computing, it has some interesting features that are not often found in Microsoft Windows or Unix environments. It can, for example, set permissions for file patterns — that is, set the permissions even for files that do not yet exist. Those permissions are then used should the file (or other object) be created at a later time. In other words, RACF establishes security policies rather than just permission records.

RACF has continuously evolved to support such modern security features as digital certificates/public key infrastructure services, LDAP interfaces, and case sensitive IDs/passwords. (The latter is a reluctant concession to promote interoperability with other systems, such as Unix and Linux.) The underlying zSeries hardware works closely with RACF. For example, digital certificates are protected within tamper-proof cryptographic processors. Major mainframe subsystems, especially DB2 Version 8, use RACF to provide multi-level security (MLS).

http://en.wikipedia.org/wiki/RACF

2.830.3 (FR) RACF - RESOURCE ACCESS CONTROL FACILITY

RACF est l'outil de gestion de la sécurité proposé par IBM sur ses environnements grands systèmes (AS/X, OS/X) et sur son système d'exploitation VM.

http://securit.free.fr/glossaire.htm

2.831 RADIUS - REMOTE ACCESS DIAL-IN USER SERVER

Acrónimos: RADIUS

Ver:

- *AAA - Autenticación, Autorización y Registro*
- *TACACS - Terminal Access Controller Access Control System*
- http://www.ietf.org/rfc/rfc5080
- http://www.ietf.org/rfc/rfc2866
- http://www.ietf.org/rfc/rfc2865

2.831.1 RADIUS

Abreviatura de “remote authentication and dial-in user service” (autenticación remota y servicio dial-in del usuario). Sistema de autenticación y cuentas. Comprueba que la información transferida al servidor RADIUS, como el nombre de usuario y la contraseña, sea correcta, para autorizar luego el acceso al sistema. Este método de autenticación se puede utilizar con un token, tarjeta inteligente, etc., para proporcionar autenticación de dos factores.

http://es.pcisecuritystandards.org

2.831.2 RADIUS

Es un protocolo estándar de AAA usado por todos los sistemas de control de acceso. [CCN-STIC-641:2006]

2.831.3 (EN) RADIUS

Abbreviation for “Remote Authentication Dial-In User Service.” Authentication and accounting system. Checks if information such as username and password that is passed to the RADIUS server is correct, and then authorizes access to the system. This authentication method may be used with a token, smart card, etc., to provide two-factor authentication.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.831.4 (EN) REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)

(I) An Internet protocol [R2865] for carrying dial-in users' authentication information and configuration information between a shared, centralized authentication server (the RADIUS server) and a network access server (the RADIUS client) that needs to authenticate the users of its network access ports. (See: TACACS.) [RFC4949:2007]

2.831.5 (EN) REMOTE ACCESS DIAL-IN USER SERVICE - RADIUS

an Internet Security protocol (RFC 2138 and RFC 2139) for authenticating remote users. [ISO-18028-4:2005]

2.831.6 (FR) RADIUS

Abréviation de «Remote authentication and Dial-In User Service», service d’usager commuté à authentification distante. Système d’authentification et de comptabilité. Vérifie si des informations comme le nom d’utilisateur et le mot de passe transmis au serveur RADIUS sont exactes, et autorise ensuite l’accès au système. Cette méthode d’authentification peut être utilisée avec un token, une carte à puce, etc., pour assurer une authentification à deux facteurs.

http://fr.pcisecuritystandards.org/

2.832 RAID

Acrónimos: RAID, RAID, RAID

2.832.1 MATRIZ REDUNDANTE DE DISCOS INDEPENDIENTES (RAID)

La matriz redundante de discos independientes (RAID) implica la combinación de dos o más unidades para mejorar el rendimiento y la tolerancia a los fallos. Además, la combinación de dos o más discos ofrece una mejora en la confiabilidad e incremento del tamaño del volumen de datos Un RAID distribuye los datos a través de los diferentes discos, pero el sistema operativo considera a este conjunto como un disco simple.

http://www.recall.es/why-recall/data-protection-terminology

2.832.2 RAID

hace referencia a un sistema de almacenamiento que usa múltiples discos duros entre los que distribuye o replica los datos. Dependiendo de su configuración (a la que suele llamarse nivel), los beneficios de un RAID respecto a un único disco son uno o varios de los siguientes: mayor integridad, mayor tolerancia a fallos, mayor throughput (rendimiento) y mayor capacidad.

http://es.wikipedia.org/wiki/RAID

2.832.3 (EN) RAID

RAID is an umbrella term for computer data storage schemes that divide and replicate data among multiple hard disk drives. RAID's various designs balance or accentuate two key design goals: increased data reliability and increased I/O (input/output) performance.

http://en.wikipedia.org/wiki/RAID

2.833 RAINBOW (TABLAS RAINBOW)

Ver:

- *Función resumen*

2.833.1 ATAQUE DE TABLAS RAINBOW

Método de ataque de datos que utiliza una tabla computarizada previa de cadenas de hash (resumen de mensaje de longitud fija) para identificar la fuente de datos original, usualmente mediante el craqueo de la contraseña o los hashes de datos del titular de la tarjeta.

http://es.pcisecuritystandards.org

2.833.2 RAINBOW TABLE ATTACK:

A method of data attack using a pre-computed table of hash strings (fixed-length message digest) to identify the original data source, usually for cracking password or cardholder data hashes.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.833.3 (FR) ATTAQUE DE TABLEAU ARC-EN-CIEL

Une méthode d'attaque de données utilisant un tableau précalculé de chaînes de hachage (digestion de message de longueur fixe) pour identifier la source d'origine des données, habituellement casser un mot de passe ou les hachages de données de titulaire de carte.

http://fr.pcisecuritystandards.org/

2.834 RANSOMWARE

2.834.1 RANSOMWARE

El ransomware es un código malicioso para secuestrar datos, una forma de explotación en la cual el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado.

El ransomware se propaga a través de archivos adjuntos de correo electrónico, programas infectados y sitios web comprometidos. Un programa de malware ransomware también puede ser llamado criptovirus, criptotroyano o criptogusano.

Los atacantes pueden usar uno de varios enfoques diferentes para extorsionar a sus víctimas:

- Después de que la víctima descubre que no puede abrir un archivo, recibe un correo electrónico con una nota de rescate exigiendo una cantidad relativamente pequeña de dinero a cambio de una clave privada. El atacante advierte que si el rescate no se paga en una fecha determinada, la clave privada será destruida y los datos se perderán para siempre.
- La víctima es engañada para que crea que es el objeto de una investigación policial. Tras ser informada de que se ha encontrado software sin licencia o contenido web ilegal en su computadora, se le da instrucciones a la víctima sobre cómo pagar una multa electrónica.
- El malware encripta subrepticiamente los datos de la víctima, pero no hace nada más. En este enfoque, el secuestrador de datos prevé que la víctima buscará en internet cómo solucionar el problema y hace dinero con la venta de software anti-ransomware en sitios web legítimos.

Para protegerse contra el secuestro de datos, los expertos insisten en que los usuarios respalden sus datos de manera regular. Si se produce un ataque, no pague un rescate. En su lugar, limpie el disco duro y restaure los datos desde su copia de seguridad.

http://searchdatacenter.techtarget.com/es/

2.834.2 (EN) RANSOMWARE

Ransomware is malware for data kidnapping, an exploit in which the attacker encrypts the victim's data and demands payment for the decryption key.

Ransomware spreads through e-mail attachments, infected programs and compromised websites. A ransomware malware program may also be called a cryptovirus, cryptotrojan or cryptoworm.

Attackers may use one of several different approaches to extort money from their victims:

- After a victim discovers he cannot open a file, he receives an email ransom note demanding a relatively small amount of money in exchange for a private key. The attacker warns that if the ransom is not paid by a certain date, the private key will be destroyed and the data will be lost forever.
- The victim is duped into believing he is the subject of an police inquiry. After being informed that unlicensed software or illegal web content has been found on his computer, the victim is given instructions for how to pay an electronic fine.
- The malware surreptitiously encrypts the victim's data but does nothing else. In this approach, the data kidnapper anticipates that the victim will look on the Internet for how to fix the problem and makes money by selling anti-ransomware software on legitimate websites.

To protect against data kidnapping, experts urge that users backup data on a regular basis. If an attack occurs, do not pay a ransom. Instead, wipe the disk drive clean and restore data from the backup.

http://whatis.techtarget.com/

2.834.3 (EN) RANSOMWARE

Malicious software created by a hacker to restrict access to the computer system that it infects and demand a ransom paid to the creator of the malicious software for the restriction to be removed. Some forms of ransomware may encrypt files on the system's hard drive, while others may simply lock the system and display messages to coax the user into paying.

http://home.mcafee.com/virusinfo/glossary

2.834.4 (EN) RANSOMWARE

Ransomware is a form of malware in which rogue software code effectively holds a user's computer hostage until a "ransom" fee is paid. Ransomware often infiltrates a PC as a computer worm or Trojan horse that takes advantage of open security vulnerabilities. Most ransomware attacks are the result of clicking on an infected e-mail attachment or visiting a hacked website.

Upon compromising a computer, ransomware will typically either lock a user's system or encrypt files on the computer and then demand payment before the system or files will be restored.

http://www.webopedia.com/TERM/R/ransomware.html

2.835 RC-2 - SISTEMA DE CIFRA DE SECRETO COMPARTIDO

Acrónimos: RC-2

Ver:

- *Cifrado en bloque*
- *Criptografía de clave secreta*
- http://en.wikipedia.org/wiki/RC2

2.835.1 RC-2 - SISTEMA DE CIFRA DE SECRETO COMPARTIDO

Algoritmo de cifra creado por Ron Rivest, coautor del RSA.

Cifra por bloques de 64 bits con una clave de tamaño variable (8 a 128 bits).

2.835.2 (EN) RC2, RC4, RC5, ETC.

A series of encryption algorithms published by RSA Security; all developed by cryptography pioneer Ron Rivest. (Rivest Cipher 2, or Ron's Code 2 = RC2) All of them are important commercial implementations of symmetric key cryptography where the entity that encrypts and the entity that decrypts both must know the same key.

RC2 was developed as a replacement for DES (Data Encryption Standard) and has been in widespread use in a number of commercial software packages, for SSL and S/MIME implementations, and others. It has had an historical advantage over its competitor, DES, in that, until the laws were liberalized in 2000, along with RC4, it had special export status. In order to be exported a relatively short key length, a weak implementation of 40 bits had to be used. E-mail and web browser interoperability across country borders was a driving factor.

http://www.rsasecurity.com/glossary/

2.835.3 (EN) RC-2 - ENCRYPTION SYSTEM BASED ON A SHARED SECRET

Block cipher designed by Ron Rivest in 1987. "RC" stands for "Ron's Code" or "Rivest Cipher"; other ciphers designed by Rivest include RC4, RC5 and RC6.

RC2 is a 64-bit block cipher with a variable size key. Its 18 rounds are arranged as a source-heavy Feistel network, with 16 rounds of one type (MIXING) punctuated by two rounds of another type (MASHING). A MIXING round consists of four applications of the MIX transformation.

http://en.wikipedia.org/wiki/RC2

2.836 RC-4 - SISTEMA DE CIFRA DE SECRETO COMPARTIDO

Acrónimos: RC-4

Ver:

- *Criptografía de clave secreta*
- *Cifrado de flujo*
- http://en.wikipedia.org/wiki/RC4

2.836.1 RC-4 - SISTEMA DE CIFRA DE SECRETO COMPARTIDO

Algoritmo de cifra creado por Ron Rivest, coautor del RSA.

Cifrador de flujo con una clave de tamaño variable.

Se utiliza ampliamente en navegadores WWW.

2.836.2 RC4 O ARC4

es el sistema de cifrado de flujo más utilizado y se usa en algunos de los protocolos más populares como Transport Layer Security (TLS/SSL) (para proteger el tráfico de Internet) y Wired Equivalent Privacy (WEP) (para añadir seguridad en las redes inalámbricas). RC4 fue excluido en seguida de los estándares de alta seguridad por los criptógrafos y algunos modos de usar el algoritmo de criptografía RC4 lo han llevado a ser un sistema de criptografía muy inseguro, incluyendo su uso WEP. No está recomendado su uso en los nuevos sistemas, sin embargo, algunos sistemas basados en RC4 son lo suficientemente seguros para un uso común.

http://es.wikipedia.org/wiki/RC4

2.836.3 (EN) RC4 (OR ARCFOUR)

is the most widely-used software stream cipher and is used in popular protocols such as Secure Sockets Layer (SSL) (to protect Internet traffic) and WEP (to secure wireless networks). While remarkable in its simplicity, RC4 falls short of the high standards of security set by cryptographers, and some ways of using RC4 lead to very insecure cryptosystems (including WEP). It is not recommended for use in new systems. However, some systems based on RC4 are secure enough for practical use.

http://en.wikipedia.org/wiki/RC4

2.837 RC-5 - SISTEMA DE CIFRA DE SECRETO COMPARTIDO

Acrónimos: RC-5

Ver:

- *Cifrado en bloque*
- *Criptografía de clave secreta*
- http://en.wikipedia.org/wiki/RC5

2.837.1 RC-5 - SISTEMA DE CIFRA DE SECRETO COMPARTIDO

Algoritmo de cifra creado por Ron Rivest, coautor del RSA.

Cifra por bloques de tamaño variable (32, 64 o 128 bits) con una clave de tamaño variable (entre 0 y 2040 bits).

2.837.2 (EN) RC-5 - ENCRYPTION SYSTEM BASED ON A SHARED SECRET

RC5 is a block cipher notable for its simplicity. Designed by Ronald Rivest in 1994, RC stands for "Rivest Cipher", or alternatively, "Ron's Code" (compare RC2 and RC4). The Advanced Encryption Standard (AES) candidate RC6 was based on RC5.

http://en.wikipedia.org/wiki/RC5

2.838 RC-6 - SISTEMA DE CIFRA DE SECRETO COMPARTIDO

Acrónimos: RC-6

Ver:

- *Cifrado en bloque*
- *Criptografía de clave secreta*
- http://en.wikipedia.org/wiki/RC6

2.838.1 RC-6 - SISTEMA DE CIFRA DE SECRETO COMPARTIDO

Algoritmo de cifra creado por Ron Rivest, coautor del RSA.

2.838.2 RC-6 - SISTEMA DE CIFRA DE SECRETO COMPARTIDO

Algoritmo de cifra basado en un secreto compartido (clave). Cifra el texto en bloques de 128 bits. Utiliza claves de 128, 192 o 256 bits.

2.838.3 RC-6 - SISTEMA DE CIFRA DE SECRETO COMPARTIDO

Unidad de cifrado por bloques de clave simétrica derivada a partir de RC5. Fue diseñada por Ron Rivest, Matt Robshaw, Ray Sidney, y Yiqun Lisa Yin para cumplir los requerimientos de la competencia de la AES. El algoritmo llegó entre los cinco finalistas y fue propuesto para los proyectos NESSIE y CRYPTREC. Es un diseño privado de la empresa RSA Security.

La unidad RC6 tiene tamaño de bloque de 128 bits y acepta claves de tamaño 128, 192 y 256 bits, pero, al igual que RC5, puede ser parametrizado para soportar una amplia variedad de longitudes

de palabra, tamaños de clave y número de vueltas. RC6 es muy similar a RC5 en estructura, utilizando rotaciones dependientes de los datos, sumas modulares y operaciones de XOR; de hecho, RC6 puede ser visto como una entremezcla de dos procesos de cifrado paralelo RC5. Sin embargo, RC6 utiliza una operación extra de multiplicación no presente en RC5 para lograr que la rotación sea dependiente de cada bit en una palabra, y no solamente de los bits menos significativos.

http://es.wikipedia.org/wiki/RC6

2.838.4 (EN) RC-6 - ENCRYPTION SYSTEM BASED ON A SHARED SECRET

Symmetric key block cipher derived from RC5. It was designed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin to meet the requirements of the Advanced Encryption Standard (AES) competition. The algorithm was one of the five finalists, and was also submitted to the NESSIE and CRYPTREC projects. It is proprietary of RSA Security.

RC6 proper has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits, but, like RC5, it can be parameterised to support a wide variety of word-lengths, key sizes and number of rounds. RC6 is very similar to RC5 in structure, using data-dependent rotations, modular addition and XOR operations; in fact, RC6 could be viewed as interweaving two parallel RC5 encryption processes. However, RC6 does use an extra multiplication operation not present in RC5 in order to make the rotation dependent on every bit in a word, and not just the least significant few bits.

http://en.wikipedia.org/wiki/RC6

2.839 REBAJAR EL NIVEL

Ver:

- *Información clasificada*
- *Desclasificar*

2.839.1 REBAJAR EL NIVEL

Rebajar el nivel de clasificación de una cierta información sin alterar su contenido.

2.839.2 (EN) DOWNGRADE

(I) /data security/ Reduce the security level of data (especially the classification level) without changing the information content of the data. (Compare: downgrade.) [RFC4949:2007]

2.839.3 (EN) DOWNGRADE ATTACK

(I) A type of man-in-the-middle attack in which the attacker can cause two parties, at the time they negotiate a security association, to agree on a lower level of protection than the highest level that could have been supported by both of them. (Compare: downgrade.) [RFC4949:2007]

2.839.4 DOWNGRADE.

A determination that classified informa-tion requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect a lower degree of protection. [DoD 5220:2006]

2.840 RECOGIDA DE PISTAS DE AUDITORÍA

Ver:

- *Auditoría*

2.840.1 REGISTRO DE AUDITORÍA

También denominado “pista de auditoría”. Registro cronológico de las actividades del sistema. Esta herramienta proporciona una pista independientemente verificable que permite la reconstrucción, revisión y evaluación de la secuencia de entornos y actividades que rodean o conducen a las operaciones, los procedimientos o eventos relacionados a una transacción desde el inicio hasta los resultados finales.

http://es.pcisecuritystandards.org

2.840.2 RECOGIDA DE PISTAS DE AUDITORÍA

recolección de datos relativos a eventos de seguridad de la información con el propósito de ser utilizados para revisión, análisis y monitorización continua.

2.840.3 (EN) AUDIT LOG

Also referred to as “audit trail.” Chronological record of system activities. Provides an independently verifiable trail sufficient to permit reconstruction, review, and examination of sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from inception to final results.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.840.4 (EN) AUDIT LOG

A chronological record of system activities. Includes records of system accesses and operations performed in a given period. [CNSSI_4009:2010]

2.840.5 (EN) AUDIT REDUCTION TOOLS

Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. These tools generally remove records generated by specified classes of events, such as records generated by nightly backups. [CNSSI_4009:2010]

2.840.6 (EN) AUDIT TRAIL

A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result. [CNSSI_4009:2010]

2.840.7 (EN) AUDIT LOGGING

the gathering of data on information security events for the purpose of review and analysis, and ongoing monitoring. [ISO-18028-1:2006]

2.840.8 (FR) JOURNAL D'AUDIT

Également appelé «vérification à rebours». Enregistrement chronologique des activités du système. Il fournit un suivi vérifiable et indépendant suffisant pour autoriser la reconstitution, la vérification et l'examen de l'ordre des environnements et activités impliqués dans une opération, une procédure ou un événement lors d'une transaction, du début au résultat final.

http://fr.pcisecuritystandards.org/

2.841 RECOMMENDED

Ver:

- http://www.ietf.org/rfc/rfc2119

2.841.1 (EN) SHOULD

This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

2.842 RECORTE DE REGISTROS

2.842.1 RECORTE DE REGISTROS

Recorte o eliminación de los registros del sistema con objeto de ocultar actividades comprometedoras.

2.842.2 (EN) LOG CLIPPING

Log clipping is the selective removal of log entries from a system log to hide a compromise.

http://www.sans.org/security-resources/glossary-of-terms/

2.843 RECUPERACIÓN

Ver:

- *Gestión de incidentes*
- *Restablecimiento de la seguridad*
- *Opción de recuperación*

2.843.1 RECUPERACIÓN

1. [criptografía] Recuperación del texto original a través del criptoanálisis.
2. [integridad de los sistemas] Retorno del sistema a un modo de operación seguro tras un incidente accidental o un ataque deliberado.
3. [desastres] Reconstrucción del sistema tras un desastre.

2.843.2 (EN) RECOVERY

The phase in the incident response plan that ensures that affected systems or services are restored to a condition specified in the service delivery objectives (SDOs) or business continuity plan (BCP)

ISACA, Cybersecurity Glossary, 2014

2.843.3 (EN) RECOVERY ACTION

Execution of a response or task according to a written procedure

ISACA, Cybersecurity Glossary, 2014

2.843.4 (EN) RECOVERY

1. (I) /cryptography/ The process of learning or obtaining cryptographic data or plain text through cryptanalysis. (See: key recovery, data recovery.)

2a. (I) /system integrity/ The process of restoring a secure state in a system after there has been an accidental failure or a successful attack. (See: secondary definition under "security", system integrity.)

2b. (I) /system integrity/ The process of restoring an information system's assets and operation following damage or destruction. (See: contingency plan.)

[RFC4949:2007]

2.844 RECUPERACIÓN DE CLAVES

Ver:

- *Claves encapsuladas*
- *Depósito de claves*
- *Clave*
- *Clave criptográfica*

2.844.1 RECUPERACIÓN DE CLAVES

Término general que engloba a los distintos sistema de gestión de claves en los que se deposita parte o la totalidad de la clave empleada para cifrar, de modo que se permita una posterior recuperación de los mensajes cifrados mediante un procedimiento distinto al empleo del canal normal de comunicación. (v. Depósito de claves). [CESID:1997]

2.844.1 (EN) KEY RECOVERY

Mechanisms and processes that allow authorized parties to retrieve the cryptographic key used for data confidentiality. [CNSSI_4009:2010]

2.844.2 (EN) KEY RECOVERY

1. (I) /cryptanalysis/ A process for learning the value of a cryptographic key that was previously used to perform some cryptographic operation. (See: cryptanalysis, recovery.)

2. (I) /backup/ Techniques that provide an intentional, alternate means to access the key used for data confidentiality service in an encrypted association. [DoD4] (Compare: recovery.)

[RFC4949:2007]

2.844.3 (EN) KEY RECOVERY

A function in the lifecycle of keying material; mechanisms and processes that allow authorized entities to retrieve keying material from key backup or archive. [NIST-SP800-57:2007]

2.845 RED DE CONFIANZA

Ver:

- *Confianza*

2.845.1 RED DE CONFIANZA

Confianza transitiva. Si A confía en B, y B confía en C, B puede presentarle a A suficientes garantías como para que A llegue a confiar en C "porque B lo asegura". Las relaciones de confianza puede llegar a configurar una verdadera red.

2.845.2 (EN) WEB OF TRUST

(D) /PGP/ A PKI architecture in which each certificate user defines their own trust anchor(s) by depending on personal relationships. (See: trust anchor. Compare: hierarchical PKI, mesh PKI.) [RFC4949:2007]

2.845.3 (EN) WEB OF TRUST

A web of trust is the trust that naturally evolves as a user starts to trust other's signatures, and the signatures that they trust.

http://www.sans.org/security-resources/glossary-of-terms/

2.846 RED PRIVADA VIRTUAL

Acrónimos: RPV (es), VPN

Ver:

- *Túnel*
- *IPsec - IP security*

2.846.1 VPN

Acrónimo de “virtual private network” (red privada virtual). Una red informática donde algunas conexiones son circuitos virtuales dentro de redes más extensas, como Internet, en lugar de conexiones directas por medio de cables físicos. Cuando este es caso, los puntos finales de una red virtual se transmiten a través de una red mayor. Al contrario de una aplicación común, formada por comunicaciones seguras en la red pública, una red VPN puede presentar o no funciones de seguridad, como la autenticación y el cifrado de contenidos.

Una VPN se puede utilizar con un token, tarjeta inteligente, etc., para proporcionar autenticación de dos factores.

http://es.pcisecuritystandards.org

2.846.2 RED PRIVADA VIRTUAL

Las redes privadas virtuales, también conocidas por sus siglas VPN (Virtual Private Network), son una clase de redes que se configuran dentro de una red pública. Para establecerlas, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado.

http://www.inteco.es/glossary/Formacion/Glosario/

2.846.3 RED PRIVADA VIRTUAL

Mecanismo que permite el establecimiento de una comunicación segura y flexible entre dos nodos, entre un nodo y una red o entre dos redes cuando dicha comunicación ha de atravesar un medio inseguro. [CCN-STIC-401:2007]

2.846.4 RED PRIVADA VIRTUAL

Conexión segura entre dos extremos que utiliza como base una red insegura, normalmente Internet. [CCN-STIC-612:2006]

2.846.5 (EN) VPN

Acronym for “virtual private network.” A computer network in which some of connections are virtual circuits within some larger network, such as the Internet, instead of direct connections by physical wires. The end points of the virtual network are said to be tunneled through the larger network when this is the case. While a common application consists of secure communications through the public Internet, a VPN may or may not have strong security features such as authentication or content encryption. A VPN may be used with a token, smart card, etc., to provide two-factor authentication.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.846.6 (EN) VIRTUAL PRIVATE NETWORK (VPN)

Protected information system link utilizing tunneling, security controls (see Information Assurance), and endpoint address translation giving the impression of a dedicated line. [CNSSI_4009:2010]

2.846.7 (EN) VIRTUAL PRIVATE NETWORK (VPN)

(I) A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (e.g., the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network. (See: tunnel.) [RFC4949:2007]

2.846.8 (EN) VIRTUAL PRIVATE NETWORK

Restricted-use logical computer network that is constructed from the system resources of a physical network, e.g. by using encryption and/or by tunneling links of the virtual network across the real network. [ISO-18028-1:2006]

2.846.9 (EN) VIRTUAL PRIVATE NETWORK - VPN

a private network utilising shared networks. E.g., A network based on a cryptographic tunnelling protocol operating over another network infrastructure. [ISO-18028-4:2005]

2.846.10 (EN) VIRTUAL PRIVATE NETWORK

Virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks. [NIST-SP800-77:2005]

2.846.11 (EN) VIRTUAL PRIVATE NETWORKS (VPN)

A VPN is the application of encryption, data integrity,and authentication protocols to provide a secure connection between a D/A and a remote device or user. The authentication controls restrict the connection ability to only authorized users; the encryption controls ensure data confidentiality between the D/A and the remote device/user; the data integrity controls protect the data from modification during transit between the D/A and the remote user. When the data stream itself is also encrypted, the use of VPNs to send already-encrypted communications through an encrypted tunnel constitutes a form of double encryption.

Mobile Security Reference Architecture, May 23, 2013

2.846.12 (EN) VIRTUAL PRIVATE NETWORK (VPN)

A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network. For example, if a corporation has LANs at several different sites, each connected to the Internet by a firewall, the corporation could create a VPN by (a) using encrypted tunnels to connect from firewall to firewall across the Internet and (b) not allowing any other traffic through the firewalls. A VPN is generally less expensive to build and operate than a dedicated real network, because the virtual network shares the cost of system resources with other users of the real network.

http://www.sans.org/security-resources/glossary-of-terms/

2.846.13 (FR) VPN

Acronyme de «virtual private network», réseau privé virtuel. Réseau informatique dans lequel certaines connexions sont des circuits virtuels au sein d'un réseau plus important, comme Internet, remplaçant les connexions directes par des câbles physiques. Les points terminaux du réseau virtuel sont alors tunnelisés à travers le réseau de plus grande dimension. Alors qu'une application commune consiste en plusieurs communications sécurisées par le réseau Internet public, un VPN peut comporter ou non des fonctionnalités de sécurité, comme l'authentification ou le cryptage de

contenu. Un VPN peut être utilisé avec un token, une carte à puce, etc., pour assurer une authentification à deux facteurs.

http://fr.pcisecuritystandards.org/

2.846.14 (FR) VPN (VIRTUAL PRIVATE NETWORK)

Réseau d'ordinateurs constituant un sous-réseau privé permettant l'échange d'informations à travers des réseaux d'une autre topologie comme si les ordinateurs en communication étaient situés au sein d'un même réseau local. Ces liaisons correspondent à des chemins protégés empruntant les réseaux publics comme Internet. Généralement, les VPN sont chiffrés afin de garantir la confidentialité des informations échangées.

http://www.cases.public.lu/functions/glossaire/

2.846.15 (FR) VPN - VIRTUAL PRIVATE NETWORK (RESEAU PRIVE VIRTUEL)

Un VPN est un réseau de données qui utilise les moyens de télécommunications d'un réseau public en ajoutant des services de sécurité et des protocoles de tunneling.

Internet est en général utilisé pour établir un VPN pour des raisons de coûts.

http://securit.free.fr/glossaire.htm

2.847 RED TRAMPA

Ver:

- *Sistema trampa*

2.847.1 RED TRAMPA

Red de sistemas que simulan una red real pero han sido desplegados para engañar a posibles intrusos.

2.847.2 HONEY POT

En español, Tarro de miel. Es un sistema diseñado para analizar cómo los intrusos emplean sus armas para intentar entrar en un sistema -analizan las vulnerabilidades- y alterar, copiar o destruir sus datos o la totalidad de éstos -por ejemplo, borrando el disco duro del servidor-. Por medio del aprendizaje de sus herramientas y métodos se puede, entonces, proteger mejor los sistemas. Pueden constar de diferentes aplicaciones, una de ellas sirve para capturar al intruso o aprender cómo actúan sin que ellos sepan que están siendo vigilados.

http://www.inteco.es/glossary/Formacion/Glosario/

2.847.3 (EN) HONEYNET:

A virtual environment consisting of multiple honeypots, designed to deceive an intruder into thinking that he or she has located a network of computing devices of targeting value.

The Tallinn Manual, 2013

2.847.4 (EN) HONEY NET

A network of honeypots.

2.847.5 (EN) HONEY NET

A honeynet is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security.

http://searchtechtarget.techtarget.com/glossaryBrowseAlpha/

2.847.6 (EN) HONEYNET

Honeypot built to appear to be an entire collection or variety of systems, or a system of honeypots and intrusion detection systems designed to collect information on a broader scale than a single honeypot can manage.

2.848 REFLECTION_ATTACK

2.848.1 (EN) REFLECTION ATTACK

An attacker can abuse an authentication protocol susceptible to reflection attack in order to defeat it. Doing so allows the attacker illegitimate access to the target system, without possessing the requisite credentials. Reflection attacks are of great concern to authentication protocols that rely on a challenge-handshake or similar mechanism. An attacker can impersonate a legitimate user and can gain illegitimate access to the system by successfully mounting a reflection attack during authentication.

Attack Execution Flow

- The attacker opens a connection to the target server and sends it a challenge
- The server responds by returning the challenge encrypted with a shared secret as well as its own challenge to the attacker
- Since the attacker does not possess the shared secret, he initiates a second connection to the server and sends it, as challenge, the challenge received from the server on the first connection
- The server treats this as just another handshake and responds by encrypting the challenge and issuing its own to the attacker
- The attacker now receives the encrypted challenge on the second connection and sends it as response to the server on the first connection, thereby successfully completing the handshake and authenticating to the server.

Attack Pattern 90

http://capec.mitre.org/data/index.html

2.849 REGISTRO DE ACTIVIDAD

2.849.1 REGISTRAR

Contabilizar, enumerar los casos reiterados de alguna cosa o suceso. "Registraron cuidadosamente todas sus entradas y salidas."

DRAE. Diccionario de la Lengua Española.

2.849.2 REGISTRO

Registro de la actividad de los usuarios: tiempo de conexión, servicios utilizados, datos accedidos, etc. Los datos recogidos se utilizan para obtener estadísticas, planificar ampliaciones de capacidad, facturación de servicios, auditoría y asignación de costes, entre otros fines.

2.849.3 LOG

Un log es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (who, what, when, where y why) un evento ocurre para un dispositivo en particular o aplicación.

http://www.inteco.es/glossary/Formacion/Glosario/

2.849.4 LOGGING / LOG

Registro de actividades. [CCN-STIC-641:2006]

2.849.5 TRAZAS DE REGISTRO (LOG)

Registro de información de una aplicación o sistema con el objetivo de conservar el estado y actividad en sus diferentes intervalos de tiempo. Es vital la sincronización de tiempo para su integridad y correlación entre dispositivos. [CCN-STIC-400:2006]

2.849.6 (EN) LOG:

A log is a file used to record activities or events. generated by a variety of devices. including computer operating systems. applications. network switches and routers. and virtually any computing device. There is no standard for the common format or structure of a log. [knapp:2014]

2.849.7 (EN) LOG MANAGEMENT:

Log management is the process of collecting and storing logs for purposes of log analysis and data forensics. and/or for purposes of regulatory compliance and account- ability. Log management typically involves collection of logs. some degree of normalization or categorization. and short-term (for analysis) and long-term storage (for compliance). [knapp:2014]

2.849.8 (EN) LOGGING

Systematically recording specified events in the order that they occurred to provide a data trail for subsequent analysis.

http://www.qtsnet.com/SecuritySolutions/security_glossary.html

2.849.9 (EN) LOG

A record of actions and events that take place on a computer. Logging creates a record of actions and events that take place on a computer.

http://www.symantec.com/avcenter/refa.html

2.849.10 (FR) LOG / LOGGING

Processus qui enregistre généralement sous forme d'un fichier texte avec la date et l'heure les opérations effectuées (connexions, accès aux ressources, évènements, erreurs?) par des utilisateurs ou des processus sur un système, un serveur ou une application.

http://www.cases.public.lu/functions/glossaire/

2.850 REGISTRO DE AUDITORÍA

Ver:

- *Auditoría*

2.850.1 REGISTRO DE AUDITORÍA

Unidad discreta de datos registrados en la pista de auditoría sobre la ocurrencia de un suceso. Un registro de auditoría consiste en un conjunto de descriptores, cada uno de los cuales tiene un conjunto de atributos asociados. Cada registro tiene siempre un descriptor de auditoría para los campos de cabecera y, normalmente, un descriptor de auditoría adicional, que detalla el (los) sujeto(s) y objeto(s) involucrados en el suceso. [Ribagorda:1997]

2.850.2 REGISTRO DE AUDITORÍA DE SEGURIDAD

Conjunto de datos recogidos, y si procede usados, para llevar a cabo una auditoría de seguridad (ISO-7498-2).

Es término sinónimo de "registro de auditoría".

[Ribagorda:1997]

2.850.3 (EN) AUDIT RECORD

The audit information saved to the audit log.

The audit record contains the following information:

- Audit event
- SAP user ID and client, if known
- Terminal name
- Transaction code
- Report name
- Time and date when the event occurred
- Process ID

- Session number
- Additional information

http://help.sap.com/saphelp_glossary/en/

2.851 REGISTRO DE CLAVES

Ver:

- *Clave*
- *Clave criptográfica*

2.851.1 REGISTRO DE CLAVES

Notarización por una autoridad de una cierta clave.

2.851.2 (EN) KEY REGISTRATION

A function in the lifecycle of keying material; the process of officially recording the keying material by a registration authority. [NIST-SP800-57:2007]

2.852 RELLENADO DE TRÁFICO

Ver:

- *Análisis de tráfico*

2.852.1 RELLENADO DE TRÁFICO

Generación y transmisión de nuestras espurias de comunicación, unidas de datos espurios o datos espurios dentro de las unidades de datos (ISO-7498-2).

Según la citada norma es el mecanismo de seguridad encargado de suministrar el servicio de confidencialidad del tráfico de datos.

[Ribagorda:1997]

2.852.2 TRÁFICO DE RELLENO

Mecanismo de seguridad que, a base de lanzar por la red mensajes sin contenido, consigue que haya un flujo constante de mensajes, dificultando el análisis de flujo de tráfico. [CESID:1997]

2.852.3 RELLENO DE TRÁFICO

Generación de instancias de comunicación espurias, de unidades de datos/o datos espurios en las unidades de datos. [ISO-7498-2:1989]

2.852.4 (EN) TRAFFIC PADDING

(I) "The generation of spurious instances of communication, spurious data units, and/or spurious data within data units." [ISO-7498-2] [RFC4949:2007]

2.852.5 (EN) TRAFFIC PADDING

The generation of spurious instances of communication, spurious data units and/or spurious data within data units. [ISO-7498-2:1989]

2.852.6 (FR) BOURRAGE

Production d'instances de communication parasites, d'unités de données parasites et/ou de données parasites dans des unités de données. [ISO-7498-2:1989]

2.853 RENOVACIÓN DEL CERTIFICADO

Ver:

- *Certificado X.509*

2.853.1 RENOVACIÓN DEL CERTIFICADO

Prórroga del periodo de validez de un certificado electrónico. Se realiza por medio de la emisión de un nuevo certificado.

2.854 REPLICACIÓN DE DISCOS

[disk_shadowing = replicación de discos]]

2.854.1 REPLICACIÓN DE DISCOS

Mecanismo de respaldo consistente en que los datos se graban simultáneamente en dos discos físicos o dos servidores.

2.854.2 (EN) DISK SHADOWING

A back-up process that involves writing images to two physical disks or servers simultaneously.

http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-b-glossary.aspx

2.855 REPUDIO

Ver:

- *No repudio*

2.855.1 REPUDIO

Denegación, por una de las entidades implicadas en un a comunicación, de haber participado en la totalidad o en parte de dicha comunicación (ISO-7498-2). [Ribagorda:1997]

2.855.2 REPUDIO

Negación de una de las partes que intervinieron en una comunicación de haber participado total o parcialmente en ella. [CESID:1997]

2.855.3 REPUDIO

Negación de una de las entidades implicadas en una comunicación de haber participado en toda la comunicación o en parte de ella. [ISO-7498-2:1989]

2.855.4 (EN) REPUDIATION

1. (I) Denial by a system entity that was involved in an association (especially a communication association that transfers data) of having participated in the relationship. (See: accountability, non-repudiation service.)

2. (I) A type of threat action whereby an entity deceives another by falsely denying responsibility for an act. (See: deception.)

Usage: This type of threat action includes the following subtypes:

- False denial of origin: Action whereby an originator denies responsibility for sending data.
- False denial of receipt: Action whereby a recipient denies receiving and possessing data.

3. (O) /OSIRM/ "Denial by one of the entities involved in a communication of having participated in all or part of the communication." [ISO-7498-2]

[RFC4949:2007]

2.855.5 (EN) REPUDIATION

Denial by one of the entities involved in a communication of having participated in all or part of the communication. [ISO-7498-2:1989]

2.855.6 (FR) RÉPUDIATION

Le fait, pour une des entités impliquées dans la communication, de nier avoir participé aux échanges, totalement ou en partie. [ISO-7498-2:1989]

2.856 REQUIRED

Ver:

- http://www.ietf.org/rfc/rfc2119

2.856.1 (EN) MUST

This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

2.857 RESILIENCIA

2.857.1 RESILIENCIA

1. f. Psicol. Capacidad humana de asumir con flexibilidad situaciones límite y sobreponerse a ellas.

2. f. Mec. Capacidad de un material elástico para absorber y almacenar energía de deformación.

DRAE. Diccionario de la Lengua Española.

2.857.2 RESILIENCIA

Capacidad de los sistemas para seguir operando pese a estar sometidos a un ciberataque, aunque sea en un estado degradado o debilitado. Así mismo, incluye la capacidad de restaurar con presteza sus funciones esenciales después de un ataque.

2.857.3 RESILIENCIA:

Capacidad de adaptación de una organización en un entorno complejo y cambiante.[UNE Guía 73:2010]

2.857.4 RESISTENCIA

(Diseño del Servicio) La habilidad de un Elemento de Configuración o Servicio de TI a resistir Fallos o de Recuperarse rápidamente tras un Fallo. Por ejemplo, un cable reforzado resistirá fallos cuando esté bajo estrés.

Ver Tolerancia a Fallos.

[ITIL:2007]

2.857.5 RESISTENCIA

La capacidad de un sistema o red para recuperarse de forma automática de una interrupción, por lo general con un efecto reconocible mínimo. [COBIT:2006]

2.857.6 (EN) RESILIENCE

the ability of a substance to return to its original shape after it has been bent, stretched or pressed

Oxford Advanced Learner's Dictionary.

2.857.7 (EN) RESILIENCE

The ability of a system or network to resist failure or to recover quickly from any disruption, usually with minimal recognizable effect

ISACA, Cybersecurity Glossary, 2014

2.857.8 (EN) RESILIENCE

the ability of systems to operate while under attack, even in a degraded or debilitated state, and to rapidly recover operational capabilities for essential functions after a successful attack. The concept of information system resilience can also be applied to the other classes of threats, including threats from environmental disruptions and/or human errors of omission/commission. [CSS US:2012]

2.857.9 (EN) RESILIENCE

generally as the capacity of an information system or network to continue to operate despite incidents, or to carry on normal operations smoothly notwithstanding technical problems.

OECD, Cybersecurity Policy Making at a Turning Point, 2012

2.857.10 (EN) NETWORK RESILIENCE

A computing infrastructure that provides continuous business operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged), rapid recovery if failure does occur, and the ability to scale to meet rapid or unpredictable demands. [CNSSI_4009:2010]

2.857.11 RESILIENCE

adaptive capacity of an organization in a complex and changing environment [ISO Guide 73:2009]

2.857.12 (EN) RESILIENCE:

ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions

Extended Definition:

1) ability of systems, infrastructures, government, business, and citizenry to resist, absorb recover from, or adapt to an adverse occurrence that may cause harm, destruction, or loss of national significance

2) capacity of an organization to recognize threats and hazards and make adjustments that will improve future protection efforts and risk reduction measures

Annotation: Resilience can be factored into vulnerability and consequence estimates when measuring risk.

DHS Risk Lexicon, September 2008

2.857.13 (EN) RESILIENCE

(Service Design) The ability of a Configuration Item or IT Service to resist Failure or to Recover quickly following a Failure. For example, an armoured cable will resist failure when put under stress.

See Fault Tolerance.

[ITIL:2007]

2.857.14 (EN) RESILIENCE

The ability of a system or network to recover automatically from any disruption, usually with minimal recognisable effect. [COBIT:2006]

2.857.15 (EN) RESILIENCE

The capability of an IT infrastructure, including physical, personnel, IT, and operational security controls, to maintain essential services and protect critical assets while preempting and repelling attacks and minimizing the extend of corruption and compromise.

Complete Guide to Security and Privacy Metrics, D.S. Herrmann, Auerbach Publications, 2007.

2.857.16 (EN) RESILIENCY

The ability of an organization to recover from a significant disruption and resume critical operations.

http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-b-glossary.aspx

2.857.17 (EN) RESILIENCY TESTING

Testing of an institution's business continuity and disaster recovery resumption plans.

http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-b-glossary.aspx

2.857.18 (FR) RÉSILIENCE

capacité d'adaptation d'un organisme dans un environnement complexe et changeant [ISO Guide 73:2009]

2.857.19 (FR) RÉSILIENCE

(Conception de services) La capacité d'un élément de configuration ou d'un service des TI à résister à une panne ou à avoir une reprise rapide suite à une défaillance. Par exemple, un câble blindé résistera mieux à la défaillance lorsqu'il sera soumis à une tension.

Voir Tolérance de panne.

[ITIL:2007]

2.858 RESISTENTE A COLISIONES

Ver:

- *Hash*
- *Colisión*

2.858.1 RESISTENTE A COLISIONES

Propiedad de una función, tal que es computacionalmente imposible construir distintos mensajes de entrada que den la misma salida (ISO/IEC ISO-10118-1) [Ribagorda:1997]

2.858.2 (EN) COLLISION-RESISTANT HASH-FUNCTION

A hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output.

NOTE. Computational feasibility depends on the specific security requirements and environment.

[ISO-10118-1:2000]

2.859 RESPONSABLE DE LA INFORMACIÓN

Ver:

- *Información*
- *Propietario de la información*

2.859.1 RESPONSABLE DE LA INFORMACIÓN

Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad. [CCN-STIC-801:2010]

2.859.2 (EN) INFORMATION OWNER

Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, classification, collection, processing, dissemination, and disposal. See also information steward.

NIST 800-53: Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

[CNSSI_4009:2010]

2.860 RESPONSABLE DEL SISTEMA DE INFORMACIÓN

Ver:

- *Sistema de información*

2.860.1 RESPONSABLE DEL SISTEMA

Persona que se encarga de la explotación del sistema de información. [CCN-STIC-801:2010]

2.860.2 (EN) INFORMATION SYSTEM OWNER (OR PROGRAM MANAGER)

Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. [NIST-SP800-53:2013]

2.861 RESPONSABLE DE SEGURIDAD CORPORATIVA

Acrónimos: CSO

Ver:

- *Responsable de seguridad de la información*
- *Responsable de seguridad del sistema*
- *Criptocustodio*

2.861.1 RESPONSABLE DE SEGURIDAD CORPORATIVA

Persona encargada de velar por la armonización de la seguridad de la información en sus diferentes vertientes: protección física, protección de los servicios y respeto de la privacidad.

2.861.2 (EN) CHIEF SECURITY OFFICER (CSO)

The person usually responsible for all security matters both physical and digital in an enterprise

ISACA, Cybersecurity Glossary, 2014

2.861.3 (EN) CHIEF SECURITY OFFICER (CSO)

A CSO has the responsibility for global and enterprisewide information security; he/she is also responsible for the physical security, protection services and privacy of the corporation and its employees. In other words, the CSO is responsible for coordinating all corporate activities with security implications.

http://www.csoonline.com/glossary/

2.862 RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

Acrónimos: CIO

Ver:

- *Responsable de seguridad de la información*
- *Responsable de seguridad del sistema*
- *Criptocustodio*

2.862.1 RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

El responsable de seguridad de la información es un cargo dentro de organizaciones preocupadas por la seguridad de la información. Típicamente reporta a responsables ejecutivos de operaciones o finanzas.

2.862.2 (EN) CHIEF INFORMATION OFFICES (CIO)

Agency official responsible for: 1) providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information systems are acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; 2) developing, maintaining, and facilitating the implementation of a sound and integrated information system architecture for the agency; and 3) promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

Note: Organizations subordinate to federal agencies may use the term Chief Information Officer to denote individuals filling positions with similar security responsibilities to agency-level Chief Information Officers. [CNSSI_4009:2010]

2.862.3 (EN) CHIEF INFORMATION OFFICER

Agency official responsible for:

(i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency;

(ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and

(iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

[NIST-SP800-53:2013] [FIPS-200:2006]

2.862.4 (EN) CHIEF INFORMATION OFFICER

The chief information officer or CIO is a job title for the head of information technology group within an organization. They often report to the chief executive officer or chief financial officer. In military organizations, they report to the commanding officer or commanding general of the organization.

http://en.wikipedia.org/wiki/Chief_Information_Officer

2.863 RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

Acrónimos: CISO

Ver:

- *Responsable de seguridad corporativa*
- *Responsable de seguridad del sistema*
- *Criptocustodio*

2.863.1 RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

Persona encargada de velar por la seguridad de la información de la organización. Su labor consiste en estar al día de la evolución tecnológica en la medida en que afecta a la seguridad de la información, estableciendo puentes entre el responsable de seguridad corporativa y los responsables de tecnología. No suele incluir entre sus responsabilidades la seguridad física, ni la gestión de riesgos, ni la continuidad de las operaciones.

2.863.2 (EN) CHIEF INFORMATION SECURITY OFFICER (CISO)

The person in charge of information security within the enterprise

ISACA, Cybersecurity Glossary, 2014

2.863.3 (EN) CISO (CHIEF INFORMATION SECURITY OFFICER)

The CISO (chief information security officer) is a senior-level executive responsible for aligning security initiatives with enterprise programs and business objectives, ensuring that information assets and technologies are adequately protected.

http://whatis.techtarget.com/

2.863.4 (EN) CHIEF INFORMATION SECURITY OFFICER

See 'Senior Agency Information Security Officer'. [NIST-SP800-53:2013]

2.863.5 (EN) CHIEF INFORMATION SECURITY OFFICES (CISO)

See Senior Agency Information Security Officer. [CNSSI_4009:2010]

2.863.6 (EN) SENIOR AGENCY INFORMATION SECURITY OFFICER (SAISO)

Official responsible for carrying out the Chief Information Officer responsibilities under the Federal Information Security Management Act (FISMA) and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information systems security officers.

Note: Organizations subordinate to federal agencies may use the term Senior Information Security Officer or Chief Information Security Officer to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers. [CNSSI_4009:2010]

2.863.7 (EN) SENIOR (AGENCY) INFORMATION SECURITY OFFICER

Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.

Note: Organizations subordinate to federal agencies may use the term *Senior Information Security Officer* or *Chief Information Security Officer* to denote individuals filling positions with similar responsibilities to *Senior Agency Information Security Officers*.

U.S. Code 44, Sec. 3544. Federal agency responsibilities, 2007

2.863.8 (EN) CHIEF INFORMATION SECURITY OFFICER (CISO)

The position of CISO is relatively new in most organizations. The CISO should be providing tactical information security advice and examining the ramifications of new technologies. In most corporations the CISO reports to the CIO or CTO. The CISO role does not usually include responsibility for physical security, risk management and business continuity, which are more often delegated to the CSO.

http://www.csoonline.com/glossary/

2.864 RESPONSABLE DE SEGURIDAD DEL SISTEMA

Acrónimos: SSO

Ver:

- *Responsable de seguridad corporativa*
- *Responsable de seguridad de la información*
- *Criptocustodio*

2.864.1 RESPONSABLE DE SEGURIDAD DEL SISTEMA

Responsable de que se cumple la política de seguridad relativa a un sistema de información.

2.864.2 JEFE DE SEGURIDAD

Principal responsable de los asuntos relacionados con la seguridad de una entidad.

http://es.pcisecuritystandards.org

2.864.3 (EN) INFORMATION SYSTEMS SECURITY OFFICER (ISSO)

Individual assigned responsibility for maintaining the appropriate operational security posture for an information system or program. [CNSSI_4009:2010]

2.864.4 (EN) SYSTEM SECURITY OFFICER (SSO)

(I) A person responsible for enforcement or administration of the security policy that applies to a system. (Compare: manager, operator.) [RFC4949:2007]

2.864.5 (EN) SECURITY OFFICER

Primary responsible person for an entity's security-related affairs.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.864.6 (FR) RESPONSABLE DE LA SÉCURITÉ

La principale personne responsable des questions liées à la sécurité d'une entité.

http://fr.pcisecuritystandards.org/

2.865 RESTABLECIMIENTO DE LA SEGURIDAD

2.865.1 RESTABLECIMIENTO DE SEGURIDAD

Acciones que se ejecutan y procedimientos que se aplican cuando se detecta o se sospecha que se ha producido una infracción de la seguridad. [X.810:1995]

2.865.2 (EN) SECURITY RECOVERY

Actions that are taken and procedures that are carried out when a violation of security is either detected or suspected to have taken place. [X.810:1995]

2.865.3 (FR) RÉTABLISSEMENT DE LA SÉCURITÉ

actions qui sont menées et procédures qui sont utilisées lorsqu'une violation de sécurité est soit détectée soit soupçonnée d'avoir eu lieu. [X.810:1995]

2.866 RESTOS (BUSCAR ENTRE LOS)

Ver:

- *Basuring en memoria*
- *Basura (buscar entre la)*

2.866.1 RESTOS (BUSCAR ENTRE LOS)

Obtención de información a base de rebuscar en restos abandonados por programas o procesos a su terminación.

2.866.2 (EN) SCAVENGING

Searching through object residue to acquire data. [CNSSI_4009:2010]

2.866.3 (EN) SCAVENGING

Searching through data residue in a system to gain unauthorized knowledge of sensitive data.

http://www.sans.org/security-resources/glossary-of-terms/

2.867 RESUMEN CRIPTOGRÁFICO

Ver:

- *Hash code*
- *Valor resumen*
- *Función resumen*
- *Hash*

2.867.1 RESUMEN

Es término sinónimo de: "autenticador", "huella digital" y "valor de verificación criptográfico". [Ribagorda:1997]

2.867.2 (EN) MESSAGE DIGEST

(D) Synonym for "hash result". (See: cryptographic hash.) [RFC4949:2007]

2.868 RETO

Ver:

- *Pregunta-respuesta*

2.868.1 RETO

Dato que se remite a la entidad que deseamos autenticar a fin de que, combinándolo con la información secreta, demuestre que la conoce sin revelarla.

2.868.2 (EN) CHALLENGE

A random message created using a PRNG mechanism to be sent to another party for authentication purposes.

2.868.3 (EN) CHALLENGE

Procedure parameter used in conjunction with secret parameters to produce a response. [ISO-9798-5:2004]

2.869 REUTILIZACIÓN

Ver:

- *Terminación de soportes de información*
- *Soporte*

2.869.1 REUTILIZACIÓN

Utilización de un soporte de información para contener una nueva información tras haberse asegurado de que no quedan restos de la información previa.

2.869.2 (EN) OBJECT REUSE

Reassignment and re-use of a storage medium containing one or more objects after ensuring no residual data remains on the storage medium. [CNSSI_4009:2010]

2.870 REVENTADO DE CONTRASEÑAS

Ver:

- *Contraseña*

2.870.1 REVENTADO DE CONTRASEÑAS

Determinación de contraseñas de usuarios a partir del conocimiento de la contraseña cifrada (o del fichero de contraseñas cifradas).

2.870.2 (EN) PASSWORD CRACKING

Password cracking is the process of attempting to guess passwords, given the password file information.

http://www.sans.org/security-resources/glossary-of-terms/

2.871 REVENTAR

Ver:

- *Cracker*

2.872 REVISIÓN DE CÓDIGO

2.872.1 REVISIÓN DE CÓDIGO

Revisión manual o automatizada de un programa, usualmente de su código fuente.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/risk/248-BSI.html

2.872.2 (EN) CODE REVIEW

A manual or automated review of computer software, usually source code.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/risk/248-BSI.html

2.873 REVOCACIÓN DE UNA CLAVE

Ver:

- *Clave*
- *Clave criptográfica*

2.873.1 REVOCACIÓN DE UNA CLAVE

Eliminación de una clave de los sistemas y dispositivos que la usan, con anterioridad al periodo previsto de uso.

2.873.2 (EN) KEY REVOCATION

A function in the lifecycle of keying material; a process whereby a notice is made available to affected entities that keying material should be removed from operational use prior to the end of the established cryptoperiod of that keying material. [NIST-SP800-57:2007]

2.874 RFID - IDENTIFICACIÓN POR RADIO FRECUENCIA

Acrónimos: RFID

2.874.1 RFID

(siglas de Radio Frequency IDentification, en español Identificación por radiofrecuencia) es un sistema de almacenamiento y recuperación de datos remoto que usa dispositivos denominados etiquetas, transpondedores o tags RFID. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio. Las tecnologías RFID se agrupan dentro de las denominadas Auto ID (Automatic Identification, o Identificación Automática).

Una etiqueta RFID es un dispositivo pequeño, similar a una pegatina, que puede ser adherida o incorporada a un producto, animal o persona. Contienen antenas para permitirles recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID. Las etiquetas pasivas no necesitan alimentación eléctrica interna, mientras que las activas sí lo requieren. Una de las ventajas del uso de radiofrecuencia (en lugar, por ejemplo, de infrarrojos) es que no se requiere visión directa entre emisor y receptor.

http://es.wikipedia.org/wiki/RFID

2.874.2 (EN) RFID - RADIO FREQUENCY IDENTIFICATION

a wireless technology used by smartcards and tags.

2.875 RIESGO

Ver:

- *Gestión de riesgos*
- *Apreciación de los riesgos*
- *Identificación de los riesgos*
- *Propietario del riesgo*

- *Análisis de riesgos*
- *consecuencia*
- *nivel de riesgo*
- *Evaluación de riesgos*
- *Tlerancia al riesgo*
- *Tratamiento del riesgo*
- *Control*
- *Riesgo residual*
- *Asunción del riesgo*

2.875.1 RIESGO

Efecto de la incertidumbre sobre la consecución de los objetivos. [UNE-ISO GUÍA 73:2010]

NOTA 1 Un efecto es una desviación, positiva y/o negativa, respecto a lo previsto.

NOTA 2 La incertidumbre es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un suceso, de sus consecuencias o de su probabilidad.

NOTA 3 Con frecuencia, el riesgo se caracteriza por referencia a sucesos potenciales y a sus consecuencias o una combinación de ambas

NOTA 4 Con frecuencia, el riesgo se expresa en términos de combinación de las consecuencias de un suceso (incluyendo los cambios en las circunstancias) y de su probabilidad.

NOTA 5: En el contexto de sistemas de gestión de la seguridad de la información, los riesgos de seguridad de la información se pueden expresar como el efecto de la incertidumbre sobre los objetivos de seguridad de la información.

NOTA 6: El riesgo de seguridad de la información se relaciona con la posibilidad de que las amenazas exploten vulnerabilidades de un activo o grupo de activos de información y causen daño a una organización.

[UNE-ISO/IEC 27000:2014]

2.875.2 RIESGO

Efecto de la incertidumbre sobre la consecución de los objetivos.

NOTA 4. Con frecuencia, el riesgo se expresa en términos de combinación de las consecuencias de un suceso (incluyendo los cambios en las circunstancias) y de su probabilidad.

[ISO Guía 73:2010]

2.875.3 RIESGO

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. [UNE-71504:2008]

2.875.4 RIESGOS POTENCIALES

Los riesgos del sistema de información en la hipótesis de que no hubieran salvaguardas presentes. [UNE-71504:2008]

2.875.5 RIESGO

Un posible Evento que podría causar daño o pérdidas, o afectar la habilidad de alcanzar Objetivos. Un Riesgo es medido por la probabilidad de una Amenaza, la Vulnerabilidad del Activo a esa Amenaza, y por el Impacto que tendría en caso que ocurriera. [ITIL:2007]

2.875.6 RIESGO

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. [Magerit:2012]

2.875.7 RIESGO

Probabilidad de que una amenaza se materialice aprovechando una vulnerabilidad causando daño (impacto) en un proceso o sistema. [CCN-STIC-401:2007]

2.875.8 RIESGO

El potencial de que una amenaza específica explote las debilidades de un activo o grupo de activos para ocasionar pérdida y/o daño a los activos. Por lo general se mide por medio de una combinación del impacto y la probabilidad de ocurrencia. [COBIT:2006]

2.875.9 RIESGO ACUMULADO

Dícese del calculado tomando en consideración el valor propio de un acti-vo y el valor de los activos que depende de él. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma. [Magerit:2012]

2.875.10 RIESGO REPERCUTIDO

Dícese del calculado tomando en consideración únicamente el valor propio de un activo. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma, medidas ambas sobre ac-tivos de los que depende. [Magerit:2012]

2.875.11 RIESGO

Probabilidad de que una vulnerabilidad propia de un sistema de información sea explotada por las amenazas a dicho sistema, con el objetivo de penetrarlo. [CESID:1997]

2.875.12 (EN) RISK

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, February 12, 2014

2.875.13 (EN) RISK

effect of uncertainty on objectives [ISO Guide 73:2009]

NOTE 1: An effect is a deviation from the expected — positive or negative.

NOTE 2: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

NOTE 3: Risk is often characterized by reference to potential events and consequences, or a combination of these.

NOTE 4: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

NOTE 5: In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives.

NOTE 6: Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

[ISO/IEC 27000:2014]

2.875.14 (EN) RISK

effect of uncertainty on objectives

NOTE 4. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

[ISO Guide 73:2009]

2.875.15 (EN) BUSINESS RISK

A probable situation with uncertain frequency and magnitude of loss (or gain) [RiskIT-PG:2009]

2.875.16 (EN) INHERENT RISK

The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls) [RiskIT-PG:2009]

2.875.17 (EN) IT RISK

The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise [RiskIT-PG:2009]

2.875.18 (EN) IT RISK ISSUE

1: An instance of an IT risk

2: A combination of control, value and threat conditions that impose a noteworthy level of IT risk

[RiskIT-PG:2009]

2.875.19 (EN) RISK

potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences

Extended Definition: potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence

Annotation:

1) Risk is defined as the potential for an unwanted outcome. This potential is often measured and used to compare different future situations.

2) Risk may manifest at the strategic, operational, and tactical levels.

DHS Risk Lexicon, September 2008

2.875.20 (EN) RISK

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:

(i) the adverse impacts that would arise if the circumstance or event occurs; and

(ii) the likelihood of occurrence.

Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. [FIPS 200, Adapted]

[NIST-SP800-53:2013]

2.875.1 (EN) RISK

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.

Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

[CNSSI_4009:2010]

2.875.2 (EN) RISK

1. (I) An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result. (See: residual risk.)

2. (O) /SET/ "The possibility of loss because of one or more threats to information (not to be confused with financial or business risk)." [SET2]

[RFC4949:2007]

2.875.3 (EN) RISK

A possible Event that could cause harm or loss, or affect the ability to achieve Objectives. A Risk is measured by the probability of a Threat, the Vulnerability of the Asset to that Threat, and the Impact it would have if it occurred. [ITIL:2007]

2.875.4 (EN) RISK

The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss and/or damage to the assets. It usually is measured by a combination of impact and probability of occurrence. [COBIT:2006]

2.875.5 (EN) RISK

The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. [FIPS-200:2006]

2.875.6 (EN) RISK

As used in this guideline, the term 'risk' means a combination of:

- the likelihood that a particular vulnerability in an agency information system will be either intentionally or unintentionally exploited by a particular threat resulting in a loss of confidentiality, integrity, or availability, and
- the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability will have on agency operations (including mission, functions, and public confidence in the agency), an agencys assets, or individuals (including privacy) should there be a threat exploitation of information system vulnerabilities.

[NIST-SP800-60V2:2004]

2.875.7 (EN) RISK

A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting adverse impact. Reducing either the threat or the vulnerability reduces the risk. [TDIR:2003]

2.875.8 (EN) RISK

A measure of the exposure to which a system or potential system may be subjected. [CRAMM:2003]

2.875.9 (EN) IT-RELATED RISK

The net mission/business impact (probability of occurrence combined with impact) from a particular threat source exploiting, or triggering, a particular information technology vulnerability. IT related-risks arise from legal liability or mission/business loss due to:

- Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information.
- Non-malicious errors and omissions.
- IT disruptions due to natural or man-made disasters.
- Failure to exercise due care and diligence in the implementation and operation of the IT.

[NIST-SP800-33:2001]

2.875.10 (EN) RISK

Flaws and bugs lead to risk. Risks are not failures. Risks capture the probability that a flaw or a bug will impact the purpose of the software. Risk measures also take into account the potential damage that can occur. A very high risk is not only likely to happen but also likely to cause great harm. Risks can be managed by technical and non-technical means.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/risk/248-BSI.html

2.875.11 (EN) RISK

Risks capture the likelihood that a vulnerability will be exploited, as well as the potential damage (impact) that will occur if it is. It is important to note that risks, threats, and exploits are all separate things. Risks may be present in the target software, on the target host, or in the broader operational environment of the software.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/attack/590-BSI.html

2.875.12 (EN) RISK

A measure of the potential degree to which protected information is subject to loss through adversary exploitation.

http://www.ioss.gov/docs/definitions.html

2.875.13 (EN) TOTAL RISK

The potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability). [TDIR:2003]

2.875.14 (EN) RISK

The uncertainty that can create exposure to undesired future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to impede the achievement of an organization's objectives.

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

2.875.15 RISK

In the context of RIDM, risk is the potential for shortfalls, which may be realized in the future, with respect to achieving explicitly-stated performance commitments. The performance shortfalls may be related to institutional support for mission execution, or related to any one or more of the following mission execution domains: safety, technical, cost, schedule.

As applied to CRM, risk is characterizedas a set of triplets:

a. The scenario(s) leading to degraded performance in one or more performance measures,
b. The likelihood(s) of those scenarios,
c. The consequence(s), impact, or severity of the impact on performance that would result if those scenarios were to occur.

Uncertainties are included in the evaluation of likelihoods and consequences.

NASA Risk Management Handbook, NASA/SP-2011-3422, Version 1.0, November 2011

2.875.16 (FR) RISQUE

effet de l'incertitude sur l'atteinte des objectifs [ISO Guide 73:2009]

2.875.17 (FR) RISQUE

Un événement possible pouvant causer une déficience ou une perte, ou affecter la possibilité d'atteindre des objectifs. Un risque se mesure par la probabilité d'une menace, la vulnérabilité d'un actif à cette menace et l'impact qu'il aurait s'il se produisait. [ITIL:2007]

2.875.18 (FR) RISQUE

Incertitude que peut engendrer l'exposition à des événements ou résultats non désirés. Il s'agit de l'expression de la probabilité et de l'incidence d'un événement susceptible de nuire à la réalisation des objectifs d'une organisation.

http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578

2.876 RIESGO RESIDUAL

Ver:

- *Riesgo*

2.876.1 RIESGO RESIDUAL

Riesgo remanente después del tratamiento del riesgo.

NOTA 1 El riesgo residual puede contener riesgos no identificados.

NOTA 2 El riesgo residual también se puede conocer como "riesgo retenido".

[UNE-ISO GUÍA 73:2010] [UNE-ISO/IEC 27000:2014]

2.876.2 RIESGOS RESIDUALES

Riesgos remanentes que existen después de que se hayan tomado las medidas de seguridad. [UNE-71504:2008]

2.876.3 RIESGO RESIDUAL

Riesgo remanente después del tratamiento del riesgo.

NOTA 1. El riesgo residual puede contener riesgos no identificados.

NOTA 2. El riesgo residual también se puede conocer como "riesgo retenido".

[UNE Guía 73:2010]

2.876.4 (EN) RESIDUAL RISK

risk remaining after risk treatment

NOTE 1: Residual risk can contain unidentified risk.

NOTE 2: Residual risk can also be known as “retained risk”.

[ISO Guide 73:2009] [ISO-27000:2014]

2.876.1 (EN) RESIDUAL RISK

Portion of risk remaining after security measures have been applied. [CNSSI_4009:2010]

2.876.2 (EN) RESIDUAL RISK

risk remaining after risk treatment

NOTE 1. Residual risk can contain unidentified risk.

NOTE 2. Residual risk can also be known as “retained risk”.

[ISO Guide 73:2009]

2.876.3 (EN) RESIDUAL RISK

The remaining risk after management has implemented risk response. [RiskIT-PG:2009]

2.876.4 (EN) RISK INDICATOR

A metric capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk tolerance. [RiskIT-PG:2009]

2.876.5 (EN) RESIDUAL RISK:

risk that remains after risk management measures have been implemented

DHS Risk Lexicon, September 2008

2.876.6 (EN) RESIDUAL RISK

(I) The portion of an original risk or set of risks that remains after countermeasures have been applied. (Compare: acceptable risk, risk analysis.) [RFC4949:2007]

2.876.7 (EN) RESIDUAL RISK

The potential for the occurrence of an adverse event after adjusting for the impact of all in-place safeguards. [TDIR:2003]

2.876.8 (EN) RESIDUAL RISK

The remaining, potential risk after all IT security measures are applied. There is a residual risk associated with each threat. [NIST-SP800-33:2001]

2.876.9 (FR) RISQUE RÉSIDUEL

risque subsistant après le traitement du risque

NOTE 1. Un risque résiduel peut inclure un risque non identifié.

NOTE 2. Un risque résiduel peut également être appelé «risque pris»

[ISO Guide 73:2009]

2.877 RIPEMD

Acrónimos: RIPEMD

Ver:

- *Hash*
- http://en.wikipedia.org/wiki/RIPEMD

2.877.1 RIPEMD-160

(acrónimo de RACE Integrity Primitives Evaluation Message Digest, primitivas de integridad del resumen del mensaje) es un algoritmo del resumen del mensaje de 160 bits (y función criptográfica de hash) desarrollado en Europa por Hans Dobbertin, Antoon Bosselaers y Bart Preneel, y publicados primeramente en 1996. Es una versión mejorada de RIPEMD, que estaba basado sobre los principios del diseño del algoritmo MD4, y es similar en seguridad y funcionamiento al más popular SHA-1.

También existen versiones de 128, 256 y 320 bits de este algoritmo, llamadas RIPEMD-128, RIPEMD-256 y RIPEMD-320 respectivamente. La versión 128 bits fue pensada solamente como un reemplazo para el RIPEMD original, que eran también de 128 bits, y en la que habían sido encontradas razones para cuestionar su seguridad. Las versiones de 256 y 320 bits solamente disminuyen la posibilidad de colisiones hash accidentales, y no tienen niveles más altos de seguridad con respecto a RIPEMD-128 y RIPEMD-160.

http://es.wikipedia.org/wiki/RIPEMD-160

2.877.2 (EN) RIPEMD

RIPEMD-160 is a 160-bit message digest algorithm (and cryptographic hash function) developed in Europe by Hans Dobbertin, Antoon Bosselaers and Bart Preneel, and first published in 1996. It is an improved version of RIPEMD, which in turn was based upon the design principles used in MD4, and is similar in performance to the more popular SHA-1.

There also exist 128, 256 and 320-bit versions of this algorithm, called RIPEMD-128, RIPEMD-256, and RIPEMD-320, respectively. The 128-bit version was intended only as a drop-in replacement for the original RIPEMD, which was also 128-bit, and which had been found to have questionable security. The 256 and 320-bit versions diminish only the chance of accidental collision, and don't have higher levels of security as compared to, respectively, RIPEMD-128 and RIPEMD-160.

http://en.wikipedia.org/wiki/RIPEMD

2.878 ROBO DE IDENTIDADES

Ver:

- *Identidad*

- *Impostura*
- *Fraude de identidad*

2.878.1 SUPLANTACIÓN DE IDENTIDAD

Es la actividad maliciosa en la que un atacante se hace pasar por otra persona. Los motivos pueden ser el fraude, acoso o cyberbulling.

Un ejemplo es, en las redes sociales, crear un perfil de otra persona e interactuar con otros usuarios haciéndose pasar por ella.

http://www.inteco.es/glossary/Formacion/Glosario/

2.878.2 ROBO DE IDENTIDADES

Se dice cuando un atacante se hace con los medios de identificación de una entidad de tal forma que puede utilizarlos para suplantar efectivamente la identidad de la entidad. Habitualmente, se roban identidades bien para suplantar a la víctima, bien para obtener información personal de la misma.

2.878.3 (EN) IDENTITY THEFT

While there is no generally accepted definition nor consistent use of the term, identity theft commonly involves criminal acts of fraudulently (without his or her knowledge or consent) obtaining and using another person's identity information. The term "identity fraud" is sometimes used as a synonym, although it also encompasses the use of a false, not necessarily real, identity.

Cybercrime Convention Committee (T-CY)

2.878.4 (EN) IDENTITY THEFT

Identity theft is the theft of the credentials that we use to do business. When access controls are inadequate, the credentials that people use to authenticate to their credit card companies, banks or shopping sites may be disclosed to the wrong people. In addition, thieves have developed many ways to use e-mail and the Internet to collect this information.

Once perpetrators have the information they can use it as if they were the victim, running up credit card debt, or taking money out of bank accounts or investment savings.

http://www.rsasecurity.com/glossary/

2.878.5 (EN) IDENTITY THEFT

is where a crook obtains key pieces of personal information, such as Social Security number, drivers license information, name, address, mothers maiden name, and more so that they can impersonate a real person. The crook can then assume that persons identity. There are really two variants here: a crook can open new accounts in a victims name, this is referred to true account identity theft, or the crook can use the personal information to gain access to victims existing accounts, which is often referred to as account takeover identity theft.

http://idtheft.about.com/od/glossaryofterms/Identity_Theft_Glossary_of_Terms.htm

2.878.6 (EN) IDENTITY THEFT

Identity theft is a crime in which an imposter obtains key pieces of personal information, such as Social Security or driver's license numbers, in order to impersonate someone else. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials. In addition to running up debt, an imposter might provide false identification to police, creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen.

http://searchsecurity.techtarget.com/

2.879 ROBO DE SESIÓN

2.879.1 SESSION HIJACKING

Session hijacking, also known as TCP session hijacking, is a method of taking over a Web user session by surreptitiously obtaining the session ID and masquerading as the authorized user. Once the user's session ID has been accessed (through session prediction), the attacker can masquerade as that user and do anything the user is authorized to do on the network.

http://searchsoftwarequality.techtarget.com/glossary/

2.879.2 (EN) SESSION HIJACK ATTACK

An attack in which the Attacker is able to insert himself or herself between a Claimant and a Verifier subsequent to a successful authentication exchange between the latter two parties. The Attacker is able to pose as a Subscriber to the Verifier or vice versa to control session data exchange. Sessions between the Claimant and the Relying Party can also be similarly compromised. [NIST-SP800-63:2013]

2.879.3 (EN) SESSION HIJACKING

Take over a session that someone else has established.

2.879.4 (EN) SESSION HIJACKING

An intrusion technique whereby a hacker sends a command to an already existing connection between two machines, in order to wrest control of the connection away from the machine that initiated it. The hacker's goal is to gain access to a server while bypassing normal authentication measures.

http://www.watchguard.com/glossary/

2.879.5 (EN) SESSION STEALING

See session hijacking

http://www.watchguard.com/glossary/

2.879.6 (EN) SESSION HI-JACKING

The result of a users session being compromised by an attacker. The attacker could reuse this stolen session to masquerade as the user.

http://www.webappsec.org/projects/glossary/

2.879.7 (EN) SESSION ID

A string of data provided by the web server, normally stored within a cookie or URL. A Session ID tracks a users session, or perhaps just his current session, as he traverse the web site.

http://www.webappsec.org/projects/glossary/

2.879.8 (EN) SESSION MANIPULATION

An attack technique used to hi-jack another users session by altering a session ID or session credential value.

http://www.webappsec.org/projects/glossary/

2.879.9 (EN) SESSION PREDICTION

An attack technique used to create fraudulent session credentials or guess other users current session IDs. If successful, an attacker could reuse this stolen session to masquerade as another user.

http://www.webappsec.org/projects/glossary/

2.879.10 (EN) SESSION REPLAY

When a web site permits an attacker to reuse old session credentials or session IDs for authorization.

http://www.webappsec.org/projects/glossary/

2.879.11 (EN) HIJACK ATTACK

A form of active wiretapping in which the attacker seizes control of a previously established communication association.

http://www.sans.org/security-resources/glossary-of-terms/

2.880 ROGUEWARE

Ver

- *Scareware*

2.880.1 EL ROGUE SOFTWARE

(en español, software bandido o también falso antivirus) es un tipo de programa informático malintencionado cuya principal finalidad es hacer creer que una computadora está infectada por algún tipo de virus, induciendo a pagar una determinada suma de dinero para eliminarlo.

http://es.wikipedia.org/wiki/Rogue_software

2.880.2 (EN) ROGUEWARE

The Rogueware threat consists of any kind of fake software that cybercriminals distribute (e.g. via social engineering techniques) in order to lure users to their malicious intentions.

ENISA Threat Landscape [Deliverable – 2012-09-28]

2.880.3 (EN) ROGUE SECURITY SOFTWARE

is a form of Internet fraud using computer malware (malicious software) that deceives or misleads users into paying money for fake or simulated removal of malware (so is a form of ransomware)—or it claims to get rid of malware, but instead introduces malware to the computer. Rogue security software has become a growing and serious security threat in desktop computing in recent years (from 2008 on).

http://en.wikipedia.org/wiki/Rogue_security_software

2.881 ROJO

Ver

- *negro*

2.881.1 ROJO

En entornos de seguridad de la información, se refiere a los elementos que manejan información sensible o clasificada sin cifrar (en claro).

2.881.2 (EN) RED

In cryptographic systems, refers to information or messages that contain sensitive or classified information that is not encrypted. See also BLACK. [CNSSI_4009:2010]

2.881.3 (EN) RED NETWORK:

A "red network“ typically refers to a trusted network. in contrast to a "black network." which is less secured. When discussing unidirectional communications in critical networks. traffic is typically only allowed outward from the red network to the black network. to allow supervisory data originating from critical assets to be collected and utilized by less secure SCADA systems. In other use cases, such as data integrity and fraud prevention. traffic may only he allowed from the black network into the red network, to prevent access to classified data once they have been stored. [knapp:2014]

2.882 ROL

Ver:

- *Control de acceso por roles*

2.882.1 ROL

papel: función que alguien o algo cumple.

DRAE. Diccionario de la Lengua Española.

2.882.2 ROL

Perfil al que se pueden adscribir usuarios. Define un conjunto de derechos de acceso a un sistema. Un usuario puede disfrutar de uno o más roles, siempre y cuando no sean incompatibles entre sí.

2.882.3 ROL

Conjunto de responsabilidades, Actividades y autorizaciones concedidas a una persona o equipo. Un Rol se define en un Proceso. Una persona o equipo puede tener múltiples Roles, por ejemplo, los Roles de Administrador de Configuración y Administrador del Cambio pueden ser llevados a cabo por una misma persona y de manera individual. [ITIL:2007]

2.882.4 (EN) ROLE

the function or position that sb has or is expected to have in an organization, in society or in a relationship

Oxford Advanced Learner's Dictionary.

2.882.5 (EN) ROLE

1. (I) A job function or employment position to which people or other system entities may be assigned in a system. (See: role- based access control. Compare: duty, billet, principal, user.)

2. (O) /Common Criteria/ A pre-defined set of rules establishing the allowed interactions between a user and the TOE.

[RFC4949:2007]

2.882.6 (EN) ROLE

A set of responsibilities, Activities and authorities granted to a person or team. A Role is defined in a Process. One person or team may have multiple Roles, for example the Roles of Configuration Manager and Change Manager may be carried out by a single person. [ITIL:2007]

2.882.7 (EN) ROLE

security attribute associated to a user defining the user access rights or limitations to services of a cryptographic module. One or more services may be associated to a role. A role may be associated to one or more users and a user may assume one or more roles. [ISO-19790:2006]

2.882.8 (EN) ROLE

a predefined set of rules establishing the allowed interactions between a user and the TOE.

TOE - Target of Evaluation

[CC:2006]

2.882.9 (FR) RÔLE

Un ensemble de responsabilités, d'activités et d'autorités attribuées à une personne ou à une équipe. Le rôle est défini dans un processus. Une personne ou une équipe peut avoir plusieurs rôles, par exemple, les rôles de Gestionnaire des configurations et de Gestionnaire des changements peuvent être attribués à une même personne. [ITIL:2007]

2.883 ROOTKIT

2.883.1 ROOTKIT

Es una herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo. Está disponible para una amplia gama de sistemas operativos.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.883.2 ROOTKIT

Tipo de software malicioso que, al instalarse sin autorización, es capaz de pasar desapercibido y tomar el control administrativo de un sistema informático.

http://es.pcisecuritystandards.org

2.883.3 (EN) ROOTKIT:

Malware installed on a compromised computer that allows a cyber operator to maintain privileged access to that computer and to conceal the cyber operator's activities there from other users of that or another computer.

The Tallinn Manual, 2013

2.883.4 (EN) ROOTKIT

A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means. [CNSSI_4009:2010]

2.883.5 (EN) ROOTKIT

A collection of files that is installed on a system to alter the standard functionality of the system in a malicious and stealthy way. [NIST-SP800-83:2005]

2.883.6 (EN) ROOTKIT

A set of tools used by an attacker after gaining root-level access to a host to conceal the attackers activities on the host and permit the attacker to maintain root-level access to the host through covert means. [NIST-SP800-61:2004]

2.883.7 (EN) ROOTKIT:

Type of malicious software that when installed without authorization, is able to conceal its presence and gain administrative control of a computer system.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.883.8 (EN) ROOTKIT

A collection of tools (programs) that a hacker uses to mask intrusion and obtain administrator-level access to a computer or computer network.

http://www.sans.org/security-resources/glossary-of-terms/

2.883.9 (EN) ROOTKIT

Can be either hardware or software used to gain administrative (root) control over a computer without detection. Rootkits target the BIOS, hypervisor, kernel, or boot loader. A rootkit is used to provide a hacker will full access, via a backdoor, to a machine.

PC Security Handbook, Rich Robinson

2.883.10 (EN) ROOTKIT

A rootkit is a component that uses stealth to maintain a persistent and undetectable presence on the machine. Actions performed by a rootkit, such as installation and any form of code execution, are done without end user consent or knowledge.

Rootkits do not infect machines by themselves like viruses or worms, but rather, seek to provide an undetectable environment for malicious code to execute. Attackers will typically leverage vulnerabilities in the target machine, or use social engineering techniques, to manually install rootkits. Or, in some cases, rootkits can be installed automatically upon execution of a virus or worm or simply even by browsing to a malicious website.

Once installed, an attacker can perform virtually any function on the system to include remote access, eavesdropping, as well as hide processes, files, registry keys and communication channels.

http://www.symantec.com/avcenter/refa.html

2.883.11 (FR) ROOTKIT

Il s'agit d'un groupe de logiciels mis au point par un pirate pour prendre le contrôle d'une machine. Généralement ces outils sont utilisés pour corrompre des machines Unix d'où l'utilisation de la référence root. Le rootkit propose une panoplie d'outils pirates tels que des programmes de craquage de mots de passe, des sniffers, l'installation d'un cheval de Troie etc. Une fois le rootkit installé, celui-ci corrompt les commandes standards (listage de fichiers, listage des processus actifs?) en les remplaçant par les commandes du rootkit ce qui permet d'offrir apparemment le même type de fonctionnalités à l'utilisateur du système mais en réalité dissimule la présence du rootkit sur le système par la modification des sorties écran pour en enlever toute référence au rootkit et rendre invisible ou le plus discret possible sa présence sur le système.

http://www.cases.public.lu/functions/glossaire/

2.883.12 (FR) ROOTKIT

Logiciel, ensemble de logiciels voire de techniques permettant à un individu malveillant ayant accès à un ordinateur d'en devenir administrateur (utilisateur spécifique possédant les droits les plus étendus et susceptible d'accomplir les actions les plus diverses) et de s'y maintenir en dissimulant son activité aux yeux du système. Le terme rootkit peut secondairement être utilisé pour désigner un programme non malicieux à partir du moment où ce dernier est capable de dissimuler son existence et son activité aux utilisateurs ainsi qu'aux moyens de détection classiques (antivirus, antispywares), sans pour autant permettre la prise de contrôle de l'ordinateur.

http://www.secuser.com/glossaire/

2.883.13 (FR) ROOTKIT

Ensemble de programmes destinés à compromettre une machine, majoritairement de type Unix, un rootkit est en général installé par un cheval de Troie et a pour but principal de remplacer les commandes standards (ex.: ls, netstat, ifconfig...) par des binaires malicieux permettant à un pirate d'obtenir des informations ou de prendre le contrôle total de la machine.

La présence d'un rootkit est difficile a détecter. On utilise souvent des outils de calcul d'empreintes (ex.: Tripwire) pour s'assurer que les binaires utilisés sont d'origine et n'ont pas subi de modification malveillante.

http://securit.free.fr/glossaire.htm

2.884 ROUTER CON FILTROS

Ver:

- *Guardia*
- *Pasarela de seguridad*
- *Filtrado de paquetes*
- *Filtrado de paquetes con estado*
- *Filtro de entrada*

2.884.1 ROUTER CON FILTROS

Router de interconexión que selecciona qué paquetes deja pasar y cuales no, según una cierta política de seguridad establecida.

2.884.2 (EN) FILTERING ROUTER

(I) An internetwork router that selectively prevents the passage of data packets according to a security policy. (See: guard.) [RFC4949:2007]

2.885 RSA - RIVEST, SHAMIR Y ADELMAN

Acrónimos: RSA

Ver:

- *Criptografía de clave pública*
- *Firma digital*

- http://en.wikipedia.org/wiki/RSA

2.885.1 RSA - RIVEST, SHAMIR Y ADELMAN

Cifrado asimétrico ideado por Rivest, Shamir y Adelman y publicado en 1978. Se basa en operaciones de potenciación en aritmética modular y su fortaleza radica en la dificultad de factorizar números extraordinariamente grandes. Es, con gran diferencia, la técnica asimétrica de uso más generalizado.

Su longitud de clave (pública y privada) es variable, siendo valores usuales: 512, 1024 o 2048 bits.

Frente a otras técnicas asimétricas presenta la ventaja de poderse emplear también en la firma digital.

[Ribagorda:1997]

2.885.2 RSA - RIVEST, SHAMIR Y ADELMAN

Criptosistema de clave pública, diseñado en 1978 que basa su seguridad en la dificultad de factorizar grandes números. Puede ser usado, tanto para cifrar como para producir firmas digitales. [CESID:1997]

2.885.3 (EN) RSA

algorithm for public-key cryptography. It was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

http://en.wikipedia.org/wiki/RSA#Padding_schemes

2.885.4 (FR) RSA

Algorithme créé par Rivest, Shamir et Adleman (RSA) en 1977, et basé sur la cryptographie asymétrique, RSA est l'algorithme le plus utilisé dans le monde et offre les services de sécurité essentiels tels que l'authentification, la confidentialité, l'intégrité et la signature.

RSA connaît un essor important avec les développement des infrastructures de gestion de clés (PKI).

Anciennement propriété de la société RSA Security, mais ouvert au domaine public depuis la fin 2000, l'algorithme RSA repose sur la difficulté de factoriser un grand nombre suivant ses facteurs premiers.

Les clés asymétriques utilisées dans le cadre de RSA sont classiquement de taille 512, 1024, 2048, 4096 bits. On considère à l'heure actuelle qu'une clé de 512 bits à une durée de résistance trop faible pour être utilisée.

http://securit.free.fr/glossaire.htm

2.886 S/KEY - SECURE KEY

Acrónimos: S/Key

Ver:

- http://www.ietf.org/rfc/rfc1760
- *Contraseña de un solo uso*

2.886.1 S/KEY - SECURE KEY

Mecanismo de seguridad que genera series de palabras de paso de un sólo uso. Las palabras de paso se pueden verificar fácilmente; pero son [computacionalmente] imposibles de generar salvo por el usuario auténtico.

2.886.2 (EN) S/KEY

(I) A security mechanism that uses a cryptographic hash function to generate a sequence of 64-bit, one-time passwords for remote user login. [R1760] [RFC4949:2007]

2.886.3 (EN) S/KEY

A security mechanism that uses a cryptographic hash function to generate a sequence of 64-bit, one-time passwords for remote user login. The client generates a one-time password by applying the MD4 cryptographic hash function multiple times to the user's secret key. For each successive authentication of the user, the number of hash applications is reduced by one.

http://www.sans.org/security-resources/glossary-of-terms/

2.887 S/MIME - SECURE MULTIPURPOSE MAIL EXTENSION

Acrónimos: S/MIME

2.887.1 S/MIME

Extensiones de Correo de Internet de Propósitos Múltiples / Seguro) es un estándar para criptografía de clave pública y firmado de correo electrónico encapsulado en MIME.

http://es.wikipedia.org/wiki/S/MIME

2.887.2 (EN) SECURE/MULTIPURPOSE INTERNET MAIL EXTENSIONS (S/MIME)

A set of specifications for securing electronic mail. Secure/ Multipurpose Internet Mail Extensions (S/MIME) is based upon the widely used MIME standard and describes a protocol for adding cryptographic security services through MIME encapsulation of digitally signed and encrypted objects. The basic security services offered by S/MIME are authentication, non-repudiation of origin, message integrity, and message privacy. Optional security services include signed receipts, security labels, secure mailing lists, and an extended method of identifying the signer’s certificate(s). [CNSSI_4009:2010]

2.887.3 (EN) SECURITY/MULTIPURPOSE INTERNET MAIL EXTENSIONS - S/MIME

a protocol providing secure multipurpose mail exchange. Its current version 3 consists of five parts: RFC 3369 and RFC 3370 define the message syntax, RFC 2631 to RFC 2633 define message specification, certificate handling and key agreement method. [ISO-18028-4:2005]

2.887.4 (EN) S/MIME (SECURE MULTIPURPOSE MAIL EXTENSION)

A proposed standard for encrypting and authenticating MIME data, which is used primarily for Internet e-mail.

http://www.watchguard.com/glossary/

2.887.5 (FR) S/MIME - SECURE MULTI-PURPOSE INTERNET MAIL EXTENSIONS

S/MIME est un protocole de chiffrement de messages électroniques reposant sur la technique de cryptographie asymétrique RSA.

S/MIME fournit des services de sécurité pour assurer l'authenticité d'un message et sa confidentialité. Le format des messages S/MIME est défini dans le standard PKCS #7 (Public Key Cryptography System).

http://securit.free.fr/glossaire.htm

2.888 SAFER - SECURE AND FAST ENCRYPTION ROUTINE

Acrónimos: SAFER

Ver:

- *Cifrado en bloque*
- *Criptografía de clave secreta*
- http://en.wikipedia.org/wiki/SAFER

2.888.1 SAFER - SECURE AND FAST ENCRYPTION ROUTINE

Algoritmo de cifra basado en un secreto compartido (clave). Cifra el texto en bloques de 64 bits. Utiliza claves de 64 (K-64 y SK-64) o 128 bits (K-128 y SK-128).

2.888.2 SAFER

Algoritmo público de cifrado en bloque diseñado por J. Massey para Cylink Corp. La versión SAFER K-64 cifra bloques de 64 bits con longitud de claves de 64 bits y la SAFER K-128 emplea dos claves de 64 bits cada una. [CESID:1997]

2.888.3 (EN) SAFER

The Secure And Fast Encryption Routine with 64-bit key algorithm was introduced by J. L. f block ciphers designed primarily by James Massey (one of the designers of IDEA) on behalf of Cylink Corporation. The early SAFER K and SAFER SK designs share the same encryption function, but differ in the number of rounds and the key schedule. More recent versions SAFER+ and

SAFER++ were submitted as candidates to the AES process and the NESSIE project respectively. All of the algorithms in the SAFER family are unpatented and available for unrestricted use.

http://en.wikipedia.org/wiki/SAFER

2.889 SAL

Ver:

- *Nonce*
- http://en.wikipedia.org/wiki/Salt_%28cryptography%29

2.889.1 SAL

dato aleatorio que se combina con una clave para que el resultado de una función criptográfica quede razonablemente disperso y protegido frente a ataques de diccionario.

2.889.2 (EN) SALT

A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an Attacker. [NIST-SP800-63:2013]

2.889.3 (EN) SALT

A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker. [CNSSI_4009:2010]

2.889.4 (EN) SALT

random data item produced by the signing entity during the generation of the message representative in Signature scheme 2. [ISO-9796-2:2002]

2.889.5 (EN) SALT

Random string that is concatenated with other data prior to being operated on by a hash function. See also Hash.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.889.6 (EN) SALT

A salt consists of random bits used as one of the inputs to a key derivation function. Sometimes the IV, a previously generated (preferably random) value, is used as a salt. The other input is usually a password or passphrase. The output of the key derivation function is often stored as the encrypted version of the password. It can also be used as a key for use in a cipher or other cryptographic algorithm. A salt value is typically used in a hash function.

The salt value may or may not be protected as a secret. In either case the additional salt data makes it more difficult to conduct a dictionary attack using pre-encryption of dictionary entries, as each bit of salt used doubles the amount of storage and computation required.

In some protocols, the salt is transmitted in the clear with the encrypted data, sometimes along with the number of iterations used in generating the key (for key strengthening). Cryptographic protocols that use salts include SSL and Ciphersaber.

Early Unix systems used a 12-bit salt, but modern implementations use more.

http://en.wikipedia.org/wiki/Salt_%28cryptography%29

2.889.7 (FR) VARIABLE D'ENTRÉE

Chaîne de données aléatoires qui est concaténée avec des données de source avant qu'une fonction de hachage unilatérale ne soit appliquée. Les variables d'entrée peuvent réduire l'efficacité des attaques de tableaux arc-en-ciel. Voir aussi hachage et tableaux arc-en-ciel.

http://fr.pcisecuritystandards.org/

2.890 SALA PREPARADA

Ver:

- *Hot standby*
- *Sede alternativa*

2.890.1 SALA OPERATIVA

Instalación informática de emergencia preparada para entrar en funcionamiento, caso de que un incidente inutilice los sistemas informáticos de una organización. [Ribagorda:1997]

2.890.2 (EN) HOT SITE

Backup site that includes phone systems with the phone lines already connected. Networks will also be in place, with any necessary routers and switches plugged in and turned on. Desks will have desktop PCs installed and waiting, and server areas will be replete with the necessary hardware to support business-critical functions. Within a few hours, a hot site can become a fully functioning element of an organization. [CNSSI_4009:2010]

2.890.3 (EN) HOT SITE

A fully operational off-site data processing facility equipped with hardware and system software to be used in the event of a disaster. [NIST-SP800-34:2002]

2.891 SALA VACÍA

Ver:

- *Cold standby*
- *Sede alternativa*

2.891.1 SALA VACÍA

Local dotado, únicamente, de instalaciones auxiliares (eléctricas, telefónicas, de climatización, etc.) en el que albergar temporalmente equipos y sistemas informáticos y de comunicación, caso

de que un accidente inutilice los recursos precisos para el tratamiento de la información. [Ribagorda:1997]

2.891.2 (EN) COLD SITE

Backup site that can be up and operational in a relatively short time span, such as a day or two. Provision of services, such as telephone lines and power, is taken care of, and the basic office furniture might be in place, but there is unlikely to be any computer equipment, even though the building might well have a network infrastructure and a room ready to act as a server room. In most cases, cold sites provide the physical location and basic services. [CNSSI_4009:2010]

2.891.3 (EN) COLD SITE

A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site. [NIST-SP800-34:2002]

2.892 SALVAGUARDA

Ver:

- *Control*
- *Contra medida*

2.892.1 MEDIDA DE SEGURIDAD

Medio destinado a mejorar la seguridad, especificado para un requerimiento de seguridad y que es necesario implementar para satisfacerla. Puede tratarse de medidas de previsión o de preparación, de disuasión, protección, detección, aislamiento, de "lucha", de recuperación, restauración, compensación... [EBIOS:2005]

2.892.2 SALVAGUARDA

Procedimiento o mecanismo tecnológico que reduce el riesgo. [Magerit:2012]

2.892.3 SALVAGUARDA

Práctica, procedimiento o mecanismo que trata los riesgos. [UNE-71504:2008]

2.892.4 (EN) SAFEGUARDS

Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures. [CNSSI_4009:2010]

2.892.5 (EN) SECURITY MEASURE

A measure designed to improve security, specified by a security requirement and implemented to comply with it. The effect of the measures may be to anticipate, prepare, dissuade, protect, detect, confine, combat, recover, restore, compensate, etc. [EBIOS:2005]

2.892.6 (EN) SAFEGUARD

Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. [NIST-SP800-53:2013]

2.892.7 (EN) ADMINISTRATIVE SAFEGUARDS

Administrative actions and policies and procedures (1) to manage the selection, development, implementation, and maintenance of security measures, and (2) to protect ePHI and to manage the conduct of the Covered Components' workforce in relation to the protection of ePHI.

http://www.hipaa.yale.edu/overview/glossary.html

2.892.8 (EN) PHYSICAL SAFEGUARDS

are measures, policies, and procedures to physically protect the Covered Components' Systems and related buildings and equipment that contain ePHI, from natural and environmental hazards and unauthorized intrusion.

http://www.hipaa.yale.edu/overview/glossary.html

2.892.9 (EN) TECHNICAL SAFEGUARDS

are the technology, and the policy and procedures for its use that protect electronic protected health information and control access to it.

http://www.hipaa.yale.edu/overview/glossary.html

2.892.10 (FR) MESURE DE SÉCURITÉ

Moyen destiné à améliorer la sécurité, spécifié par une exigence de sécurité et à mettre en œuvre pour la satisfaire. Il peut s'agir de mesures de prévision ou de préparation, de dissuasion, de protection, de détection, de confinement, de "lutte", de récupération, de restauration, de compensation... [EBIOS:2005]

2.892.11 (FR) SAUVEGARDE

Safeguard Les mesures sécurité minimales approuvées et les contrôles qui, quand ils sont correctement employés, permettent de prévenir et de réduire les risques d'exploitation de vulnérabilités spécifiques qui pourraient compromettre un système IT.

MG02: A Guide to Security Risk Management for Information Technology, CSE, 1996.

2.893 SAML

Acrónimos: SAML

2.893.1 SAML

Security Assertion Markup Language, lenguaje de marcas para aserciones de seguridad es un estándar XML que permitirá el intercambio de autorizaciones y autentificaciones entre entidades no relacionadas

2.893.2 (EN) SAML – AUTHENTICATION ASSERTION

An XML-based security specification developed by the Organization for the Advancement of Structured Information Standards (OASIS) for exchanging authentication (and authorization) information between trusted entities over the Internet. [NIST-SP800-63:2013]

2.893.3 (EN) SAML AUTHENTICATION ASSERTION

A SAML assertion that conveys information from a Verifier to an RP about a successful act of authentication that took place between the Verifier and a Subscriber. [NIST-SP800-63:2013]

2.893.4 (EN) SECURITY ASSERTION MARKUP LANGUAGE (SAML)

A protocol consisting of XML-based request and response message formats for exchanging security information, expressed in the form of assertions about subjects, between on-line business partners. [CNSSI_4009:2010]

2.894 SANDBOX

2.894.1 ENTORNO RESTRINGIDO

Mecanismo de protección utilizado en algunos lenguajes o entornos de programación que limita el acceso que tiene un programa a los recursos del sistema. Un recinto restringe un programa a una serie de privilegios y comandos que le dificultan o imposibilitan el causar algún daño a la información del usuario.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.894.2 (EN) SANDBOXING

A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized. [CNSSI_4009:2010]

2.894.3 (EN) SANDBOX

(I) A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized. [RFC4949:2007]

2.894.4 (EN) CONTAINER OR SANDBOX

A sandbox is a logical barrier that constrains the operation of code, data, and/or users within a defined area of a device.

Anything assigned to a sandbox has access to resources within the sandbox, but has controlled or no access to resources outside the sandbox. In this manner, activities within the sandbox are controlled to prohibit unintended interactions with resources outside the sandbox.

Mobile Security Reference Architecture, May 23, 2013

2.895 SAS 70

2.895.1 SAS 70

Informe de auditoría de una institución prestadora de servicios, preparados de acuerdo con las orientaciones impartidas en el Instituto Americano de la declaración certificada de Contador Público de Normas de Auditoría No. 70.

2.895.2 (EN) SAS 70 REPORT

An audit report of a servicing institution prepared in accordance with guidance provided in the American Institute of Certified Public Accountant's Statement of Auditing Standards Number 70.

http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-b-glossary.aspx

2.896 SATAN - SECURITY ADMINISTRATOR TOOL FOR ANALYZING NETWORKS

Acrónimos: SATAN

Ver:

- *Escáner de vulnerabilidades*

2.896.1 SATAN

Herramienta de código libre que permite inspeccionar un sistema remotamente para identificar y explotar vulnerabilidades en el mismo.

2.896.2 (EN) SATAN

A freeware program that remotely probes networks to identify weaknesses in system security.

2.897 SCADA

2.897.1 SCADA

Sistema de control industrial. Se ha convertido en crítico en cuanto puede ser objeto de un ciberataque permitiendo atacar infraestructuras críticas.

2.897.2 (EN) SUPERVISORY CONTROL AND DATA ACQUISITION

Supervisory Control and Data Acquisition (SCADA) refers to the systems and networks that communicate with industrial control systems to provide data to operators for supervisory purposes, as well as control capabilities for process management. [knapp:2014]

2.897.3 (EN) SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEM (SCADA)

Networks or systems generally used for industrial controls or to manage infrastructure such as pipelines and power systems. [CNSSI_4009:2010]

2.897.4 (EN) SCADA SYSTEMS

SCADA stands for "supervisory control and data acquisition" and in the cybersecurity context usually refers to industrial control systems that control infrastructure such as electrical power transmission and distribution, water treatment and distribution, wastewater collection and treatment, oil and gas pipelines and large communication systems. The focus is on whether as these systems are connected to the public Internet they become vulnerable to a remote attack.

http://cyber.law.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas

2.898 SCAM

2.898.1 ESTAFA

Fraude destinado a conseguir que una persona o grupo de personas entreguen dinero, bajo falsas promesas de beneficios económicos (viajes, vacaciones, premios de lotería, etc.).

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.898.2 (EN) SCAMS

Deceptive, uninvited contacts or promises designed to trick people into giving away their money or your personal information. [CSS NZ:2011]

2.898.3 (EN) 419 SCAM

A type of advance fee fraud originating from West Africa, so called because 419 is the section of the Nigerian legal code that covers the crime.

http://www.getsafeonline.org/

2.898.4 (EN) INTERNET FRAUD

Schemes to defraud consumers abound on the Internet. Among the most famous is the Nigerian, or 419, scam; the number is a reference to the section of Nigerian law that the scam violates. Although this con has been used with both fax and traditional mail, it has been given new life by the Internet. In the scheme, an individual receives an e-mail asserting that the sender requires help in transferring a large sum of money out of Nigeria or another distant country. Usually, this money is in the form of an asset that is going to be sold, such as oil, or a large amount of cash that requires laundering to conceal its source; the variations are endless, and new specifics are constantly being

developed. The message asks the recipient to cover some cost of moving the funds out of the country in return for receiving a much larger sum of money in the near future. Should the recipient respond with a check or money order, he is told that complications have developed; more money is required. Over time, victims can lose thousands of dollars that are utterly unrecoverable.

Encyclopedia Britannica.

2.899 SCAREWARE

Ver

- *Scareware*

2.899.1 (EN) SCAREWARE

Software or web site that purports to be security software reporting a threat against a user's computer to convince the user to purchase unneeded software or install malware.

http://cyber.law.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas

2.899.2 (EN) SCAREWARE

Scareware is a type of malware designed to trick victims into purchasing and downloading useless and potentially dangerous software.

http://whatis.techtarget.com/

2.899.3 (EN) ROGUEWARE

A more specific kind of rogueware is scareware, rogue security software, which tries to infect computers by providing fake security alerts.

ENISA Threat Landscape [Deliverable – 2012-09-28]

2.900 SCRIPT KIDDY

Ver:

- http://en.wikipedia.org/wiki/Script_kiddie
- *Cracker*

2.900.1 SCRIPT KIDDY

Cracker aficionado. Se limita a ejecutar procedimientos inventados por otros.

2.900.2 (EN) SCRIPT KIDDY

(D) /slang/ A cracker who is able to use existing attack techniques (i.e., to read scripts) and execute existing attack software, but is unable to invent new exploits or manufacture the tools to perform them; pejoratively, an immature or novice cracker. [RFC4949:2007]

2.900.3 (EN) SCRIPT KIDDIE

Derogatory term for inexperienced crackers who use scripts and programs developed by others, without knowing what they are or how they work, for the purpose of compromising computer accounts and files, and for launching attacks on whole computer systems (see DoS). In general, they do not have the ability to write these kinds of programs on their own.

http://en.wikipedia.org/wiki/Script_kiddie

2.900.4 (EN) SCRIPT KIDDIES

Inexperienced hackers who use publicly available tools.

http://www.getsafeonline.org/

2.901 SECOPS - SECURITY OPERATING PROCEDURES

Acrónimos: SECOPS

Ver:

- *Procedimiento operativo*
- *Procedimientos Operativos de Seguridad (POS)*

2.902 SECRÁFONO

Ver:

- *Cifrado analógico de voz*

2.902.1 SECRÁFONO (SCRAMBLER)

Equipo para realizar el cifrado analógico de la voz. [Ribagorda:1997]

2.902.2 SECRAFONÍA (SCRAMBLING)

Es término sinónimo de: Cifrado analógico de la voz. [Ribagorda:1997]

2.902.3 SECRÁFONO O SCRAMBLER

Equipo de cifra que realiza un cifrado analógico de la voz. (v. Criptófono). [CESID:1997]

2.902.4 (EN) SCRAMBLER

In telecommunications, a scrambler is a device that transposes or inverts signals or otherwise encodes a message at the transmitter to make the message unintelligible at a receiver not equipped with an appropriately set descrambling device. Whereas encryption usually refers to operations carried out in the digital domain, scrambling usually refers to operations carried out in the analog domain. Scrambling is accomplished by the addition of components to the original signal or the changing of some important component of the original signal in order to make extraction of the original signal difficult. Examples of the latter might include removing or changing vertical or horizontal sync pulses in television signals; televisions will not be able to display a picture from

such a signal. Some modern scramblers are actually encryption devices, the name remaining due to the similarities in use, as opposed to internal operation.

http://en.wikipedia.org/wiki/Scrambler

2.902.5 (EN) SCRAMBLER

A device that transposes or inverts signals or otherwise encodes a message at the transmitter to make the message unintelligible at a receiver not equipped with an appropriately set descrambling device. Note: Scramblers usually use a fixed algorithm or mechanism. However, a scrambler provides communications privacy that is inadequate for classified traffic.

http://www.atis.org/tg2k/_scrambler.html

2.903 SECRETO COMPARTIDO

Ver:

- *Negociación de claves*

2.903.1 SECRETO COMPARTIDO

Valor secreto generado como resultado de un protocolo de acuerdo de claves y que se utiliza para entrada para la función de generación de claves.

2.903.2 (EN) SHARED SECRET

A secret value that has been computed using a key agreement scheme and is used as input to a key derivation function. [NIST-SP800-57:2007]

2.903.3 (EN) SHARED SECRET

Refers to the security key for the cryptographic algorithms; it may be derived from a password. [H.530:2002]

2.904 SECRETO DÉBIL

Ver:

- *Clave*

2.904.1 SECRETO DÉBIL

Secreto fácil de adivinar, típicamente por fuerza bruta (búsqueda exhaustiva de opciones posibles).

2.904.2 (EN) WEAK SECRET

Secret that can be conveniently memorized by a human being; typically this means that the entropy of the secret is limited, so that an exhaustive search for the secret may be feasible, given knowledge that would enable a correct guess for the secret to be distinguished from an incorrect guess. [ISO-11770-4:2006]

2.905 SECRETO PERFECTO

Ver:

- *Seguridad computacional*

2.905.1 SECRETO PERFECTO

Propiedad de un cifrado que se cumple si la probabilidad de que un texto cifrado cualquiera sea el resultado de cifrar un cierto texto en claro es igual a la probabilidad de haber elegido para cifrar precisamente dicho texto en claro. Siendo así, un criptoanalista que interceptase el texto cifrado no tendría ninguna pista de cual pudiera ser el texto en claro origen del texto cifrado. Sólo los cifrados de flujo de clave continua (o sea tan larga, al menos, como el texto a cifrar) y aleatoria alcanzan el secreto perfecto.

Esta propiedad conlleva que el cifrador sea incondicionalmente seguro.

[Ribagorda:1997]

2.905.2 SECRETO PERFECTO

Propiedad de un cifrado en el que se cumple que la incertidumbre del texto claro después de conocer el cifrado es la misma que antes de ese conocimiento. [CESID:1997]

2.905.3 (EN) PERFECT SECURITY.

A private key cryptosystem for messages of length n relies on the selection by Alice and Bob of S, a secret. This gives rise to a pair of functions Es and Ds. Of cource we require Ds(Es(m)) = m. The system is said to possess perfect secrecy when for any random variable M which is independent of S, we have that M and Es(M) are independent.

2.905.4 (EN) UNCONDITIONAL SECURITY

A cryptosystem with unconditional security cannot be broken even with infinite computational resources. This is another name for Perfect Security.

2.906 SECUESTRO

Ver:

- *Ataque*

2.906.1 SECUESTRO

Método de ataque a una sesión establecida con el resultado de que el atacante se adueña de la sesión, es decir, se beneficia de la autenticación establecida el inicio de la sesión.

2.906.2 (EN) HIJACK ATTACK

(I) A form of active wiretapping in which the attacker seizes control of a previously established communication association. (See: man-in-the-middle attack, pagejacking, piggyback attack.) [RFC4949:2007]

2.906.3 (EN) HIJACK ATTACK

A form of active wiretapping in which the attacker seizes control of a previously established communication association.

2.907 SECUESTRO DE DNS

Ver:

- *Envenenamiento del DNS*
- *Pharming*
- *Suplantación de DNS*
- *Extensiones de seguridad para el DNS*

2.907.1 SECUESTRO DE DNS

Técnica de ataque contra un dominio de Internet. El atacante silencia al servidor DNS legítimo por medio de algún ataque de denegación de servicio. Una vez silenciado, lo reemplaza, funcionalmente, por un servidor fraudulento bajo dominio del atacante.

2.907.2 (EN) DOMAIN NAME HIJACKING

An attack technique where the attacker takes over a domain by first blocking access to the victim domain's DNS server, then putting up a malicious server in its place. For example, if a hacker wanted to take over fnark.com, he would have to remove the fnark.com DNS server from operation using a Denial of Service attack to block access to fnark's DNS server. Then, he would put up his own DNS server, advertising it to everyone on the Internet as fnark.com. When an unsuspecting user went to access fnark.com, he would get the attacker's domain instead of the real one.

http://www.watchguard.com/glossary/

2.908 SECURE SHELL

2.908.1 SSH

Abreviatura de “secure shell”. Conjunto de protocolos que proporcionancifrado de servicios de red, como inicio de sesión remoto o transferencia remota de archivos.

http://es.pcisecuritystandards.org

2.908.2 SECURE SHELL

SSH (Secure SHell) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo el ordenador mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X arrancado.

Además de la conexión a otras máquinas, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a las máquinas y pasar los datos de cualquier otra aplicación por un canal seguro de SSH.

http://es.wikipedia.org/wiki/SSH

2.908.3 (EN) SSH:

Abbreviation for “Secure Shell.” Protocol suite providing encryption for network services like remote login or remote file transfer.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.908.4 (EN) SECURE SHELL (SSH)

A program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.

2.908.5 (EN) SECURE SHELL

Secure Shell or SSH is a set of standards and an associated network protocol that allows establishing a secure channel between a local and a remote computer. It uses public-key cryptography to authenticate the remote computer and (optionally) to allow the remote computer to authenticate the user. SSH provides confidentiality and integrity of data exchanged between the two computers using encryption and message authentication codes (MACs). SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding arbitrary TCP ports and X11 connections; it can transfer files using the associated SFTP or SCP protocols. An SSH server, by default, listens on the standard TCP port 22.

http://en.wikipedia.org/wiki/SSH

2.908.6 (FR) SSH

Abréviation de «Secure Shell», enveloppe sécurisée. Suite de protocole fournissant un cryptage pour des services de réseau tels que la connexion à distance ou le transfert de fichiers à distance.

http://fr.pcisecuritystandards.org/

2.909 SECURITY_MARKING

2.909.1 (EN) SECURITY MARKING

Human-readable information affixed to information system components, removable media, or output indicating the distribution limitations, handling caveats and applicable security markings. [NIST-SP800-53:2013]

2.909.2 (EN) SECURITY MARKING

Human-readable indicators applied to a document, storage media, or hardware component to designate security classification, categorization and/or handling restrictions applicable to the information contained therein. For intelligence information, these could include compartment and subcompartment indicators and handling restrictions. [CNSSI_4009:2010]

2.910 SEDE ALTERNATIVA

Ver:

- *Sala preparada*
- *Warm site*
- *Sala vacía*

2.910.1 SEDE ALTERNATIVA

Sede para ubicar temporalmente los recursos del Sistema de Información durante una emergencia.

2.910.2 (EN) RECOVERY SITE

An alternate location for processing information (and possibly conducting business) in an emergency. Usually distinguished as “hot” sites that are fully configured centers with compatible computer equipment and “cold” sites that are operational computer centers without the computer equipment.

http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-b-glossary.aspx

2.910.3 (EN) ALTERNATE SITE

Site which may be used for temporary relocation of office or IT facilities during an emergency.

2.911 SEED

Ver:

- *Cifrado en bloque*
- *Criptografía de clave secreta*
- http://www.ietf.org/rfc/rfc4269
- http://www.ietf.org/rfc/rfc4010
- [ISO-18033-3:2005]
- http://en.wikipedia.org/wiki/SEED

2.911.1 SEED

Algoritmo de cifra basado en un secreto compartido (clave). Cifra el texto en bloques de 128 bits. Utiliza claves de 128 bits.

2.911.2 (EN) SEED

SEED is a block cipher developed by the Korean Information Security Agency. It is used broadly throughout South Korean industry, but seldom found elsewhere. It gained popularity in Korea because 40 bit SSL was not considered strong enough (see Transport Layer Security#Early short keys), so the Korean Information Security Agency developed its own standard.

http://en.wikipedia.org/wiki/SEED

2.912 SEGEMENTACIÓN DE LA RED

2.912.1 SEGMENTACIÓN DE RED

La segmentación de red separa componentes del sistema que almacenan, procesan o transmiten datos del titular de la tarjeta de sistemas que no lo hacen. Una segmentación de red adecuada puede reducir el alcance del entorno de los datos del titular de la tarjeta y, por lo tanto, reducir el alcance de la evaluación de las PCI DSS. Consulte la sección Segmentación de red en Requisitos de las DSS PCI y procedimientos de evaluación de seguridad para obtener información acerca del uso de segmentación de red. La segmentación de red no es un requisito de las PCI DSS. Consulte Componentes del sistema.

http://es.pcisecuritystandards.org/

2.912.2 (EN) NETWORK SEGMENTATION:

Network segmentation isolates system components that store, process, or transmit cardholder data from systems that do not. Adequate network segmentation may reduce the scope of the cardholder data environment and thus reduce the scope of the PCI DSS assessment. See the Network Segmentation section in the PCI DSS Requirements and Security Assessment Procedures for guidance on using network segmentation. Network segmentation is not a PCI DSS requirement. See System Components.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.912.3 (FR) SEGMENTATION RÉSEAU

Également nommé «segmentation» ou «isolation». La segmentation de réseau isole les composants du système, qui stockent, traitent ou transmettent les données de titulaires de cartes, de ceux qui ne le font pas. Une segmentation réseau appropriée peut réduire le champ d'application de l'environnement des données de titulaires de cartes, et ainsi celui de l'évaluation PCI DSS. Voir le chapitre Segmentation réseau dans les Conditions et procédures d'évaluation de sécurité de la norme PCI DSS pour plus d'informations sur son utilisation. La segmentation réseau n'est pas une condition de la norme PCI DSS.

http://fr.pcisecuritystandards.org/

2.913 SEGREGACIÓN DE TAREAS

Acrónimos: SoD

2.913.1 SEPARACIÓN DE FUNCIONES

Práctica que consiste en dividir los pasos de una función entre varias personas para evitar que un solo individuo pueda arruinar todo el proceso.

http://es.pcisecuritystandards.org

2.913.2 SEPARACIÓN DE FUNCIONES

1. Proceso que utiliza dos o más entidades separadas (normalmente personas), que operan concertadamente para proteger funciones sensibles o informaciones, de modo que ninguna persona aislada sea capaz de acceder o utilizar un recurso, por ejemplo una clave criptográfica (ISO-8732).

2, Procedimiento de seguridad que exige la concurrencia de dos o más personas para realizar tareas críticas. De este modo, se anula la posibilidad de que un solo individuo autorizado pueda abusar de sus derechos para cometer alguna acción ilícita.

[Ribagorda:1997]

2.913.3 (EN) SEGREGATION/SEPARATION OF DUTIES (SOD)

A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets

Scope Note: Segregation/separation of duties is commonly used in large IT organizations so that no single person is in a position to introduce fraudulent or malicious code without detection.

ISACA, Cybersecurity Glossary, 2014

2.913.4 (EN) SEPARATION OF DUTIES

(I) The practice of dividing the steps in a system process among different individual entities (i.e., different users or different roles) so as to prevent a single entity acting alone from being able to subvert the process. Usage: a.k.a. "separation of privilege". (See: administrative security, dual control.) [RFC4949:2007]

2.913.5 (EN) SEGREGATION OF DUTIES

A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals responsibility for initiating and recording transactions and custody of assets. [COBIT:2006]

2.913.6 (EN) SEPARATION OF DUTIES

Practice of dividing steps in a function among different individuals, so as to keep a single individual from being able to subvert the process.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.913.7 (EN) SEPARATION OF DUTIES

Separation of duties is the principle of splitting privileges among multiple individuals or systems.

http://www.sans.org/security-resources/glossary-of-terms/

2.913.8 (FR) SÉPARATION DES OBLIGATIONS

Pratique consistant à répartir les divers aspects d’une fonction entre divers individus, afin d’éviter qu’une personne seule ne puisse corrompre l’ensemble du processus.

http://fr.pcisecuritystandards.org/

2.914 SEGURIDAD

Ver:

- *Seguridad de la información*
- *Seguridad de las operaciones*
- *Seguridad técnica*
- *Seguridad en las comunicaciones*
- *Compusec*
- *TEMPEST*
- *Seguridad física*
- *Seguridad del personal*
- *Seguridad procedimental*
- *Seguridad operacional*

2.914.1 SEGURIDAD

seguridad

1. f. Cualidad de seguro.

seguro, ra.

1. adj. Libre y exento de todo peligro, daño o riesgo.

DRAE. Diccionario de la Lengua Española.

2.914.2 (EN) SECURITY

A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach. [CNSSI_4009:2010]

2.914.3 (EN) SECURITY

1a. (I) A system condition that results from the establishment and maintenance of measures to protect the system.

1b. (I) A system condition in which system resources are free from unauthorized access and from unauthorized or accidental change, destruction, or loss. (Compare: safety.)

2. (I) Measures taken to protect a system.

Tutorial: Parker [Park] suggests that providing a condition of system security may involve the following six basic functions, which overlap to some extent:

- "Deterrence": Reducing an intelligent threat by discouraging action, such as by fear or doubt. (See: attack, threat action.)
- "Avoidance": Reducing a risk by either reducing the value of the potential loss or reducing the probability that the loss will occur. (See: risk analysis. Compare: "risk avoidance" under "risk".)

- "Prevention": Impeding or thwarting a potential security violation by deploying a countermeasure.
- "Detection": Determining that a security violation is impending, is in progress, or has recently occurred, and thus make it possible to reduce the potential loss. (See: intrusion detection.)
- "Recovery": Restoring a normal state of system operation by compensating for a security violation, possibly by eliminating or repairing its effects. (See: contingency plan, main entry for "recovery".)
- "Correction": Changing a security architecture to eliminate or reduce the risk of reoccurrence of a security violation or threat consequence, such as by eliminating a vulnerability.

[RFC4949:2007]

2.914.4 (EN) SECURITY

All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability.

Note. A product, system, or service is considered to be secure to the extent that its users can rely that it functions (or will function) in the intended way. This is usually considered in the context of an assessment of actual or perceived threats. a) The capability of the software product to protect information and data so that unauthorised persons or systems cannot read or modify them and authorised persons or systems are not denied access to them [ISO/IEC 9126-1].

[ISO-15443-1:2005]

2.914.5 (EN) SECURITY

Security is a system property. Security is much more that a set of functions and mechanisms. Information technology security is a system characteristic as well as a set of mechanisms which span the system both logically and physically. [NIST-SP800-33:2001]

2.914.6 (EN) SECURITY GOAL

The IT security goal is to enable an organization to meet all mission/business objectives by implementing systems with due care consideration of IT-related risks to the organization, its partners, and its customers. [NIST-SP800-33:2001]

2.914.7 (EN) SECURITY

the combination of confidentiality, integrity and availability. [ITSEC:1991]

2.915 SEGURIDAD BASADA EN EL OSCURANTISMO

2.915.1 SEGURIDAD BASADA EN EL OSCURANTISMO

Pretensión de que la seguridad de un sistema se mantiene o se mejora por el hecho de que el mecanismo de seguridad sea secreto.

2.915.2 (EN) SECURITY BY OBSCURITY

(O) Attempting to maintain or increase security of a system by keeping secret the design or construction of a security mechanism. [RFC4949:2007]

2.916 SEGURIDAD COMPUTACIONAL

Ver:

- *Seguridad incondicional*

2.916.1 COMPUTACIONALMENTE SEGURO

Se dice de un criptosistema cuya seguridad dimana del tiempo (o el costo) absolutamente desmesurado necesario para vulnerarlo. Es un concepto relativo al estado de la tecnología en cada época. [Ribagorda:1997]

2.916.2 SISTEMA COMPUTACIONALMENTE SEGURO

Criptosistema en el que, con los medios informáticos actuales, no es viable obtener el texto claro correspondiente a un texto cifrado sin conocer la clave. [CESID:1997]

2.916.3 SISTEMA CONDICIONALMENTE SEGURO

Criptosistema que un agresor, con los medios que dispone actualmente, no puede violar. [CESID:1997]

2.916.4 SISTEMA PROBABLEMENTE SEGURO

Criptosistema en el que no se puede demostrar matemáticamente su integridad, pero que no ha sido violado. [CESID:1997]

2.916.5 (EN) COMPUTATIONAL SECURITY

A cryptosystem has computational security if the best possible algorithm for breaking the system requires at least N operations, N being a suitably large number.

2.917 SEGURIDAD DE LA INFORMACIÓN

Acrónimos: INFOSEC, STIC (es)

Ver:

- *Información*
- *Seguridad*
- *Garantía de la información*

2.917.1 SEGURIDAD DE LA INFORMACIÓN

Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables. [UNE-71504:2008]

2.917.2 SEGURIDAD DE LA INFORMACIÓN

La preservación de la confidencialidad, la integridad y la disponibilidad de la información. Puede, además, abarcar otras propiedades, como la autenticidad, responsabilidad, fiabilidad y prevención del repudio. [UNE-ISO/IEC 27000:2014]

2.917.3 SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN

la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Reglamento (CE) n 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información.

2.917.4 SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (STIC)

Protección de la información almacenada, procesada o transmitida, por Sistemas de las Tecnologías de la Información y las Comunicaciones (Sistemas), mediante la aplicación de las medidas necesarias que aseguren o garanticen la confidencialidad, integridad y disponibilidad de la información y la integridad y disponibilidad de los propios Sistemas.

2.917.1 SEGURIDAD INFORMÁTICA

Disciplina que involucra técnicas, aplicaciones y dispositivos que aseguran la autenticidad, integridad y privacidad de la información contenida dentro de un sistema informático, así como su transmisión.

Técnicamente resulta muy difícil desarrollar un sistema informático que garantice la completa seguridad de la información, sin embargo, el avance de la tecnología ha posibilitado la disposición de mejores medidasde seguridad para evitar daños y problemas que puedan ser aprovechados por los intrusos. Dentro de la seguridad informática se pueden mencionar dos tipos:

- Seguridad lógica: Conjunto de medidas de seguridad y herramientas informáticas de control de acceso a los sistemas informáticos.
- Seguridad física: Controles externos al ordenador, que tratan de protegerlo contra amenazas de naturaleza física como incendios, inundaciones, etc.

http://www.inteco.es/glossary/Formacion/Glosario/

2.917.2 SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN (SSI)

Protección de los sistemas de información, y especialmente de los elementos esenciales, contra cualquier acceso no autorizado, accidental o deliberado, a los criterios de seguridad. [EBIOS:2005]

2.917.3 SEGURIDAD DE LA INFORMACIÓN

Protección de la información que garantiza la confidencialidad, integridad y disponibilidad.

http://es.pcisecuritystandards.org

2.917.4 SEGURIDAD DE LA INFORMACIÓN

1. Combinación de confidencialidad integridad y disponibilidad (ITSEC).

2. Disciplina cuyo objetivo es el estudio de los métodos y medios de protección frente a revelaciones, modificaciones o destrucciones de la información o ante fallos en el proceso, almacenamiento o transmisión de dicha información.

[Ribagorda:1997]

2.917.5 SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN (INFOSEC O SSI)

Conjunto de medidas destinadas a garantizar la confidencialidad, [CESID:1997]

2.917.6 (EN) INFORMATION SECURITY

preservation of confidentiality, integrity and availability of information

NOTE. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

[ISO/IEC 27000:2014]

2.917.1 (EN) INFORMATION SYSTEMS SECURITY (INFOSEC)

Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. See Information Assurance. [CNSSI_4009:2010]

2.917.2 (EN) DATA SECURITY

Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. See also information security. [CNSSI_4009:2010]

2.917.3 (EN) INFORMATION SECURITY (INFOSEC)

(N) Measures that implement and assure security services in information systems, including in computer systems (see: COMPUSEC) and in communication systems (see: COMSEC). [RFC4949:2007]

2.917.4 (EN) DATA SECURITY

(I) The protection of data from disclosure, alteration, destruction, or loss that either is accidental or is intentional but unauthorized. [RFC4949:2007]

2.917.5 (EN) INFORMATION SECURITY.

The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by executive order. [DoD 5220:2006]

2.917.6 (EN) NETWORK AND INFORMATION SECURITY

means the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems.

REGULATION (EC) No 460/2004 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 10 March 2004 establishing the European Network and Information Security Agency.

2.917.7 (EN) INFORMATION SECURITY

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [NIST-SP800-53:2013] [FIPS-200:2006] [FIPS-199:2004]

2.917.8 (EN) INFORMATION SECURITY

The application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems against loss of confidentiality, integrity or availability, whether accidental or intentional, and to prevent loss of integrity or availability of the systems themselves.

Notes.

- INFOSEC measures include those of computer, transmission, emission and cryptographic security.
- Such measures also include detection, documentation and countering of threats to information and to the systems.

[CCN-STIC-401:2007]

2.917.9 (EN) INFORMATION SECURITY

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

U.S. Code 44, Sec. 3542. Definitions, 2007

2.917.1 (EN) INFORMATION SYSTEMS SECURITY (ISS)

Protection of information systems and especially essential elements, against any unauthorised violation of the security criteria, whether accidental or deliberate. [EBIOS:2005]

2.917.2 (EN) INFORMATION SECURITY

Protection of information to insure confidentiality, integrity, and availability.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.917.3 (EN) INFORMATION SECURITY

Information security is the theory and practice of setting up and using computer and communication systems to protect the integrity of information, prevent the loss of information during processing, and ensuring that those who need information have access to it whilst at the same time others who have no right of access should not.

http://www.itrainonline.org/itrainonline/mmtk/

2.917.4 (FR) SÉCURITÉ DES INFORMATIONS

Protection des informations pour garantir la confidentialité, l'intégrité et la disponibilité.

http://fr.pcisecuritystandards.org/

2.917.5 (FR) SÉCURITÉ DE L'INFORMATION

Satisfaction des besoins de sécurité des biens essentiels. [EBIOS:2010]

2.917.1 (FR) SECURITE DES SYSTEMES D'INFORMATION (SSI)

Protection des systèmes d'information, et en particulier des éléments essentiels, contre toute atteinte des critères de sécurité non autorisée, qu'elle soit accidentelle ou délibérée. [EBIOS:2005]

2.918 SEGURIDAD DE LAS EMANACIONES

Acrónimos: EMSEC

Ver:

- *Emanaciones*
- *TEMPEST*
- Protección de las emanaciones (EMSEC)

2.918.1 SEGURIDAD DE LAS EMANACIONES O SEGURIDAD TEMPEST

Conjunto de medidas destinadas a evitar fugas de información derivadas de emisiones electromagnéticas no deseadas de equipos electrónicos. [CCN-STIC-150:2006]

2.918.2 SEGURIDAD DE LAS EMANACIONES O SEGURIDAD TEMPEST

Medidas de seguridad destinadas a evitar compromisos por emisiones electromagnéticas no deseadas de equipos electrónicos. [CESID:1997]

2.918.3 (EN) EMANATIONS SECURITY (EMSEC)

Protection resulting from measures taken to deny unauthorized individuals information derived from intercept and analysis of compromising emissions from crypto-equipment or an information system. See TEMPEST. [CNSSI_4009:2010]

2.918.4 (EN) EMANATIONS SECURITY (EMSEC)

(I) Physical security measures to protect against data compromise that could occur because of emanations that might be received and read by an unauthorized party. (See: emanation, TEMPEST.) [RFC4949:2007]

2.918.5 (EN) EMISSION SECURITY

The protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from intercept and from an analysis of compromising emanations from systems. [IRM-5239-8:1995]

2.919 SEGURIDAD DE LAS OPERACIONES

Acrónimos: OPSEC

Ver:

- *Seguridad*

2.919.1 SEGURIDAD DE LAS OPERACIONES

Procesos orientados a identificar, controlar y proteger la información relativa a operaciones propias frente a los intentos del atacante orientados a descubrir nuestros planes con anticipación.

2.919.1 (EN) OPERATIONS SECURITY (OPSEC)

Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures. [CNSSI_4009:2010]

2.919.2 (EN) OPERATIONS SECURITY (OPSEC)

(I) A process to identify, control, and protect evidence of the planning and execution of sensitive activities and operations, and thereby prevent potential adversaries from gaining knowledge of capabilities and intentions. (See: communications cover. Compare: operational security.) [RFC4949:2007]

2.920 SEGURIDAD DE LAS PERSONAS

Ver:

- *Seguridad del personal*

2.920.1 SEGURIDAD DE LAS PERSONAS

Mantener a las personas libres de daños físicos.

2.920.2 (EN) SAFETY

(I) The property of a system being free from risk of causing harm (especially physical harm) to its system entities. (Compare: security.) [RFC4949:2007]

2.920.3 (EN) SAFETY

Safety is the need to ensure that the people involved with the company, including employees, customers, and visitors, are protected from harm.

http://www.sans.org/security-resources/glossary-of-terms/

2.921 SEGURIDAD DEL PERSONAL

Ver:

- *Seguridad*
- *Seguridad de las personas*

2.921.1 SEGURIDAD DEL PERSONAL

Procedimientos para asegurar que los que acceden a un sistema disfrutan de la habilitación necesaria y tienen necesidad de conocer, siempre de acuerdo a la política de seguridad correspondiente.

2.921.2 (EN) PERSONNEL SECURITY

(I) Procedures to ensure that persons who access a system have proper clearance, authorization, and need-to-know as required by the system's security policy. (See: security architecture.) [RFC4949:2007]

2.921.3 (EN) PERSONNEL SECURITY

The procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances. [IRM-5239-8:1995]

2.922 SEGURIDAD DISCRECIONAL

Ver:

- *TCSEC - Trusted Computer System Evaluation Criteria*

2.922.1 SEGURIDAD DISCRECIONAL

Aquellos aspectos de la política de seguridad que conllevan la prestación de servicios de seguridad a consecuencia de una petición por entidad solicitante de comunicaciones. (ISO-7498-2). [Ribagorda:1997]

2.922.2 (EN) DISCRETIONARY SECURITY PROTECTION

The C1 system class. It consists of rather limited security features. The Orange Book describes C1 systems as an environment of "cooperating users processing data at the same level(s) of security." Security features are primarily intended to prevent users from making honest mistakes that could

damage the system (eg. by writing over system memory or critical software) or from interfering with other users' work (by deleting or modifying their programs or data). The security features are insufficient to keep a determined intruder out. The system architecture must be capable of protecting system code from user programs. It must be tested to ensure proper operation and that security features can't be bypassed in any obvious way. There are also specific documentation requirements.

Two main user-visible features required in this class are passwords and discretionary protection of files and other objects.

[TCSEC:1985]

2.923 SEGURIDAD EN LAS COMUNICACIONES

Acrónimos: COMSEC

Ver:

- *TRANSEC - Seguridad de las transmisiones*
- *Seguridad*

2.923.1 SEGURIDAD EN LAS COMUNICACIONES

Medidas y controles para denegar el acceso a través de las redes a entidades no autorizadas, así como para garantizar la autenticidad de las partes en comunicación. La seguridad de las comunicaciones incluye criptografía, transmisiones, emisiones y seguridad física.

2.923.2 SEGURIDAD DE LAS COMUNICACIONES (COMSEC)

Resultado de un conjunto de medidas de seguridad aplicadas a las telecomunicaciones y orientadas a impedir que entidades no autorizadas puedan tener acceso o estudiar la información transmitida y a garantizar su autenticación. (v. Seguridad criptológica, Seguridad de las transmisiones, Seguridad de las emanaciones, Seguridad física y del personal). [CESID:1997]

2.923.3 SEGURIDAD CRIPTOLÓGICA

Componente de la seguridad de las comunicaciones que resulta de utilizar un criptosistema adecuado para los requerimientos de protección de la información y de su correcto empleo. [CESID:1997]

2.923.1 (EN) COMMUNICATIONS SECURITY (COMSEC)

A component of Information Assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emissions security, and physical security of COMSEC materia. [CNSSI_4009:2010]

2.923.2 (EN) COMMUNICATION SECURITY (COMSEC)

(I) Measures that implement and assure security services in a communication system, particularly those that provide data confidentiality and data integrity and that authenticate communicating entities. [RFC4949:2007]

2.923.3 (EN) COMMUNICATIONS SECURITY (COMSEC).

Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government relating to national security and to ensure the authenticity of such communications. [DoD 5220;2006]

2.923.4 (EN) COMMUNICATIONS SECURITY (COMSEC)

The application of cryptographic security, transmission and emission security, physical security measures, operational practices and controls to deny unauthorized access to information derived from telecommunications and that ensure the authenticity of such telecommunications.

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

2.924 SEGURIDAD EXTREMO A EXTREMO

Ver:

- *Seguridad*

2.924.1 SEGURIDAD EXTREMO A EXTREMO

Cuando la información está asegurada entre extremos: desde el origen hasta el destino.

2.924.2 (EN) END-TO-END SECURITY

Safeguarding information in an information system from point of origin to point of destination. [CNSSI_4009:2010]

2.925 SEGURIDAD FÍSICA

Ver:

- *Seguridad*

2.925.1 SEGURIDAD FÍSICA

1. Conjunto de medidas usadas para proporcionar protección física a los recursos de información contra amenazas intencionadas o accidentales (ISO-7498-2).

2. Conjunto de controles externos al ordenador, que tratan de proteger a éste y su entorno de amenazas de naturaleza física como incendios, inundaciones, atentados, etc.

Normalmente, se materializan mediante dispositivos eléctricos, electrónicos, etc.

[Ribagorda:1997]

2.925.2 SEGURIDAD FÍSICA Y DEL PERSONAL

Conjunto de medidas que protegen la documentación y equipos ante pérdidas, robos o accesos por personal no autorizado, incluyendo además la formación y habilitación de las personas que deban acceder a materias clasificadas. [CESID:1997

2.925.3 SEGURIDAD FÍSICA

Medidas adoptadas para proporcionar la protección física de los recursos contra amenazas deliberadas o accidentales. [ISO-7498-2:1989]

2.925.4 (EN) PHYSICAL SECURITY

(I) Tangible means of preventing unauthorized physical access to a system. Examples: Fences, walls, and other barriers; locks, safes, and vaults; dogs and armed guards; sensors and alarm bells. [FP031, R1455] (See: security architecture.) [RFC4949:2007]

2.925.5 (EN) PHYSICAL SECURITY

The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information. [IRM-5239-8:1995]

2.925.6 (EN) PHYSICAL SECURITY

The measures used to provide physical protection of resources against deliberate and accidental threats. [ISO-7498-2:1989]

2.925.7 (FR) SÉCURITÉ PHYSIQUE

Mesures prises pour assurer la protection des ressources contre des menaces délibérées ou accidentelles. [ISO-7498-2:1989]

2.926 SEGURIDAD GESTIONADA

2.926.1 SEGURIDAD GESTIONADA

Se dice cuando la gestión de la seguridad se encarga a una empresa externa. Es típico externalizar los sistemas de detección de intrusión, respuesta ante incidentes, protección perimetral, comunicaciones alternativas, etc.

2.926.2 (EN) MANAGED SECURITY SERVICES PROVIDER (MSSP)

A Managed Security Services Provider is a company that handles network security services (such as intrusion detection and prevention, spam blocking and firewall capabilities) for its clients. MSSPs are outsourcing providers.

http://www.csoonline.com/glossary/

2.926.3 (EN) MANAGED SECURITY SERVICE PROVIDER (MSSP)

An **managed security service provider (MSSP)** provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services. MSSPs use high-availability security operation centers (either from their own facilities or from other data center providers) to provide 24/7 services designed to reduce the number of operational security personnel an enterprise needs to hire, train and retain to maintain an acceptable security posture.

http://www.gartner.com/it-glossary/

2.927 SEGURIDAD INCONDICIONAL

Ver:

- *Seguridad computacional*
- *Holocríptico*

2.927.1 INCONDICIONALMENTE SEGURO

Se dice de un cifrado que es seguro con independencia del tiempo o los recursos ilimitados que puedan invertirse para tratar de vulnerarlo.

Tal cifrado alcanza el secreto perfecto.

[Ribagorda:1997]

2.927.2 SISTEMA INCONDICIONALMENTE SEGURO U HOLOCRÍPTICO

Criptosistema en el que matemáticamente se puede demostrar que sin el conocimiento de la clave no se puede obtener el texto claro correspondiente a un texto cifrado. [CESID:1997]

2.927.3 (EN) INFORMATION-THEORETIC SECURITY

"Unbreakable" security, in which no amount of cryptanalysis can break a cipher or system. One time pads are an example (providing the pads are not lost nor stolen nor used more than once, of course).

Same as unconditionally secure.

http://www.totse.com/en/privacy/encryption/crypglos.html

2.928 SEGURIDAD OPERACIONAL

Ver:

- *Seguridad*

2.928.1 SEGURIDAD OPERACIONAL

Garantías de poder mantener bajo control la gestión de un sistema y sus características de seguridad.

2.928.2 (EN) OPERATIONAL SECURITY

1. (I) System capabilities, or performance of system functions, that are needed either (a) to securely manage a system or (b) to manage security features of a system. (Compare: operations security (OPSEC).) [RFC4949:2007]

2.929 SEGURIDAD PROCEDIMENTAL

Ver:

- *Seguridad*

2.929.1 SEGURIDAD ADMINISTRATIVA Y ORGANIZATIVA (MANAGEMENT SECURITY)

Aspecto de la seguridad relacionado con la gestión de la misma. Se manifiesta en la formulación de políticas y procedimientos de seguridad.

Más concretamente, se establece mediante: la asignación d responsabilidades, el establecimiento de una política de clasificación de la información, de una política de personal (selección y formación en temas de seguridad informática, cláusulas de penalización en contratos por abuso o negligencia, etc.), de procedimientos de registro de incidente, de auditoría, etc. También comprende la gestión de riesgos y los planes de contingencia.

[Ribagorda:1997]

2.929.2 (EN) PROCEDURAL SECURITY

The management constraints and supplemental controls established to provide an acceptable level of protection for data. [IRM-5239-8:1995]

2.930 SEGURIDAD TÉCNICA

Ver:

- *Seguridad*

2.930.1 SEGURIDAD TÉCNICA

Conjunto de técnicas y controles de seguridad que se implementan en el interior de los propios equipos y sistemas de tecnologías de la información, sea en el hardware o sea en el software, para proteger, principalmente, los programas y los datos que procesan, almacenan y transmiten, aunque en ocasiones también prevengan de las amenazas sobre el propio hardware.

Por prevenir de los ataques al hardware y al software es preferible al término seguridad técnica al de seguridad lógica, que algunos emplean.

[Ribagorda:1997]

2.930.2 (EN) TECHNICAL SECURITY

(I) Security mechanisms and procedures that are implemented in and executed by computer hardware, firmware, or software to provide automated protection for a system. (See: security architecture. Compare: administrative security.) [RFC4949:2007]

2.930.3 (EN) TECHNICAL SECURITY

The discovery, elimination, and mitigation of security vulnerabilities that can be exploited by technical means. It includes all facets of security that involve the detection and/or neutralization of technical collection threats or the application of security technology; the traditional fields of TEMPEST and technical surveillance countermeasures (TSCM); and extends to new techniques,

technology, and instrumentation that may allow exploitation of security vulnerabilities by technical means. [NSA/CSS REG 90-6]

2.930.4 (EN) TECHNICAL SECURITY EVALUATION (TSE)

An evaluation of all factors related to potential vulnerabilities of technical penetration of a facility, system, network, product, or equipment. Typical considerations include security against acoustical, optical, audio frequency, radio frequency, and other methods of penetration as well as adequacy of electronic protection. A TSE includes TSCM, TEMPEST, and TEAPOT considerations. [NSA/CSS REG 90-6]

2.931 SELLO

2.931.1 SELLO

Valor de comprobación criptográfico que sustenta la integridad pero que no protege contra falsificaciones hechas por el destinatario (es decir, no proporciona servicios de no repudio). Cuando un sello está asociado con un elemento de datos, se dice que el elemento de datos está sellado.

NOTA. Aunque un sello por sí mismo no proporciona el no repudio, algunos mecanismos de no repudio utilizan el servicio de integridad proporcionado por los sellos, por ejemplo, para proteger las comunicaciones con terceras partes confiables.

[X.810:1995]

2.931.2 (EN) SEAL

A cryptographic check-value that supports integrity but does not protect against forgery by the recipient (i.e. it does not provide non-repudiation). When a seal is associated with a data element, that data element is said to be sealed.

NOTE. Although a seal does not by itself provide non-repudiation, some non-repudiation mechanisms make use of the integrity service provided by seals, e.g. to protect communications with trusted third parties.

[X.810:1995]

2.931.3 (FR) SCELLÉ

valeur de contrôle cryptographique qui met en oeuvre l'intégrité mais qui ne protège pas d'une falsification du récepteur (c'est-à-dire qu'il n'offre pas la non-répudiation). Lorsqu'un scellé est associé à un élément de données, cet élément de données est dit scellé.

NOTE. Bien qu'un scellé n'offre pas lui-même la non-répudiation, certains mécanismes de non-répudiation font usage du service d'intégrité offert par les scellés, par exemple, pour protéger les communications avec des tierces parties de confiance.

[X.810:1995]

2.932 SELLO ELECTRÓNICO

2.932.1 SELLO ELECTRÓNICO

«sello electrónico», datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos; [PE-CONS 60/14]

2.932.2 SELLO ELECTRÓNICO AVANZADO

«sello electrónico avanzado», un sello electrónico que cumple los requisitos contemplados en el artículo 36; [PE-CONS 60/14]

2.932.3 SELLO ELECTRÓNICO CUALIFICADO

«sello electrónico cualificado», un sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico; [PE-CONS 60/14]

2.932.4 DATOS DE CREACIÓN DEL SELLO ELECTRÓNICO

«datos de creación del sello electrónico», los datos únicos que utiliza el creador del sello electrónico para crearlo; [PE-CONS 60/14]

2.932.5 CERTIFICADO DE SELLO ELECTRÓNICO

«certificado de sello electrónico», una declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de esa persona; [PE-CONS 60/14]

2.932.6 CERTIFICADO CUALIFICADO DE SELLO ELECTRÓNICO

«certificado cualificado de sello electrónico», un certificado de sellos electrónicos que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo III; [PE-CONS 60/14]

2.932.7 DISPOSITIVO DE CREACIÓN DE SELLO ELECTRÓNICO

«dispositivo de creación de sello electrónico», un equipo o programa informático configurado que se utiliza para crear un sello electrónico; [PE-CONS 60/14]

2.932.8 DISPOSITIVO CUALIFICADO DE CREACIÓN DE SELLO ELECTRÓNICO

«dispositivo cualificado de creación de sello electrónico», un dispositivo de creación de sellos electrónicos que cumple mutatis mutandis los requisitos enumerados en el anexo II; [PE-CONS 60/14]

2.932.9 ¿QUÉ ES UN CERTIFICADO DE SELLO DE EMPRESA?

Un certificado de sello de empresa es un certificado técnico que puede ser utilizado por un aplicativo de forma desasistida, también por un grupo de personas pertenecientes a un departamento o

grupo de trabajo. Es un certificado que puede compararse en el mundo físico al uso habitual en el día a día de una empresa de un sello de caucho.

Es adecuado para la firma de comprobantes de recepción electrónicos, firma de newsletters o comunicaciones de empresa, firma de logs y backups ..etc.

http://www.camerfirma.com/ayuda/faq/sello-de-empresa/

2.932.10 (EN) ELECTRONIC SEAL

'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity; [PE-CONS 60/14]

2.932.11 (EN) ADVANCED ELECTRONIC SEAL

'advanced electronic seal' means an electronic seal, which meets the requirements set out in Article 36; [PE-CONS 60/14]

2.932.12 (EN) QUALIFIED ELECTRONIC SEAL

'qualified electronic seal' means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal; [PE-CONS 60/14]

2.932.13 (EN) ELECTRONIC SEAL CREATION DATA

'electronic seal creation data' means unique data, which is used by the creator of the electronic seal to create an electronic seal; [PE-CONS 60/14]

2.932.14 (EN) CERTIFICATE FOR ELECTRONIC SEAL

'certificate for electronic seal' means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person; [PE-CONS 60/14]

2.932.15 (EN) 'QUALIFIED CERTIFICATE FOR ELECTRONIC SEAL

'qualified certificate for electronic seal' means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III; [PE-CONS 60/14]

2.932.16 (EN) ELECTRONIC SEAL CREATION DEVICE

'electronic seal creation device' means configured software or hardware used to create an electronic seal; [PE-CONS 60/14]

2.932.17 (EN) QUALIFIED ELECTRONIC SEAL CREATION DEVICE

'qualified electronic seal creation device' means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II; [PE-CONS 60/14]

2.932.18 (FR) CACHET ÉLECTRONIQUE

"cachet électronique", des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières;

2.932.19 (FR) CACHET ÉLECTRONIQUE AVANCÉ

"cachet électronique avancé", un cachet électronique qui satisfait aux exigences énoncées à l'article 36; [PE-CONS 60/14]

2.932.20 (FR) CACHET ÉLECTRONIQUE QUALIFIÉ

"cachet électronique qualifié", un cachet électronique avancé qui est créé à l'aide d'un dispositif de création de cachet électronique qualifié et qui repose sur un certificat qualifié de cachet électronique; [PE-CONS 60/14]

2.932.21 (FR) DONNEES DE CREATION DE CACHET ELECTRONIQUE

"données de création de cachet électronique", des données uniques qui sont utilisées par le créateur du cachet électronique pour créer un cachet électronique; [PE-CONS 60/14]

2.932.22 (FR) CERTIFICAT DE CACHET ÉLECTRONIQUE

"certificat de cachet électronique", une attestation électronique qui associe les données de validation d'un cachet électronique à une personne morale et confirme le nom de cette personne; [PE-CONS 60/14]

2.932.23 (FR) CERTIFICAT QUALIFIE DE CACHET ELECTRONIQUE

"certificat qualifié de cachet électronique", un certificat de cachet électronique, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'annexe III; [PE-CONS 60/14]

2.932.24 (FR) DISPOSITIF DE CREATION DE CACHET ELECTRONIQUE

"dispositif de création de cachet électronique", un dispositif logiciel ou matériel configuré utilisé pour créer un cachet électronique; [PE-CONS 60/14]

2.932.25 (FR) DISPOSITIF DE CREATION DE CACHET ELECTRONIQUE QUALIFIE

"dispositif de création de cachet électronique qualifié", un dispositif de création de cachet électronique qui satisfait mutatis mutandis aux exigences fixées à l'annexe II; [PE-CONS 60/14]

2.933 SELLO DE TIEMPO

Ver:

- *Servicio de fechado electrónico*
- *Solicitante del sello de tiempo*

- *Verificador del sello de tiempo*
- *Autoridad de sellado de tiempo*
- *Política de sellos de tiempo*
- http://www.ietf.org/rfc/rfc3161

2.933.1 FECHAR

Poner fecha a un escrito.

DRAE. Diccionario de la Lengua Española.

2.933.2 SELLO DE TIEMPO ELECTRÓNICO

«sello de tiempo electrónico», datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante; [PE-CONS 60/14]

2.933.3 SELLO CUALIFICADO DE TIEMPO ELECTRÓNICO

«sello cualificado de tiempo electrónico», un sello de tiempo electrónico que cumple los requisitos establecidos en el artículo 42; [PE-CONS 60/14]

2.933.4 SELLO DE TIEMPO

estructura de datos que proporciona un enlace verificable criptográficamente entre la representación de unos datos y un instante de tiempo.

NOTA. Un sello de tiempo puede incluir más información en el enlace.

[traducción de ISO/IEC 18014-1]

2.933.5 ESTAMPILLA DE TIEMPO

1. Campo de datos usado por una entidad para verificar que un mensaje no es una repetición de otro anterior (ISO/IEC ISO-9798-1).

2. Valor insertado en un mensaje para indicar la jora y día en que fue creado. Usualmente este valor se firma digitalmente, par evitar alteraciones que inutilizarían su propósito de evitar ulteriores repeticiones de los mensajes.

[Ribagorda:1997]

2.933.6 MARCA HORARIA

Registro de la creación o existencia de una información con el fin de evitar su posterior repetición. [CESID:1997]

2.933.7 (EN) ELECTRONIC TIME STAMP

'electronic time stamp' means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time; [PE-CONS 60/14]

2.933.8 (EN) QUALIFIED ELECTRONIC TIME STAMP

'qualified electronic time stamp' means an electronic time stamp which meets the requirements laid down in Article 42; [PE-CONS 60/14]

2.933.9 (EN) TRUSTED TIMESTAMP

A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time. [CNSSI_4009:2010]

2.933.10 (EN) TIME STAMP

A data item which denotes a point in time with respect to a common time reference. [ISO-11770-3:2008]

2.933.11 (EN) TIME STAMP

1. (I) /noun/ With respect to a data object, a label or marking in which is recorded the time (time of day or other instant of elapsed time) at which the label or marking was affixed to the data object. (See: Time-Stamp Protocol.)

2. (O) /noun/ "With respect to a recorded network event, a data field in which is recorded the time (time of day or other instant of elapsed time) at which the event took place." [A1523]

[RFC4949:2007]

2.933.12 (EN) TIME-STAMP PROTOCOL

(I) An Internet protocol (RFC 3161) that specifies how a client requests and receives a time stamp from a server for a data object held by the client. [RFC4949:2007]

2.933.13 (EN) TRUSTED TIME-STAMP

A time-stamp assured by a time-stamping authority. [ISO-13888-1:2004]

2.933.14 (EN) TIME-STAMP RENEWAL

Renewal issues a new time-stamp to extend the validity period of an earlier time-stamp. [ISO-18014-2:2002]

2.933.15 (EN) TIME-STAMP TOKEN

data structure containing a verifiable cryptographic binding between a data items representation and a timevalue.

NOTE. A time-stamp token may also include additional data items in the binding.

[ISO-18014-1:2002]

2.933.16 (EN) TIME-STAMP

A time value used to indicate when a particular activity, action or an occurrence of an event took place. [X.790:1995]

2.933.17 (FR) HORODATAGE ÉLECTRONIQUE

"horodatage électronique", des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant; [PE-CONS 60/14]

2.933.18 (FR) HORODATAGE ÉLECTRONIQUE QUALIFIÉ

"horodatage électronique qualifié", un horodatage électronique qui satisfait aux exigences fixées à l'article 42; [PE-CONS 60/14]

2.934 SEMIFORMAL

Ver:

- *Informal*
- *Formal*
- *Criterios comunes*

2.934.1 SEMIFORMAL

expresado con un lenguaje restringido con una semántica definida; pero sin llegar a un formalismo matemático que permita demostraciones.

2.934.2 (EN) SEMIFORMAL

expressed in a restricted syntax language with defined semantics. [CC:2006]

2.935 SEMILLA (1)

Ver:

- *Generador de números seudo-aleatorio*

2.935.1 SEMILLA

Conjunto de símbolos que aplicado a un generador de números aleatorios permite el arranque del mismo. [Ribagorda:1997]

2.935.2 SEMILLA O CLAVE GENERADORA DE CLAVES

Clave que, aplicada a un generador de claves, genera electrónicamente otras claves. [CESID:1997]

2.935.3 (EN) SEED KEY

a secret value used to initialise a cryptographic function or operation. [ISO-19790:2006]

2.935.4 (EN) SEED

string of bits that is used as input to a deterministic random bit generator (DRBG). The seed will determine a portion of the state of the DRBG. [ISO-18031:2005]

2.936 SENSIBILIDAD

Ver:

- *Información sensible*
- *Etiqueta de sensibilidad*

2.936.1 SENSIBILIDAD

Característica de un recurso que presupone su valor o importancia. [X.509:2005]

2.936.2 SENSIBILIDAD

1. Característica de un recurso que expresa su valor o importancia y, quizás, su vulnerabilidad a amenazas accidentales o deliberadas (ISO-7498-2).

2. Medida del daño que podría suponer la pérdida de información, su revelación, modificación, o destrucción no autorizada.

[Ribagorda:1997]

2.936.3 SENSIBILIDAD

Característica de un recurso relativa a su valor o importancia y eventualmente a su vulnerabilidad. [ISO-7498-2:1989]

2.936.4 (EN) SENSITIVITY

A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection. [CNSSI_4009:2010]

2.936.5 (EN) SENSITIVITY

Characteristic of a resource that implies its value or importance. [X.509:2005]

2.936.6 (EN) SENSITIVITY

The characteristic of a resource which implies its value or importance, and may include its vulnerability. [ISO-7498-2:1989]

2.936.7 (FR) SENSIBILITÉ

caractéristique d'une ressource liée à sa valeur ou à son importance. [X.509:2005]

2.936.8 (FR) SENSIBILITÉ

Caractéristique d'une ressource relative à sa valeur ou à son importance et, éventuellement, à sa vulnérabilité. [ISO-7498-2:1989]

2.937 SERPENT

Ver:

- *Cifrado en bloque*
- *Criptografía de clave secreta*
- *AES - Advanced Encryption Standard*
- http://en.wikipedia.org/wiki/Serpent_%28cipher%29

2.937.1 SERPENT

Algoritmo de cifra basado en un secreto compartido (clave). Cifra el texto en bloques de 128 bits. Utiliza claves de 128, 192 o 256 bits.

2.937.2 (EN) SERPENT

(O) A symmetric, 128-bit block cipher designed by Ross Anderson, Eli Biham, and Lars Knudsen as a candidate for the AES. [RFC4949:2007]

2.938 SERVICIO DE AUTENTICACIÓN

Ver:

- *Autenticación*

2.938.1 SERVICIO DE AUTENTICACIÓN

Servicio de seguridad que verifica la identidad alegada por una entidad.

2.938.2 (EN) AUTHENTICATION SERVICE

(I) A security service that verifies an identity claimed by or for an entity. (See: authentication.)

Tutorial: In a network, there are two general forms of authentication service: data origin authentication service and peer entity authentication service.

[RFC4949:2007]

2.939 SERVICIO DE CONFIANZA

2.939.1 SERVICIO DE CONFIANZA

«servicio de confianza», el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en:

a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o

b) la creación, verificación y validación de certificados para la autenticación de sitios web, o

c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios;

[PE-CONS 60/14]

2.939.2 SERVICIO DE CONFIANZA CUALIFICADO

«servicio de confianza cualificado», un servicio de confianza que cumple los requisitos aplicables establecidos en el presente Reglamento; [PE-CONS 60/14]

2.939.3 PRESTADOR DE SERVICIOS DE CONFIANZA

«prestador de servicios de confianza», una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianzas; [PE-CONS 60/14]

2.939.4 PRESTADOR CUALIFICADO DE SERVICIOS DE CONFIANZA

«prestador cualificado de servicios de confianza», un prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la cualificación; [PE-CONS 60/14]

2.939.5 (EN) TRUST SERVICE

'trust service' means an electronic service normally provided for remuneration which consists of:

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

(b) the creation, verification and validation of certificates for website authentication, or

(c) the preservation of electronic signatures, seals or certificates related to those services;

[PE-CONS 60/14]

2.939.6 (EN) QUALIFIED TRUST SERVICE

'qualified trust service' means a trust service that meets the applicable requirements laid down in this Regulation; [PE-CONS 60/14]

2.939.7 (EN) TRUST SERVICE PROVIDER

'trust service provider' means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider; [PE-CONS 60/14]

2.939.8 (EN) QUALIFIED TRUST SERVICE PROVIDER

'qualified trust service provider' means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body; [PE-CONS 60/14]

2.939.9 (FR) SERVICE DE CONFIANCE

"service de confiance", un service électronique normalement fourni contre rémunération qui consiste en:

a) la création, la vérification et la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envois recommandés électroniques et de certificats relatifs à ces services; ou

b) la création, la vérification et la validation de certificats pour l'authentification de sites internet; ou

c) la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services;

[PE-CONS 60/14]

2.939.10 (FR) SERVICE DE CONFIANCE QUALIFIÉ

"service de confiance qualifié", un service de confiance qui satisfait aux exigences du présent règlement; [PE-CONS 60/14]

2.939.11 (FR) PRESTATAIRE DE SERVICES DE CONFIANCE

"prestataire de services de confiance", une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié; [PE-CONS 60/14]

2.939.12 (FR) PRESTATAIRE DE SERVICES DE CONFIANCE QUALIFIE

"prestataire de services de confiance qualifié", un prestataire de services de confiance qui fournit un ou plusieurs services de confiance qualifiés et a obtenu de l'organe de contrôle le statut qualifié; [PE-CONS 60/14]

2.940 SERVICIO DE ENTREGA ELECTRÓNICA CERTIFICADA

2.940.1 SERVICIO DE ENTREGA ELECTRÓNICA CERTIFICADA

«servicio de entrega electrónica certificada», un servicio que permite transmitir datos entre partes terceras por medios electrónicos y aporta pruebas relacionadas con la gestión de los datos transmitidos, incluida la prueba del envío y la recepción de los datos, y que protege los datos transmitidos frente a los riesgos de pérdida, robo, deterioro o alteración no autorizada; [PE-CONS 60/14]

2.940.2 SERVICIO CUALIFICADO DE ENTREGA ELECTRÓNICA CERTIFICADA

«servicio cualificado de entrega electrónica certificada», un servicio de entrega electrónica certificada que cumple los requisitos establecidos en el artículo 44; [PE-CONS 60/14]

2.940.3 (EN) ELECTRONIC REGISTERED DELIVERY SERVICE

'electronic registered delivery service' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations; [PE-CONS 60/14]

2.940.4 (EN) QUALIFIED ELECTRONIC REGISTERED DELIVERY SERVICE

'qualified electronic registered delivery service' means an electronic registered delivery service which meets the requirements laid down in Article 44; [PE-CONS 60/14]

2.940.5 (FR) SERVICE D'ENVOI RECOMMANDÉ ÉLECTRONIQUE

"service d'envoi recommandé électronique", un service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée; [PE-CONS 60/14]

2.940.6 (FR) SERVICE D'ENVOI RECOMMANDE ELECTRONIQUE QUALIFIE

"service d'envoi recommandé électronique qualifié", un service d'envoi recommandé électronique qui satisfait aux exigences fixées à l'article 44; [PE-CONS 60/14]

2.941 SERVICIO DE FECHADO ELECTRÓNICO

Acrónimos: TSS

Ver:

- *Sello de tiempo*

2.941.1 SERVICIO DE FECHADO ELECTRÓNICO

Servicio que asegura la existencia de unos ciertos datos en un instante determinado.

2.941.2 (EN) TIME-STAMPING SERVICE (TSS)

a service providing evidence that a data item existed before a certain point in time. [ISO-18014-1:2002]

2.941.3 (EN) TIME STAMPING SERVICE

A service which attests the existence of electronic data at a precise instant of time.

NOTE. Time stamping services are useful and probably indispensable to support long-term validation of signatures.

[ISO-15945:2002]

2.942 SERVICIO DE SEGURIDAD

2.942.1 SERVICIO DE SEGURIDAD

Servicio suministrado por uno o más niveles de un sistema abierto de comunicación, que garantiza la seguridad del sistema y de las transferencias de datos (ISO-7498-2).

Los servicios reconocidos por la norma citada son: confidencialidad, autenticación, integridad, no repudio, control de acceso y disponibilidad.

[Ribagorda:1997]

2.942.2 SERVICIO DE SEGURIDAD

Referido a un sistema de telecomunicaciones, servicio proporcionado por un nivel determinado que aporta aspectos parciales de seguridad a la transferencia de información por dicho sistema. Se materializa en unos mecanismos de seguridad. [CESID:1997]

2.942.3 SERVICIO DE SEGURIDAD

Servicio proporcionado por una capa de sistemas abiertos comunicantes, que garantiza la seguridad adecuada de los sistemas y de la transferencia de datos. [ISO-7498-2:1989]

2.942.4 (EN) SECURITY SERVICE

A capability that supports one, or more, of the security requirements (Confidentiality, Integrity, Availability). Examples of security services are key management, access control, and authentication. [CNSSI_4009:2010]

2.942.5 (EN) SECURITY SERVICE

A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers. [ISO-7498-2:1989]

2.942.6 (FR) SERVICE DE SÉCURITÉ

Service, fourni par une couche de systèmes ouverts, garantissant une sécurité des systèmes et du transfert de données. [ISO-7498-2:1989]

2.943 SET - SECURE ELECTRONIC TRANSACTIONS

Acrónimos: SET

Ver:

- http://www.globeset.com

2.943.1 SET: SECURE ELECTRONIC TRANSACTION

SET es un protocolo elaborado por iniciativa de VISA y MasterCard al que se adhirieron inicialmente un gran número de grandes bancos y empresas de software de todo el mundo. Se preveía que en poco tiempo se generalizaría su uso, pero, varios años después de su puesta en marcha, observamos que sigue sin generalizarse su uso y los expertos no ven probable que sea utilizado en el futuro.

http://www.eumed.net/cursecon/ecoinet/seguridad/set.htm

2.943.2 (EN) SECURE ELECTRONIC TRANSACTIONS (SET)

Secure Electronic Transactions is a protocol developed for credit card transactions in which all parties (customers, merchant, and bank) are authenticated using digital signatures, encryption protects the message and provides integrity, and provides end-to-end security for credit card transactions online.

http://www.sans.org/security-resources/glossary-of-terms/

2.943.3 (FR) SET - SECURE ELECTRONIC TRANSACTIONS

Protocole de sécurisation des transactions financières sur Internet, SET a été initié par Visa, Mastercard, Microsoft et Netscape en particulier.

SET repose sur la technique de cryptographie asymétrique RSA pour l'authentification mutuelle, la confidentialité et la signature, et fait intervenir une tierce partie de confiance entre le marchand, le client et la banque.

http://securit.free.fr/glossaire.htm

2.944 SEUDOALEATORIO

Ver:

- *Generador de números aleatorios*
- *Aleatorio*

2.944.1 SEUDOALEATORIO

Sucesión de datos generados por un algoritmo pero que pasan las pruebas habituales de aleatoriedad.

Los números aleatorios son necesarios en gran número de técnicas y protocolos criptográficos, como generación de claves criptográficas, sistemas de autenticación fuerte, etc.

[Ribagorda:1997]

2.944.2 (EN) PSEUDORANDOM

(I) A sequence of values that appears to be random (i.e., unpredictable) but is actually generated by a deterministic algorithm. (See: compression, random, random number generator.) [RFC4949:2007]

2.945 SEUDÓNIMO

2.945.1 SEUDÓNIMO

1. adj. Dicho de un autor: Que oculta con un nombre falso el suyo verdadero.

3. m. Nombre utilizado por un artista en sus actividades, en vez del suyo propio.

DRAE. Diccionario de la Lengua Española.

2.945.2 (EN) PSEUDONYM

1. A subscriber name that has been chosen by the subscriber that is not verified as meaningful by identity proofing.

2. An assigned identity that is used to protect an individual's true identity.

[CNSSI_4009:2010]

2.946 S-FTP

2.946.1 S-FTP

Acrónimo de "Secure-FTP" (FTP seguro). S-FTP posee la capacidad de cifrar la información de autenticación y los archivos de datos en tránsito. Consulte FTP.

http://es.pcisecuritystandards.org

2.946.2 (EN) S-FTP

Acronym for Secure-FTP. S-FTP has the ability to encrypt authentication information and data files in transit. See FTP.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.946.3 (FR) S-FTP

Acronyme de Secure-FTP, FTP sécurisé. S-FTP a la capacité de crypter les informations d'authentification et les fichiers de données en transit. Voir FTP.

http://fr.pcisecuritystandards.org/

2.947 SHACAL

Ver:

- *Cifrado en bloque*
- *Criptografía de clave secreta*
- https://www.cosic.esat.kuleuven.be/nessie/
- http://en.wikipedia.org/wiki/SHACAL

2.947.1 SHACAL

Algoritmo de cifra basado en un secreto compartido (clave). Cifra el texto en bloques de 128-512 bits. Utiliza claves de 160 (SHACAL-1) o 256 bits (SHACAL-2).

2.947.2 (EN) SHACAL

In cryptography, SHACAL-1 and SHACAL-2 are block ciphers based on cryptographic hash functions from the SHA family. They were designed by Helena Handschuh and David Naccache of the smart card manufacturer Gemplus.

SHACAL-1 (originally simply SHACAL) is a 160-bit block cipher based on SHA-1, and supports keys from 128-bit to 512-bit. SHACAL-2 is a 256-bit block cipher based upon the larger hash function SHA-256.

http://en.wikipedia.org/wiki/SHACAL-2

2.948 SHALL

Ver:

- http://www.ietf.org/rfc/rfc2119
- *Obligatorio*

2.948.1 (EN) MUST

This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

2.948.2 (EN) SHALL

within normative text, shall indicates requirements strictly to be followed in order to conform to the document and from which no deviation is permitted. [CC:2006]

2.949 SHALL_NOT

Ver:

- http://www.ietf.org/rfc/rfc2119

2.949.1 (EN) MUST NOT

This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

2.950 SHA - SECURE HASH ALGORITHM

Acrónimos: SHA, SHS

Ver:

- *Hash*
- http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf
- http://www.ietf.org/rfc/rfc3174
- http://www.ietf.org/rfc/rfc3874
- http://www.ietf.org/rfc/rfc4634
- *MD5 - algoritmo resumen*
- http://en.wikipedia.org/wiki/SHA

2.950.1 ALGORITMO DE AUTENTICACIÓN SEGURO

Algoritmo federal estadounidense de autentificación normalizado en 1993. Está concebido para su uso junto con el estándar federal de firma digital.

El SHA es similar en su forma de operación al MD-5, pero produce un resumen, de 160 bits, más largo que el éste y que el de cualquier otro algoritmo de autenticación de los usados con anterioridad.

Aunque todavía no ha sido ampliamente criptoanalizado, la longitud de su resumen lo hace menos proclive que otros algoritmos de este tipo a los ataques exhaustivos.

[Ribagorda:1997]

2.950.2 SHA-1

Algoritmo hash diseñado por el National Institute for Standards and Technology (NIST) y la National Security Agency (NSA) estadounidense para aplicaciones gubernamentales que emplean el algoritmo de firma digital DSA. Proporciona una salida de 160 bits y basa su diseño en la función MD4. [CESID:1997]

2.950.3 SHA

La familia SHA (Secure Hash Algorithm, Algoritmo de Hash Seguro) es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el National Institute of Standards and Technology (NIST). El primer miembro de la familia fue publicado en 1993 es oficialmente llamado SHA. Sin embargo, hoy día, no oficialmente se le llama SHA-0 para evitar confusiones con sus sucesores. Dos años más tarde el primer sucesor de SHA fue publicado con el nombre de SHA-1. Existen cuatro variantes más que se han publicado desde entonces cuyas diferencias se basan en un diseño algo modificado y rangos de salida incrementados: SHA-224, SHA-256, SHA-384, y SHA-512 (todos ellos son referidos como SHA-2).

En 1998, un ataque a SHA-0 fue encontrado pero no fue reconocido para SHA-1, se desconoce si fue la NSA quien lo descubrió pero aumentó la seguridad del SHA-1.

http://es.wikipedia.org/wiki/SHA

2.950.4 (EN) SHA HASH FUNCTIONS

The SHA (Secure Hash Algorithm) family is a set of related cryptographic hash functions. The most commonly used function in the family, SHA-1, is employed in a large variety of popular security applications and protocols, including TLS, SSL, PGP, SSH, S/MIME, and IPSec. SHA-1 is considered to be the successor to MD5, an earlier, widely-used hash function. Both are reportedly compromised. In some circles, it is suggested that SHA-256 or greater be used for critical technology. The SHA algorithms were designed by the National Security Agency (NSA) and published as a US government standard.

The first member of the family, published in 1993, is officially called SHA; however, it is often called SHA-0 to avoid confusion with its successors. Two years later, SHA-1, the first successor to SHA, was published. Four more variants have since been issued with increased output ranges and a slightly different design: SHA-224, SHA-256, SHA-384, and SHA-512 sometimes collectively referred to as SHA-2.

http://en.wikipedia.org/wiki/SHA

2.951 SHIM (SYSTEM HEALTH AND INTRUSION MONITORING)

Acrónimos: SHIM

Ver:

- *Sistema de detección de intrusiones*
- *Sistema de prevención de intrusiones*

2.951.1 SHIM (SYSTEM HEALTH AND INTRUSION MONITORING)

En sistemas de detección y prevención de intrusión, se trata de una capa de análisis que se intercepta los intercambios de datos entre aplicaciones.

2.951.2 (EN) SHIM

A layer of host-based intrusion detection and prevention code placed between existing layers of code on a host that intercepts data and analyzes it. [NIST-SP800-94:2007]

2.952 SHOULD

Ver:

- http://www.ietf.org/rfc/rfc2119
- *Obligatorio*

2.952.1 (EN) SHOULD

This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

2.952.2 (EN) SHOULD

within normative text, should indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required. (ISO/IEC) The CC interprets 'not necessarily required' to mean that the choice of another possibility requires a justification of why the preferred option was not chosen. [CC:2006]

2.953 SHOULD NOT

Ver:

- http://www.ietf.org/rfc/rfc2119

2.953.1 (EN) SHOULD NOT

This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

2.954 SHOULDER SURFING

2.954.1 SHOULDER SURFING

Espiar por detrás de un hombro para tratar de ver información interesante. Es un método comúnmente usado para acceder cuentas de otras personas.

http://www.segu-info.com.ar/glosario/

2.954.2 (EN) SHOULDER SURFING

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand.

http://searchsecurity.techtarget.com/

2.954.3 (EN) SHOULDER SURFING

In computer security, shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. It is commonly used to obtain passwords, PINs, security codes, and similar data.

https://en.wikipedia.org/wiki/Shoulder_surfing_%28computer_security%29

2.955 SIDEJACKING

2.955.1 SIDEJACKING

práctica relacionada al Session hijacking, pero generalmente con el invasor y la víctima en una misma red. Son muy frecuentes los ataques de este tipo en hotspots Wi-Fi sin seguridad habilitada.

2.955.2 (EN) CAPEC-102: SESSIONSIDEJACKING

Attack Pattern ID: 102

Session sidejacking takes advantage of an unencrypted communication channel between a victim and target system. The attacker sniffs traffic on a network looking for session tokens in unencrypted traffic. Once a session token is captured, the attacker performs malicious actions by using the stolen token with the targeted application to impersonate the victim.

This attack is a specific method of session hijacking, which is exploiting a valid session token to gain unauthorized access to a target system or information. Other methods to perform a session hijacking are session fixation, cross-site scripting, or compromising a user or server machine and stealing the session token.

https://capec.mitre.org/data/definitions/

2.955.3 (EN) SIDEJACKING

Term used to describe the malicious act of hijacking an engaged Web session with a remote service by intercepting and using the credentials that identified the user/victim to that specific server. Typically, SideJacking is most common on sites that require authentication through a username and password, such as online Web mail accounts as well as social networking sites. SideJacking works only if the site catches a non-SSL cookie, so any Web site that uses SSL exclusively would be safe from SideJackers. SideJacking was first demonstrated by Robert Graham, CEO of Errata Security at Black Hat in 2007.

http://www.webopedia.com/TERM/S/SideJacking.html

2.955.4 (EN) SIDEJACKING

Sidejacking refers to the use of unauthorized identification credentials to hijack a valid Web session remotely in order to to take over a specific Web server. Usually sidejacking attacks are performed through accounts where the user types in their username and password. Sidejacking attacks work to find a nonsecure sockets layer (SSL) cookie. Usually, websites that have users type in their usernames and passwords are the type that get sidejacked. Websites that use SSLs don't have as much of a chance of being sidejacked, but if the webmasters neglect to authenticate the site itself through encryption, SSL use can be negated. Unsecured Wi-Fi hot spots are also vulnerable.

http://www.techopedia.com/definition/4105/sidejacking

2.956 SIN CLASIFICAR

Ver:

- *Información clasificada*

2.956.1 UNCLASSIFIED ("SIN CLASIFICAR")

Técnicamente no es un nivel de clasificación, pero es usado por los documentos gubernamentales que no poseen una de las clasificaciones presentadas arriba.

http://es.wikipedia.org/wiki/Informaci%C3%B3n_clasificada

2.956.2 (EN) UNCLASSIFIED

Information that has not been determined pursuant to E.O. 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and that is not designated as classified. [CNSSI_4009:2010]

2.956.3 (EN) UNCLASSIFIED

Technically not a classification level; but this is a feature of some classification schemes, used for government documents that do not merit a particular classification. This is because the information is low-impact, and therefore does not require any special protection, such as vetting of personnel.

2.956.4 (EN) UNCLASSIFIED

Unclassified is a security classification assigned to official information that does not warrant the assignment of Confidential, Secret, or Top Secret markings but which is not publicly-releasable without authorization.

http://www.fas.org/sgp/eprint/bagley.html

2.956.5 (FR) NON CLASSIFIÉ (UNCLASSIFIED)

Techniquement, ce n'est pas une classification, mais ce niveau est utilisé pour les documents gouvernementaux dont le niveau de sensibilité ne correspond pas à une des classifications ci-dessus. Ces documents peuvent être lus sans avoir une habilitation spécifique.

http://fr.wikipedia.org/wiki/Information_classifi%C3%A9e

2.957 SM3

Ver:

- *Hash*

2.957.1 SM3

Algoritmo de hash. Desarrollo del gobierno chino. Acepta mensajes en bloques de 512 bits, generando un resumen de 256 bits.

2.957.2 (EN) SM3

SM3 Cryptographic Hash Algorithm is a chinese national cryptographic hash algorithm standard published by the China National Cryptography Bureau in December 2010 . The SM3 take input messages as 512 bits blocks and generates 256 bits digest values, same as SHA-256.

http://infosec.pku.edu.cn/~guanzhi/libsm3/

2.958 SINGLE SIGN-ON

Acrónimos: SSO

Ver:

- *Kerberos*

2.958.1 SINGLE SIGN-ON

Single sign-on (SSO) es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación.

Hay cinco tipos principales de SSO, también se los llama reduced sign on systems (en inglés, sistemas de autenticación reducida).

- Enterprise single sign-on (E-SSO), también llamado legacy single sign-on, funciona luego de una autenticación primaria, interceptando los requerimientos de login presentados por las aplicaciones secundarias para completar los mismos con el usuario y

contraseña. Los sistemas E-SSO permiten interactuar con sistemas que pueden deshabilitar la presentación de la pantalla de login.

- Web single sign-on (Web-SSO), también llamado Web access management (Web-AM) trabaja sólo con aplicaciones y recursos accedidos vía web. Los accesos son interceptados con la ayuda de un servidor proxy o de un componente instalado en el servidor web destino. Los usuarios no autenticados que tratan de acceder son redirigidos a un servidor de autenticación y regresan solo después de haber logrado un acceso exitoso. Se utilizan cookies, para reconocer aquellos usuarios que acceden y su estado de autenticación.
- Kerberos es un método popular de externalizar la autenticación de los usuarios. Los usuarios se registran en el servidor Kerberos y reciben un "ticket", luego las aplicaciones-cliente lo presentan para obtener acceso.
- Federation es una nueva manera de concebir este tema, también para aplicaciones Web. Utiliza protocolos basados en estándares para habilitar que las aplicaciones puedan identificar los clientes sin necesidad de autenticación redundante.
- OpenID es un proceso de SSO distribuido y descentralizado donde la identidad se compila en una url que cualquier aplicación o servidor puede verificar.

http://es.wikipedia.org/wiki/Single_Sign-On

2.958.2 (EN) SINGLE SIGN-ON

1. (I) An authentication subsystem that enables a user to access multiple, connected system components (such as separate hosts on a network) after a single login at only one of the components. (See: Kerberos.)

2. (O) /Liberty Alliance/ A security subsystem that enables a user identity to be authenticated at an identity provider -- i.e., at a service that authenticates and asserts the user's identity -- and then have that authentication be honored by other service providers.

[RFC4949:2007]

2.958.3 (EN) SINGLE SIGN-ON

A log-in routine in which one logon provides access to all resources on the network.

http://www.watchguard.com/glossary/

2.958.4 (EN) SINGLE SIGN-ON

Single sign-on (SSO)is a session/user authentication process that permits a user to enter one name and password in order to access multiple applications. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.

http://searchsoftwarequality.techtarget.com/glossary/

2.958.5 (FR) SINGLE SIGN ON

Procédure d'authentification évitant à l'utilisateur de devoir s'identifier sur chaque nouveau système ou nouvelle application à laquelle il accède sous le couvert d'une première authentification réalisée avec succès sur le système d'information.

http://www.cases.public.lu/functions/glossaire/

2.959 SISTEMA

Ver:

- *Sistema de información*

2.959.1 SISTEMA

Conjunto de cosas que relacionadas entre sí ordenadamente contribuyen a determinado objeto.

DRAE. Diccionario de la Lengua Española.

2.959.1 SISTEMA

conjunto de elementos mutuamente relacionados o que interactúan. [ISO-9000_es:2000]

2.959.1 SISTEMA

Determinada instalación de tecnologías de la información con un fin concreto y un entorno operacional específico (ITSEC). [Ribagorda:1997]

2.959.2 (EN) SYSTEM

Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. See also information system. [CNSSI_4009:2010]

2.959.3 (EN) SYSTEM

any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose

DHS Risk Lexicon, September 2008

2.959.4 (EN) SYSTEM

a discrete, distinguishable entity with a physical existence and a defined purpose, completely composed of integrated, interacting components, each of which does not individually comply with the required overall purpose [ISO/IEC 15288].

NOTE 1. In practice, a system is 'in the eye of the beholder' and the interpretation of its meaning is frequently clarified by the use of an associative noun, (e.g., product system, aircraft system). Alternatively the word system may be substituted simply by a context dependent synonym, (e.g., product, aircraft), though this may then obscure a system principles perspective.

NOTE 2. The system may need other systems during its life cycle to meet its requirements. Example - an operational system may need a system for conceptualization, development, production, operation, support or disposal.

[ISO-21827:2007]

2.959.5 (EN) COMPUTER SYSTEM

"computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data

Budapest Convention on Cybercrime

2.959.1 (EN) SYSTEM

A specific IT installation, with a particular purpose and operational environment [ISO/IEC 15408]. a) A combination of interacting elements organized to achieve one or more stated purposes [ISO/IEC 15288].

NOTE 1. A system may be considered as a product and/or as the services it provides [ISO/IEC 15288].

NOTE 2. In practice, the interpretation of its meaning is frequently clarified by the use of an associative noun, e.g. aircraft system. Alternatively the word system may be substituted simply by a context dependent synonym, e.g. aircraft, though this may then obscure a system principles perspective [ISO/IEC 15288].

[ISO-15443-1:2005]

2.959.1 (EN) SUBSYSTEM

A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions. [NIST-SP800-53:2013]

2.959.2 (EN) SYSTEM

is any electronic computing or communications device or the applications running thereon which can create, access, transmit or receive data. Systems are typically connected to digital networks.

Examples of Systems include:

- A computer system whether or not connected to a data network,
- A database application used by an individual or a set of clients, A computer system used to connect over a network to another computer system,
- An analog or digital voice mail system,
- Data network segments including wireless data networks, and
- Portable digital assistants.

http://www.hipaa.yale.edu/overview/glossary.html

2.959.3 (EN) SYSTEM ADMINISTRATOR (SA)

Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures. [CNSSI_4009:2010]

2.959.4 (EN) SYSTEM ADMINISTRATOR

is the technical custodian of a System. This individual provides the technology and processes to implement the decisions of the System Owner. In some circumstances, e.g. small systems, typically Basic ePHI Systems, the System Administrator and the System Owner may be the same person. System Administrators are responsible for the technical operation, maintenance, and monitoring of the System. These duties include implementing appropriate technical, physical and administrative safeguards.

See also System Owner.

http://www.hipaa.yale.edu/overview/glossary.html

2.959.5 (EN) SYSTEM OWNER

Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system. [CNSSI_4009:2010]

2.959.6 (EN) SYSTEM OWNER

is the authority, individual, or organization head who has final responsibility for Systems which create, access, transmit or receive ePHI and including responsibility for the ePHI data. In some complex Systems, the functional responsibility for the System and the responsibility for the data may lie with more than one individual. Decisions regarding who has access to the System and related ePHI data and responsibility for the Risk Analysis rest solely with the System Owner. The System Owner usually delegates responsibility for the technical management of a System to a qualified System Administrator or staff who are capable of implementing appropriate technical, physical and administrative safeguards.

See also 'System Administrator'.

http://www.hipaa.yale.edu/overview/glossary.html

2.960 SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA

Acrónimos: SAI (es), UPS

2.960.1 SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA

Sistema alternativo de suministro de tensión para interrupciones de corta duración. Sirve también para compensar otras anomalías como transitorios, ruidos, picos de tensión, etc.

Hay dos tipos de SAIs, denominados en línea y fuera de línea. En los primeros, el equipo está situado en la línea de alimentación, por lo que el tiempo de conmutación, desde el corte de tensión en la línea exterior hasta la entrada en funcionamiento del equipo, es cero. Consiguientemente, la interrupción del servicio es inapreciable para el sistema informático.

En los segundos, el equipo se sitúa en paralelo con la línea de alimentación, requiriendo un tiempo para conmutarse desde dicha línea.

[Ribagorda:1997]

2.960.2 (EN) UNINTERRUPTIBLE POWER SUPPLY - UPS

Usually a battery-based system to protect devices against power outages, sags and surges. [ISO-18028-4:2005]

2.960.3 (FR) UPS (ALIMENTATION NON INTERRUPTIBLE)

Dispositif de protection (communément désigné par le terme d' onduleur) s'intercalant entre le réseau électrique standard et les équipements informatiques qui y sont raccordés. Son rôle consiste à pallier temporairement (quelques minutes) à une panne de l'alimentation électrique et à protéger les équipements informatiques qui lui sont connectés contre des surtensions du réseau électrique (en cas de foudre par exemple).

http://www.cases.public.lu/functions/glossaire/

2.961 SISTEMA DE CIFRA

Ver:

- *Cifrado*
- *Algoritmo de cifra*
- *Algoritmo de descifrado*
- *Generación de claves*

2.961.1 SISTEMA DE CIFRA

Conjunto de componentes destinados a asegurar la confidencialidad de la información. Consta de un algoritmo para cifrar, un algoritmo para descifrar y un método para generar claves.

2.961.2 (EN) ENCRYPTION SYSTEM

cryptographic technique used to protect the confidentiality of data, and which consists of three component processes: an encryption algorithm, a decryption algorithm, and a method for generating keys. [ISO-18033-1:2005]

2.961.3 (EN) ENCIPHERMENT SYSTEM

alternative term for encryption system. [ISO-18033-1:2005]

2.962 SISTEMA DE CIFRA ASIMÉTRICA

Ver:

- *Cifrado asimétrico*
- *Técnica criptográfica asimétrica*
- *Criptografía de clave pública*
- *Sistema de cifra*

2.962.1 SISTEMA DE CIFRA ASIMÉTRICA

Sistema basado en técnicas criptográficas asimétricas, usando la parte pública para cifrar y la parte secreta para descifrar.

2.962.2 (EN) ASYMMETRIC ENCIPHERMENT SYSTEM

system based on asymmetric cryptographic techniques whose public operation is used for encipherment and whose private operation is used for decipherment. [ISO-9798-5:2004]

2.962.3 (EN) ASYMMETRIC ENCIPHERMENT SYSTEM

A system based on asymmetric cryptographic techniques whose public transformation is used for encipherment and whose private transformation is used for decipherment. [ISO-11770-3:2008]

2.963 SISTEMA DE DETECCIÓN DE INTRUSIONES

Acrónimos: IDS

Ver:

- *Intrusión*
- *Sistema de prevención de intrusiones*
- *Detección de anomalías*
- *Shim (System Health and Intrusion Monitoring)*

2.963.1 IDS

Acrónimo de “intrusion detection system” (sistema de detección de intrusiones). Software o hardware utilizado para identificar o alertar acerca de intentos de intrusión en redes o sistemas. Conformado por sensores que generan eventos de seguridad; una consola que supervisa eventos y alertas y controla los sensores; y un motor central que registra en una base de datos los eventos denotados por los sensores. Utiliza un sistema de reglas que generan alertas en respuesta a cualquier evento de seguridad detectado. Consulte IPS

http://es.pcisecuritystandards.org

2.963.2 SISTEMA DE DETECCIÓN DE INTRUSIONES

Sistema con la función de detectar indicios de ataque o compromiso desde o hacia los elementos que conforman nuestro STIC. [CCN-STIC-400:2006]

2.963.3 IDS

Programa usado para detectar accesos desautorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos piratas informáticos que usan herramientas automáticas. En el mercado existen diferentes versiones, de hardware y de software. El funcionamiento de estas herramientas se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, y/o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. Normalmente esta herramienta se integra con un cortafuegos. El detector de intrusos es incapaz de detener los ataques por si solo "excepto los que están embebidos en un dispositivo de pasarela con funcionalidad de cortafuegos", pero al estar trabajando en conjunto con el cortafuegos se convierten en una herramienta muy poderosa ya que se une la inteligencia del IDS, no solo analiza qué tipo de tráfico, si no que también revisa el contenido y su comportamiento, y el poder de bloqueo del cortafuegos, este al ser el punto donde forzosamente deben pasar los paquetes, ahí pueden ser bloqueados sin problema alguno.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.963.4 IDS

Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es una aplicación usada para detectar accesos no autorizados a un ordenador/servidor o a una red. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o a través de herramientas automáticas.

http://www.inteco.es/glossary/Formacion/Glosario/

2.963.5 (EN) INTRUSION DETECTION SYSTEMS (IDS)

Hardware or software products that gather and analyze information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from with the organizations). [CNSSI_4009:2010]

2.963.6 (EN) INTRUSION DETECTION SYSTEMS (IDS), (HOST-BASED)

IDSs which operate on information collected from within an individual computer system. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the Operating System. Furthermore, unlike network-based IDSs, host-based IDSs can more readily “see” the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks. [CNSSI_4009:2010]

2.963.7 (EN) INTRUSION DETECTION SYSTEMS (IDS), (NETWORK-BASED)

IDSs which detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment. [CNSSI_4009:2010]

2.963.8 (EN) INTRUSION DETECTION SYSTEM (IDS)

1. (N) A process or subsystem, implemented in software or hardware, that automates the tasks of (a) monitoring events that occur in a computer network and (b) analyzing them for signs of security problems. [SP31] (See: intrusion detection.)

2. (N) A security alarm system to detect unauthorized entry. [DC6/9].

Tutorial: Active intrusion detection processes can be either host- based or network-based:

- "Host-based": Intrusion detection components -- traffic sensors and analyzers -- run directly on the hosts that they are intended to protect.
- "Network-based": Sensors are placed on subnetwork components, and analysis components run either on subnetwork components or hosts.

[RFC4949:2007]

2.963.9 (EN) INTRUSION DETECTION

(I) Sensing and analyzing system events for the purpose of noticing (i.e., becoming aware of) attempts to access system resources in an unauthorized manner. (See: anomaly detection, IDS, misuse detection. Compare: extrusion detection.) [IDSAN, IDSSC, IDSSE, IDSSY]

Usage: This includes the following subtypes:

- "Active detection": Real-time or near-real-time analysis of system event data to detect current intrusions, which result in an immediate protective response.
- "Passive detection": Off-line analysis of audit data to detect past intrusions, which are reported to the system security officer for corrective action. (Compare: security audit.)

[RFC4949:2007]

2.963.10 (EN) APPLICATION-BASED INTRUSION DETECTION AND PREVENTION SYSTEM

A host-based intrusion detection and prevention system that performs monitoring for a specific application service only, such as a Web server program or a database server program.

[NIST-SP800-94:2007]

2.963.11 (EN) HOST-BASED INTRUSION DETECTION AND PREVENTION SYSTEM

A program that monitors the characteristics of a single host and the events occurring within that host to identify and stop suspicious activity. [NIST-SP800-94:2007]

2.963.12 (EN) INTRUSION DETECTION

The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents. [NIST-SP800-94:2007]

2.963.13 (EN) INTRUSION DETECTION AND PREVENTION

The process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, and attempting to stop detected possible incidents. See also intrusion prevention. [NIST-SP800-94:2007]

2.963.14 (EN) INTRUSION DETECTION SYSTEM

Software that automates the intrusion detection process. [NIST-SP800-94:2007]

2.963.15 (EN) NETWORK-BASED INTRUSION DETECTION AND PREVENTION SYSTEM

An intrusion detection and prevention system that monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify and stop suspicious activity. [NIST-SP800-94:2007]

2.963.16 (EN) NETWORK BEHAVIOR ANALYSIS SYSTEM

An intrusion detection and prevention system that examines network traffic to identify and stop threats that generate unusual traffic flows. [NIST-SP800-94:2007]

2.963.17 (EN) WIRELESS INTRUSION DETECTION AND PREVENTION SYSTEM

An intrusion detection and prevention system that monitors wireless network traffic and analyzes its wireless networking protocols to identify and stop suspicious activity involving the protocols themselves. [NIST-SP800-94:2007]

2.963.18 (EN) INTRUSION DETECTION

the formal process of detecting intrusions. The process is generally characterized by gathering knowledge about abnormal usage patterns as well as what, how, and which vulnerability has been exploited to include how and when it occurred. [ISO-18028-1:2006]

2.963.19 (EN) INTRUSION DETECTION SYSTEM (IDS)

a technical system that is used to identify that an intrusion has been attempted, is occurring, or has occurred and possibly respond to intrusions in information systems and networks. [ISO-18028-1:2006]

2.963.20 (EN) INTRUSION DETECTION SYSTEM (IDS)

Software that looks for suspicious activity and alerts administrators. [NIST-SP800-61:2004]

2.963.21 (EN) IDS

Acronym for “intrusion detection system.” Software or hardware used to identify and alert on network or system intrusion attempts. Composed of sensors that generate security events; a console to monitor events and alerts and control the sensors; and a central engine that records events logged by the sensors in a database. Uses system of rules to generate alerts in response to security events detected.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.963.22 (EN) INTRUSION PREVENTION SYSTEM.

Intrusion protection systems perform the same detection functions of an IDS. with the added capability to block traffic. Traffic can typically be blocked by dropping the offending packets). or by forcing a reset of the offending TCP/IP session. IPS works in-line. and therefore may introduce latency. [knapp:2014]

2.963.23 (EN) INTRUSION DETECTION SYSTEM

Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment

(sometimes refered to as scanning), which is a technology developed to assess the security of a computer system or network.

http://searchsecurity.techtarget.com/

2.963.1 (EN) HIDS: HOST IDS.

A Host Intrusion Detection System, which detects intrusion attempts via a Software agent running on a specific host. A HIDS detects intrusions by inspecting packets and matching the contents against defined patterns or "signatures" that indicate malicious content. and produce an alert. [knapp:2014]

2.963.2 (EN) HIPS: HOST IPS.

A Host Intrusion Prevention System. which detects and prevents intrusion attempts via a software agent running on a specific host. Like a HIDS. u HIPS detects intrusions by inspecting packets and matching the contents against defined patterns or "signatures" that indicate malicious content. and produce an alert. [knapp:2014]

2.963.3 (EN) HIDS/NIDS (HOST INTRUSION DETECTION SYSTEMS AND NETWORK INTRUSION DETECTION SYSTEMS)

Host intrusion detection systems (HIDS) and network intrusion detection systems (NIDS) are methods of security management for computers and networks. In HIDS, anti-threat applications such as firewalls, antivirus software and spyware-detection programs are installed on every network computer that has two-way access to the outside environment such as the Internet. In NIDS, anti-threat software is installed only at specific points such as servers that interface between the outside environment and the network segment to be protected.

All methods of intrusion detection (ID) involve the gathering and analysis of information from various areas within a computer or network to identify possible threats posed by hackers and crackers inside or outside the organization. Host-based and network-based ID systems have their respective advantages and limitations. The most effective protection for a proprietary network is provided by a combination of both technologies.

http://searchsecurity.techtarget.com/

2.963.4 (EN) NETWORK-BASED IDS

A network-based IDS system monitors the traffic on its network segment as a data source. This is generally accomplished by placing the network interface card in promiscuous mode to capture all network traffic that crosses its network segment.

Network traffic on other segments, and traffic on other means of communication (like phone lines) can't be monitored. Network-based IDS involves looking at the packets on the network as they pass by some sensor. The sensor can only see the packets that happen to be carried on the network segment it's attached to. Packets are considered to be of interest if they match a signature.Network -based intrusion detection passively monitors network activity for indications of attacks. Network monitoring offers several advantages over traditional host-based intrusion detection systems. Because many intrusions occur over networks at some point, and because networks are increasingly

becoming the targets of attack, these techniques are an excellent method of detecting many attacks which may be missed by host-based intrusion detection mechanisms.

http://www.sans.org/security-resources/glossary-of-terms/

2.963.5 (EN) INTRUSION DETECTION

A security service that monitors and analyzes system events to find and provide real-time or near real-time attempt warnings to access system resources in an unauthorized manner. This is the detection of break-ins or break-in attempts, by reviewing logs or other information available on a network.

http://www.symantec.com/avcenter/refa.html

2.963.6 (EN) INTRUSION DETECTION

A security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

http://www.sans.org/security-resources/glossary-of-terms/

2.963.7 (FR) IDS

Acronyme d'«intrusion detection system», système de détection d'intrusion. Logiciel ou matériel utilisé pour identifier les tentatives d'intrusion dans un réseau ou un système et donner l'alerte. Constitué de capteurs qui génèrent des événements de sécurité, d'une console pour la surveillance des événements et des alertes et le contrôle des capteurs, ainsi que d'un moteur central qui enregistre dans une base de données les événements consignés par les capteurs. Utilise un système de règles pour déclencher des alertes en réponse aux événements de sécurité détectés. Voir IPS

http://fr.pcisecuritystandards.org/

2.963.8 (FR) DÉTECTION D'INTRUSION

Mécanisme de sécurité permettant la détection d'intrusion en temps réel au niveau d'un réseau informatique. Les IDS sont de plus en plus utilisés en complément des mécanismes de sécurité existant tel que les firewalls ou autres routeurs filtrants.

http://www.cases.public.lu/functions/glossaire/

2.964 SISTEMA DE FIRMA ASIMÉTRICA

Ver:

- *Técnica criptográfica asimétrica*

2.964.1 SISTEMA DE FIRMA ASIMÉTRICA

Sistema basado en técnicas de criptografía asimétrica, donde la parte secreta se usa para firmar, mientras que la parte pública sirve para verificar la firma.

2.964.2 (EN) ASYMMETRIC SIGNATURE SYSTEM

system based on asymmetric cryptographic techniques whose private transformation is used for signing and whose public transformation is used for verification. [ISO-9798-1:1997]

2.965 SISTEMA DE GESTIÓN

2.965.1 SISTEMA DE GESTIÓN

Conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos.

NOTA 1. Un sistema de gestión puede tratar una sola disciplina o varias disciplinas.

NOTA 2. Los elementos del sistema incluyen la estructura de la organización, los roles y las responsabilidades, la planificación, la operación, etc.

NOTA 3. El alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones dentro de un grupo de organizaciones.

[ISO Anexo SL] [UNE-ISO/IEC 27000:2014]

2.965.1 (EN) MANAGEMENT SYSTEM

set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives

NOTE 1: A management system can address a single discipline or several disciplines.

NOTE 2: The system elements include the organization’s structure, roles and responsibilities, planning, operation, etc.

NOTE 3: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

[ISO Annex SL] [ISO-27000:2014]

2.966 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

Acrónimos: SGSI (es), ISMS

Ver:

- *Ciclo de Deming*
- *Gestión de la seguridad de la información*

2.966.1 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN (ISMS)

(Diseño del Servicio) Marco de Políticas, Procesos, Estándares, Líneas Maestras y herramientas que aseguran que una Organización puede alcanzar sus objetivos en la Gestión de la Seguridad de la Información. [ITIL:2007]

2.966.2 (EN) INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

(Service Design) The framework of Policy, Processes, Standards, Guidelines and tools that ensures an Organisation can achieve its Information Security Management Objectives. [ITIL:2007]

2.966.3 (EN) INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

http://www.informationstandards.com/resources_glossary.htm

2.966.4 (FR) SYSTEME DE GESTION DE LA SECURITE INFORMATIQUE (ISMS)

(Conception de services) Le cadre de travail de la politique, des processus, standards, principes et outils qui assurent à une organisation qu'elle atteindra ses objectifs de Gestion de la Sécurité de l'Information. [ITIL:2007]

2.967 SISTEMA DE INFORMACIÓN

Ver:

- *Información*
- *Sistema*

2.967.1 SISTEMA DE INFORMACIÓN

Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar (tratar), mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. [UNE-71504:2008]

2.967.2 SISTEMA DE INFORMACIÓN

aplicaciones, servicios, activos relacionados con tecnologías de la información y otros componentes para manejar información

[UNE-ISO/IEC 27000:2014]

2.967.3 SISTEMA DE INFORMACIÓN

Conjunto específico de recursos de datos estructurados organizados para recolectar, procesar, mantener, usar, compartir, diseminar o disponer de la información.

http://es.pcisecuritystandards.org

2.967.4 SISTEMA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Conjunto de equipos, métodos, procedimientos y personal, organizado de tal forma que permita almacenar, procesar o transmitir información que está bajo responsabilidad de una única Autoridad.

2.967.5 SISTEMA DE INFORMACIÓN

Los ordenadores y redes de comunicaciones electrónicas, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento. [Magerit:2012]

2.967.6 SISTEMA DE INFORMACIÓN

«sistema de información»: todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento;

Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a los ataques contra los sistemas de información, por la que se deroga la Decisión marco 2005/222/JAI del Consejo, Bruselas, 30.9.2010, COM(2010) 517 final, 2010/0273 (COD)

2.967.7 SISTEMA DE INFORMACIÓN (SI)

Conjunto de entidades organizado para cumplir funciones de procesamiento de datos. [EBIOS:2005]

2.967.8 SISTEMA DE INFORMACIÓN

los ordenadores y redes de comunicaciones electrónicas, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento.

Reglamento (CE) n 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información.

2.967.9 SISTEMAS DE INFORMACIÓN

Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

2.967.10 SISTEMA DE INFORMACIÓN (IT)

Cualquier sistema o producto destinado a almacenar, procesar, o transmitir información. [CESID:1997]

2.967.11 (EN) INFORMATION SYSTEM

application, service, information technology asset, or any other information handling component [ISO-27000:2014]

2.967.12 (EN) INFORMATION TECHNOLOGY

A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. In the context of this publication, the definition includes interconnected or dependent business systems and the environment in which they operate. [US-ESC:2012]

2.967.13 (EN) INFORMATION SYSTEM

"information system" means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance;

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, COM(2010) 517 final, 2010/0273 (COD)

2.967.1 (EN) INFORMATION SYSTEM (IS)

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control system.

[CNSSI_4009:2010]

2.967.2 (EN) INFORMATION SYSTEM

(I) An organized assembly of computing and communication resources and procedures -- i.e., equipment and services, together with their supporting infrastructure, facilities, and personnel -- that create, collect, record, process, store, transport, retrieve, display, disseminate, control, or dispose of information to accomplish a specified set of functions. (See: system entity, system resource. Compare: computer platform.) [RFC4949:2007]

2.967.3 (EN) INFORMATION SYSTEM (IS).

An assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information and textual material. [DoD 5220:2006]

2.967.4 (EN) INFORMATION SYSTEM

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

U.S. Code 44, Sec. 3502. Definitions, 2007

2.967.5 (EN) INFORMATION SYSTEM (IS)

All entities organised to accomplish the information processing functions. [EBIOS:2005]

2.967.6 (EN) SYSTÈME D'INFORMATION (SI)

Ensemble d'entités organisé pour accomplir des fonctions de traitement d'information. [EBIOS:2005]

2.967.7 (EN) INFORMATION SYSTEM

Any procedure or process, with or without IT support, that provides a way of acquiring, storing, processing or disseminating information.

2.967.8 (EN) INFORMATION SYSTEM

means computers and electronic communication networks, as well as electronic data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance.

REGULATION (EC) No 460/2004 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 10 March 2004 establishing the European Network and Information Security Agency.

2.967.9 (EN) INFORMATION SYSTEM

Information systems include applications and their supporting infrastructure. [CRAMM:2003]

2.967.10 (EN) INFORMATION SYSTEM

Discrete set of structured data resources organized for collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.967.11 (EN) INFORMATION SYSTEM

Information system means computers and electronic communication networks, and also electronic data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance.

http://www.enisa.europa.eu/

2.967.12 (FR) SYSTÈME D'INFORMATION

Ensemble distinct de ressources de données structurées pour la collecte, le traitement, la maintenance, l'utilisation, le partage, la diffusion ou l'élimination des informations.

http://fr.pcisecuritystandards.org/

2.967.13 (FR) SYSTÈME D'INFORMATION

«système d'information»: tout dispositif isolé ou groupe de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, conformément à un programme, un traitement automatisé de données informatiques, ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ces derniers en vue de leur fonctionnement, utilisation, protection et maintenance;

Proposition de DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI du Conseil, Bruxelles, le 30.9.2010, COM(2010) 517 final, 2010/0273 (COD)

2.967.14 (FR) SYSTÈME D'INFORMATION

Ensemble des moyens humains et matériels ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire l'information. [IGI 1300] [EBIOS:2010]

2.967.15 (FR) SYSTÈME D'INFORMATION

Tout moyen dont le fonctionnement consiste au traitement (stockage, modification, transmission) de l'information sous forme de données.

http://www.cases.public.lu/functions/glossaire/

2.968 SISTEMA DE PREVENCIÓN DE INTRUSIONES

Acrónimos: IPS

Ver:

- *Intrusión*
- *Sistema de detección de intrusiones*

2.968.1 IPS

Acrónimo de “intrusion prevention system” (sistema de prevención de intrusiones). El IPS va un paso más allá que el IDS y bloquea el intento de intrusión.

http://es.pcisecuritystandards.org

2.968.2 SISTEMA DE PREVENCIÓN DE INTRUSIONES

Aproximación de un IDS a la tecnología cortafuegos consistente en permitir o denegar el tráfico mediante el uso de firmas o análisis de anomalías. [CCN-STIC-400:2006]

(en) Intrusion Prevention System (IPS)

System that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets. [CNSSI_4009:2010]

2.968.3 (EN) INTRUSION PREVENTION

The process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, and attempting to stop detected possible incidents. See also intrusion detection and prevention. [NIST-SP800-94:2007]

2.968.4 (EN) INTRUSION PREVENTION SYSTEM

Software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. Also called an intrusion detection and prevention system. [NIST-SP800-94:2007]

2.968.5 (EN) INTRUSION PREVENTION SYSTEM (IPS)

a variant on intrusion detection systems that are specifically designed to provide an active response capability. [ISO-18028-1:2006]

2.968.6 (EN) IPS

Acronym for “intrusion prevention system.” Beyond an IDS, an IPS takes the additional step of blocking the attempted intrusion.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.968.7 (EN)IPS INTRUSION PREVENTION SYSTEM.

Intrusion protection systems perform the same detection functions of an IDS, with the added capability to block traffic. Traffic can typically be blocked by dropping the offending packet(s), or by forcing a reset of the offending TCP/ IP session. IPS works in-line, and therefore may introduce latency. [knapp:2014]

2.968.8 (EN) INTRUSION PREVENTION SYSTEM

Intrusion prevention is a preemptive approach to network security used to identify potential threats and respond to them swiftly. Like an intrusion detection system (IDS), an intrusion prevention system (IPS) monitors network traffic. However, because an exploit may be carried out very quickly after the attacker gains access, intrusion prevention systems also have the ability to take immediate action, based on a set of rules established by the network administrator.

http://searchsecurity.techtarget.com/

2.968.9 (EN) NIDS: NETWORK IDS.

A network intrusion detection system detects intrusion attempts via a net- work interface card. which connects to the network either in-line or via a span or tap port. [knapp:2014]

2.968.10 (EN) NIPS: NETWORK IPS.

A network intrusion prevention detection system detects and prevents intrusion attempts via a network-attached device using two or more network interface cards to support inbound and outbound network traffic, with optional bypass interfaces to preserve network reliability in the event of a NIPS failure. [knapp:2014]

2.968.11 (FR) IPS

Acronyme d'«intrusion prevention system», système de prévention d'intrusion. Au-delà de l'IDS, un ISP prend la mesure plus poussée de bloquer la tentative d'intrusion.

http://fr.pcisecuritystandards.org/

2.969 SISTEMA DE PREVENCIÓN DE INTRUSIONES EN LA RED

Acrónimos: NIPS

Ver:

- *Sistema de prevención de intrusiones*
- *Sistema de detección de intrusiones*

2.969.1 IPS

Siglas de Intrusion Prevention System (sistema de prevención de intrusiones). Es una herramienta de seguridad que detecta un posible ataque informático y reacciona para evitar su consumación.

http://www.inteco.es/glossary/Formacion/Glosario/

2.969.2 (EN) NETWORK INTRUSION PROTECTION SYSTEM (NIPS)

A network intrusion protection system (NIPS) is an umbrella term for a combination of hardware and software systems that protect computer networks from unauthorized access and malicious activity.

NIPS hardware may consist of a dedicated Network Intrusion Detection System (NIDS) device, an Intrusion Prevention System (IPS), or a combination of the two such as an Intrusion Prevention and Detection System (IPDS). Note that while an NIDS can only detect intrusions, an IPS can proactively stop an attack by following established rules, such as changing firewall settings, blocking particular Internet protocol (IP) addresses or dropping certain packets entirely. The software components of an NIPS consists of various firewall, sniffer and antivirus tools in addition to dashboards and other data visualization tools.

http://searchsecurity.techtarget.in/definition/network-intrusion-protection-system-NIPS

2.970 SISTEMA SEGURO MULTINIVEL

Acrónimos: MLS

Ver:

- http://en.wikipedia.org/wiki/Multilevel_security

2.970.1 SISTEMA SEGURO MULTINIVEL

Sistema que contiene información con diferentes niveles de clasificación y permite el acceso simultáneo de usuarios con diferentes niveles de habilitación y diferente necesidad de conocer. No obstante, el sistema es capaz de garantizar que el acceso a los objetos de información sigue estando controlado por habilitación y necesidad de conocer.

2.970.1 (EN) MULTILEVEL SECURITY (MLS)

Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization. [CNSSI_4009:2010]

2.970.2 (EN) MULTILEVEL SECURE (MLS)

(I) Describes an information system that is trusted to contain, and maintain separation between, resources (particularly stored data) of different security levels. (Examples: BLACKER, CANEWARE, KSOS, Multics, SCOMP.)

Usage: Usually understood to mean that the system permits concurrent access by users who differ in their access authorizations, while denying users access to resources for which they lack authorization.

[RFC4949:2007]

2.970.3 (EN) MULTILEVEL SECURE

A class of system containing information with different sensitivities that simultaneously permits access by users with different security clearances and needs-to-know, but prevents users from obtaining access to information for which they lack authorization. [TCSEC:1985]

2.971 SISTEMA TRAMPA

Ver:

- *Red trampa*

2.971.1 SISTEMA TRAMPA

Sistema/máquina "trampa" utilizado para atraer a posibles intrusos.

2.971.2 MÁQUINA TRAMPA (HONEYPOT)

recurso cuyo valor reside en hecho de ser comprometido. Al ser elementos no productivos, cualquier actividad dirigida u originada en ellos es considerada maliciosa y por tanto de gran utilidad en detección de intrusiones como elemento de alerta temprana. [CCN-STIC-401:2007]

2.971.3 TARRO DE MIEL

Es un sistema diseñado para analizar cómo los intrusos emplean sus armas para intentar entrar en un sistema (analizan las vulnerabilidades) y alterar, copiar o destruir sus datos o la totalidad de éstos (por ejemplo borrando el disco duro del servidor). Por medio del aprendizaje de sus herramientas y métodos se puede, entonces, proteger mejor los sistemas. Pueden constar de diferentes aplicaciones, una de ellas sirve para capturar al intruso o aprender cómo actúan sin que ellos sepan que están siendo vigilados.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.971.4 (EN) HONEYPOT:

A deception technique in which a person seeking to defend computing devices and cyber infrastructure against cyber operations uses a virtual environment designed to lure the attention of intruders with the aim of: deceiving the intruders about the nature of the environment; having the intruders waste resources on the decoy environment; and gathering counterintelligence about the intruder's intent, identity, and means and methods of cyber operation. The honeypot can be co-resident with the real targets the intruder would like to attack, but the honeypot itself is isolated from the rest of the systems being defended via software wrappers, separate hardware, and other isolation techniques such that the intruder's operations are contained.

The Tallinn Manual, 2013

2.971.5 (EN) HONEYPOT

A system (e.g., a web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders and has no authorized users other than its administrators. [CNSSI_4009:2010]

2.971.6 (EN) HONEY POT

(N) A system (e.g., a web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders, like honey is attractive to bears. (See: entrapment.) [RFC4949:2007]

2.971.7 (EN) HONEYPOT

A host that is designed to collect data on suspicious activity and has no authorized users other than its administrators. [NIST-SP800-61:2004]

2.971.8 (EN) HONEY POT

A system designed to look like a regular network but which, in fact, monitors and traces unauthorised access.

http://www.getsafeonline.org/

2.971.9 (EN) HONEY POT

A honey pot is a computer system on the Internet that is expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems.

http://searchtechtarget.techtarget.com/glossaryBrowseAlpha/

2.971.10 (EN) HONEY POT

Programs that simulate one or more network services that you designate on your computer's ports. An attacker assumes you're running vulnerable services that can be used to break into the machine. A honey pot can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack.

http://www.sans.org/security-resources/glossary-of-terms/

2.971.11 (EN) ENTRAPMENT

(I) "The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations or confusing an intruder about which flaws to exploit." [FP039] (See: honey pot.) [RFC4949:2007]

2.971.12 (FR) POT DE MIEL

Site leurre simulant un site de production configuré avec une sécurité moyenne ou minime. Le but est d'attirer les pirates informatiques afin de les détourner du véritable site de production mais aussi dans le but d'analyser leurs techniques d'intrusion et de découvrir les nouvelles tendances en la matière afin d'optimiser et d'adapter les mécanismes de protection.

http://www.cases.public.lu/functions/glossaire/

2.972 SKIPJACK

Ver:

- *Cifrado en bloque*
- *Criptografía de clave secreta*
- http://en.wikipedia.org/wiki/Skipjack_%28cipher%29

2.972.1 SKIPJACK

Algoritmo de cifra basado en un secreto compartido (clave). Cifra el texto en bloques de 64 bits. Utiliza claves de 80 bits.

2.972.2 SKIPJACK

Algoritmo de cifrado en bloque de 64 bits que emplea claves de 80 bits, desarrollado por la National Security Agency (NSA) estadounidense para su implementación en los chips Clipper y Capstone que emplean mecanismos de depósito de claves. [CESID:1997]

2.972.3 (EN) SKIPJACK

(N) A type 2, 64-bit block cipher [SKIP, R2773] with a key size of 80 bits. (See: CAPSTONE, CLIPPER, FORTEZZA, Key Exchange Algorithm.) [RFC4949:2007]

2.972.4 (EN) SKIPJACK (CIPHER)

Skipjack is a block cipher developed by the U.S. National Security Agency (NSA). Initially classified, it was originally intended for use in the controversial Clipper chip. Subsequently, the algorithm was declassified and now provides a unique insight into the cipher designs of a government intelligence agency.

http://en.wikipedia.org/wiki/Skipjack_%28cipher%29

2.973 SKIP - SIMPLE KEY MANAGEMENT FOR INTERNET PROTOCOLS

Acrónimos: SKIP

Ver:

- http://www.ietf.org/rfc/rfc2356
- *IPsec - IP security*
- *IKE - Internet Key Exchange*

2.973.1 SKIP - SIMPLE KEY MANAGEMENT FOR INTERNET PROTOCOLS

Protocolo que establece una clave de sesión entre dos equipos con conexión IP.

2.973.2 (EN) SIMPLE KEY MANAGEMENT FOR INTERNET PROTOCOLS (SKIP)

(I) A key-distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets. (See: SKIP reference in [R2356].) [RFC4949:2007]

2.974 SMURF

2.974.1 ATAQUE SMURF

es un ataque de denegación de servicio que utiliza mensajes de ping al broadcast con spoofing para inundar (flood) un objetivo (sistema atacado).

http://es.wikipedia.org/wiki/Smurf_ataque

2.974.2 (EN) SMURF

The Smurf attack works by spoofing the target address and sending a ping to the broadcast address for a remote network, which results in a large amount of ping replies being sent to the target.

http://www.sans.org/security-resources/glossary-of-terms/

2.974.3 (FR) SMURFING

Technique de piratage causant un Denial of Service d'une machine. Le smurfing consiste à usurper l'adresse IP de la cible et à émettre en son nom de nombreux paquets ICMP EchoRequest vers l'adresse broadcast d'un réseau constitué d'un grand nombre d'ordinateurs. Tous les ordinateurs du réseau répondront alors avec un paquet ICMP EchoReply à l'adresse source usurpée précédemment provoquant ainsi un déni de service de la machine cible lors de la réception des paquets non-sollicités.

http://www.cases.public.lu/functions/glossaire/

2.975 SNEAKERNET

Ver:

- *Air gap*
- http://en.wikipedia.org/wiki/Sneakernet

2.975.1 SNEAKERNET

SneakerNet es el término usado (generalmente con intento irónico) para la transferencia de la información electrónica (fichero electrónico) por los medios desprendibles físicamente que llevan (cinta magnética, disquetes, discos compactos) a partir de un ordenador personal a otro. Esto está

generalmente en lugar de la traslación de la información sobre una red de computadoras debido a las limitaciones del ancho de banda, por motivos de seguridad (para asegurar que el receptor reciba la información de manera íntegra y exclusiva) o simplemente de la carencia de una red.

http://es.wikipedia.org/wiki/Sneakernet

2.975.2 (EN) SNEAKERNET

Sneakernet is an informal term describing the transfer of electronic information, especially computer files, by physically moving removable media such as magnetic tape, floppy disks, compact discs, USB flash drives (thumb drives, USB stick), or external hard drives from one computer to another. This is usually in lieu of transferring the information over a computer network. The name is a tongue-in-cheek sound-alike to Ethernet, and refers to the use of someone wearing sneakers as the transport mechanism for the data.

Sneakernet, whether called that or not, is often used as an academic example to illustrate long ping times, and the trade-off between latency and bandwidth.

http://en.wikipedia.org/wiki/Sneakernet

2.975.3 (EN) SNEAKER NET

(D) /slang/ A process that transfers data between systems only manually, under human control; i.e., a data transfer process that involves an air gap.

[RFC4949:2007]

2.976 SNEFRU

Ver:

- *Hash*

2.976.1 SNEFRU

Algoritmo para calcular resúmenes criptográficos. Produce resúmenes de 128 o 512 bits.

Fue diseñada en Xerox Corporation por Ralph C. Merkle.

2.976.2 (EN) SNEFRU

(N) A public-domain, cryptographic hash function (a.k.a. "The Xerox Secure Hash Function") designed by Ralph C. Merkle at Xerox Corporation. Snefru can produce either a 128-bit or 256-bit output (i.e., hash result). [Schn] (See: Khafre, Khufu.) [RFC4949:2007]

2.977 SNIFFER

Ver:

- *Interceptación de contraseñas*
- *Monitorización de la red*

2.977.1 MONITOR DE RED

Programas que monitorizan la información que circula por la red con el objeto de capturar información. Las placas de red tienen un sistema de verificación de direcciones mediante el cual saben si la información que pasa por ella está dirigida o no a su sistema. Si no es así, la rechaza. Un Sniffer consiste en colocar a la placa de red en un modo llamado promiscuo, el cual desactiva el filtro de verificación de direcciones y por lo tanto todos los paquetes enviados a la red llegan a esta placa (computadora donde está instalado el Sniffer). Existen Sniffers para capturar cualquier tipo de información específica. Por ejemplo contraseñas de acceso a cuentas, aprovechándose de que generalmente no son cifradas por el usuario. También son utilizados para capturar números de tarjetas de crédito o direcciones de correo. El análisis de tráfico puede ser utilizado también para determinar relaciones entre varios usuarios (conocer con qué usuarios o sistemas se relaciona alguien en concreto). Los buenos Sniffers no se pueden detectar, aunque la inmensa mayoría, y debido a que están demasiado relacionados con el protocolo TCP/IP, si pueden ser detectados con algunos trucos.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.977.1 SNIFFER

Programa de captura de paquetes de red. Literalmente, "husmeador". [CCN-STIC-435:2006]

2.977.2 (EN) SNIFFER:

Software used to observe and record network traffic.

The Tallinn Manual, 2013

2.977.3 (EN) SNIFFER

See packet sniffer or passive wiretapping. [CNSSI_4009:2010]

2.977.4 (EN) PACKET SNIFFER

Software that observes and records network traffic. [CNSSI_4009:2010]

2.977.5 (EN) SNIFFING

(D) /slang/ Synonym for "passive wiretapping"; most often refers to capturing and examining the data packets carried on a LAN. (See: password sniffing.) [RFC4949:2007]

2.977.6 (EN) SNIFFER

A sniffer is a tool that monitors network traffic as it received in a network interface.

http://www.sans.org/security-resources/glossary-of-terms/

2.977.7 (EN) SNIFFING

A synonym for "passive wiretapping."

http://www.sans.org/security-resources/glossary-of-terms/

2.977.8 (EN) SNIFFING

The interception of data packets traversing a network.

http://www.utexas.edu/its/policies/glossary.html

2.977.9 (EN) SNIFFING

An attacker monitors information transmitted between logical or physical nodes of a network. The attacker need not be able to prevent reception or change content but must simply be able to observe and read the traffic. The attacker might precipitate or indirectly influence the content of the observed transaction, but the attacker is never the intended recipient of the information. Any transmission medium can theoretically be sniffed if the attacker can listen to the contents between the sender and recipient.

Attack Pattern 157

http://capec.mitre.org/data/index.html

2.977.10 (FR) RENIFLEUR

Sonde logicielle destinée à analyser et à capturer le trafic sur un réseau. Les pirates utilisent ce type d'outils afin de récupérer à l'insu des utilisateurs et des administrateurs réseaux des informations sensibles et confidentielles qui traversent les réseaux telles que les couples identifiants/passwords. Le sniffing est un processus de collecte d'information dit passif puisque le pirate n'entre pas en communication directe avec les machines dont il renifle et voit passer les données.

http://www.cases.public.lu/functions/glossaire/

2.978 SOLICITANTE

2.978.1 SOLICITANTE

Entidad (organización, individuo, etc.) que solicita la asignación de una entrada identificada.

2.978.2 (EN) APPLICANT

an entity (organisation, individual etc.) which requests the assignment of a register entry and entry label [ISO-15292:2001]

2.979 SOLICITANTE DEL SELLO DE TIEMPO

Ver:

- *Sello de tiempo*

2.979.1 SOLICITANTE DEL SELLO DE TIEMPO

entidad que tiene unos datos para los que desea un sello de tiempo [traducción de ISO/IEC 18014-1]

2.979.2 (EN) TIME-STAMP REQUESTER

entity which possesses data it wants to be time-stamped [ISO-18014-1:2002]

2.980 SOPORTE

Ver:

- *Terminación de soportes de información*

2.980.1 SOPORTE

Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

2.980.2 (EN) MEDIA

Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, LSI memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. [CNSSI_4009:2010]

2.980.3 (EN) MEDIA

Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. [NIST-SP800-53:2013] [FIPS-200:2006]

2.980.4 (EN) MEDIUM

Material on which data are or may be recorded, such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs. [NIST-SP800-88:2006]

2.980.5 (EN) MEDIA

Physical device that may store information.

2.981 SOX SARBANES-OXLEY ACT

Acrónimos: SOX

2.981.1 LEY SARBANES-OXLEY (LEY SOX)

En Julio 2002, el Congreso de los Estados Unidos de Norteamérica aprobó la ley Sarbanes-Oxley (Ley SOX). Su objetivo principal fue devolver a los inversionistas la confianza en los mercados de capitales después de los muy publicitados casos de bancarrota que puso a los ejecutivos, comités de auditoria y auditores independientes en tela de juicio.

En junio de 2003 la SEC aprobó las reglas de implementación de la Sección 404 de la Ley, requiriendo a los auditores independientes de compañías públicas evaluar y reportar sobre la eficiencia de los controles internos en la generación de los reportes financieros de la compañía.

http://www.seguridadinformatica.cl/docs/leysarbanes.html

2.981.2 (EN) SOX

The Sarbanes-Oxley Act of 2002 (often shortened to SOX) is legislation enacted in response to the high-profile Enron and WorldCom financial scandals to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise. The act is administered by the Securities and Exchange Commission (SEC), which sets deadlines for compliance and publishes rules on requirements. Sarbanes-Oxley is not a set of business practices and does not specify how a business should store records; rather, it defines which records are to be stored and for how long.

http://whatis.techtarget.com/

2.981.3 (EN) SOX

Administered by the Securities and Exchange Commission (SEC) in 2002, Sarbanes-Oxley regulates corporate financial records and provides penalties for their abuse. It defines the type of records that must be recorded and for how long. It also deals with falsification of data. Affecting data storage capacities and planning, Sarbanes-Oxley was enacted after the Enron and WorldCom scandals of the early 2000s. The bill was sponsored by Paul Sarbanes, Democratic Senator from Maryland and additionally authored before passage by Michael Oxley, Republican Senator from Ohio.

http://www.spectralogic.com/index.cfm?fuseaction=home.displayFile&DocID=1235

2.982 SPAM

Ver:

- http://www.ietf.org/rfc/rfc2635
- *Anti-spam*
- http://en.wikipedia.org/wiki/Spamming
- *Opt in*
- *Opt out*
- *Botnet*

2.982.1 SPAM

Se denomina ’spam’ a todo correo no deseado recibido por el destinatario, procedente de un envío automatizado y masivo por parte del emisor. El ’spam’ generalmente se asocia al correo electrónico personal, pero no sólo afecta a los correos electrónicos personales, sino también a foros, blogs y grupos de noticias.

http://www.inteco.es/glossary/Formacion/Glosario/

2.982.2 CORREO BASURA

Correo electrónico no deseado que se envía aleatoriamente en procesos por lotes. Es una extremadamente eficiente y barata forma de comercializar cualquier producto. La mayoría de usuarios están expuestos a este correo basura que se confirma en encuestas que muestran que más del 50% de todos los e-mails son correos basura. No es una amenaza directa, pero la cantidad de e-mails generados y el tiempo que lleva a las empresas y particulares relacionarlo y eliminarlo, representa un elemento molesto para los usuarios de Internet.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.982.3 (EN) SPAM

The use of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately. The most widely recognised form of spam is email spam. [CSS NZ:2011]

2.982.4 (EN) SPAM

The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. [NIST-SP800-53:2013]

2.982.5 (EN) SPAM

Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. [CNSSI_4009:2010]

2.982.6 (EN) SPAM

1a. (I) /slang verb/ To indiscriminately send unsolicited, unwanted, irrelevant, or inappropriate messages, especially commercial advertising in mass quantities.

1b. (I) /slang noun/ Electronic "junk mail". [R2635]

[RFC4949:2007]

2.982.7 (EN) SPAMMING

the sending of bulk unsolicited messages which on receipt cause adverse effects on the availability of information system resources. [ISO-18028-1:2006]

2.982.8 (EN) SPAM

Slang used for describing unsolicited commercial e-mail.

http://iab.com/

2.982.9 (EN) SPAM

Electronic junk mail or junk newsgroup postings.

http://www.sans.org/security-resources/glossary-of-terms/

2.982.10 (EN) SPAMMING

A denial-of-service attack when sending unauthorized data in excess to a system. A special case is media spamming when sending RTP packets on UDP ports. Usually the system is flooded with packets; the processing consumes precious system resources. [H.235:2005]

2.982.11 (EN) SPAM

Unsolicited email that the recipient typically does not want to receive. The spam can be either benign or a form of malware.

http://www.enisa.europa.eu/

2.982.12 (EN) SPAM

Unsolicited commercial e-mail. Also known as junk e-mail.

http://www.getsafeonline.org/

2.982.13 (FR) SPAM

Courrier électronique non sollicité envoyé en masse à de très nombreuses destinataires. Le spam est souvent à caractère publicitaire.

http://www.cases.public.lu/functions/glossaire/

2.982.14 (FR) SPAM

Message intempestif envoyé à une personne ou à un groupe de personnes lors d'une opération de spamming. Il faut prendre l'habitude de supprimer ce genre de messages sans les lire et sans cliquer sur aucun lien (y compris le lien de désabonnement), afin de ne pas encourager cette pratique et ne pas en recevoir soi-même davantage. Spam est également couramment employé pour désigner le seul polluriel (email spam).

http://www.secuser.com/glossaire/

2.982.15 (FR) SPAMMING

Usage abusif d'un système de messagerie électronique ou de traitement automatisé de données destiné à exposer délibérément et généralement de manière répétée tout ou partie de ses utilisateurs à des messages ou à des contenus non pertinents et non sollicités couramment appelés "spams", en faisant en sorte de les confondre avec les messages ou les contenus habituellement échangés ou recherchés par ces utilisateurs. Le spamming s'accompagne souvent de la part du spammer d'une ou plusieurs pratiques généralement reconnues comme illégales au niveau mondial (usurpation d'identité, collecte déloyale de données personnelles, contrefaçon de marque, escroquerie, entrave volontaire à un système,...), mais ces pratiques sont à considérer comme des circonstances aggravantes et non des caractéristiques intrinsèques du spamming. Sont par exemple considérés comme des actes de spamming le fait d'envoyer un courriel à un inconnu pour lui demander de visiter un site ou d'acheter un produit, ou encore le fait de poster dans un forum des messages sans rapport avec le thème abordé.

http://www.secuser.com/glossaire/

2.983 SPEAR PHISHING

Ver

- *Phishing*

2.983.1 SPEAR PHISHING

Phishing dirigido de forma que se maximiza la probabilidad de que el sujeto objeto del ataque pique el anzuelo.

2.983.2 (EN) SPEAR PHISHING

An attack where social engineering techniques are used to masquerade as a trusted party to obtain important information such as passwords from the victim

ISACA, Cybersecurity Glossary, 2014

2.983.3 (EN) SPEAR PHISHING

Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information.

As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.

http://searchsecurity.techtarget.com/

2.983.4 (EN) SPEAR PHISHING:

A targeted phishing attempt that seems more credible to its victims and thus has a higher probability of success. For example, a spear phishing e-mail may spoof an organization or individual that the recipient actually knows.

Cybersecurity for Dummies, Palo Alto Networks Edition, 2014

2.984 SPKI - SIMPLE PUBLIC KEY INFRASTRUCTURE

Acrónimos: SPKI

Ver:

- http://www.ietf.org/rfc/rfc2692
- http://www.ietf.org/rfc/rfc2693
- *Infraestructura de clave pública*

2.984.1 SPKI - SIMPLE PUBLIC KEY INFRASTRUCTURE

Sistema de gestión de claves públicas que es alternativo al clásico X.509.

2.984.2 (EN) SIMPLE PUBLIC KEY INFRASTRUCTURE (SPKI)

(I) A set of experimental concepts (RFCs 2692, 2693) that were proposed as alternatives to the concepts standardized in PKIX. [RFC4949:2007]

2.985 SPYWARE

Ver:

- *Código dañino*
- *Anti-spyware*
- http://en.wikipedia.org/wiki/Spyware
- http://www.cert.org/archive/pdf/spyware2005.pdf

2.985.1 SPYWARE

Tipo de software malicioso que al instalarse intercepta o toma control parcial de la computadora del usuario sin el consentimiento de este último.

http://es.pcisecuritystandards.org

2.985.2 SPYWARE

Cualquier forma de tecnología que se usa para recoger información sobre una persona o empresa, o información referente a equipos o a redes, sin su conocimiento o consentimiento. También puede venir implementado en su hardware. Puede capturar hábitos de navegación, mensajes de correo, contraseñas y datos bancarios para transmitirlos a otro destino en Internet. Al igual que los virus puede ser instalado al abrir un adjunto de correo infectado, pulsando en una ventana de publicidad o camuflado junto a otros programas que instalemos.

http://www.inteco.es/glossary/Formacion/Glosario/

2.985.3 SPYWARE

Código malicioso diseñado habitualmente para utilizar la estación del usuario infectado con objetivos comerciales o fraudulentos como puede ser mostrar publicidad o robo de información personal del usuario. [CCN-STIC-400:2006]

2.985.4 SOFTWARE ESPÍA

Cualquier forma de tecnología que se usa para recoger información sobre una persona o empresa, o información referente a equipos o a redes, sin su conocimiento o consentimiento. También puede venir implementado en su hardware. Puede capturar hábitos de navegación, mensajes de correo, contraseñas y datos bancarios para transmitirlos a otro destino en Internet. Al igual que los virus puede ser instalado al abrir un adjunto de correo infectado, pulsando en una ventana de publicidad o camuflado junto a otros programas que instalemos.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.985.1 (EN) SPYWARE

Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code. [NIST-SP800-53:2013]

2.985.2 (EN) SPYWARE

Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code. [CNSSI_4009:2010]

2.985.3 (EN) SPYWARE

(D) /slang/ Software that an intruder has installed surreptitiously on a networked computer to gather data from that computer and send it through the network to the intruder or some other interested party. (See: malicious logic, Trojan horse.) [RFC4949:2007]

2.985.4 (EN) SPYWARE

Malware intended to violate a users privacy. [NIST-SP800-83:2005]

2.985.5 (EN) SPYWARE DETECTION AND REMOVAL UTILITY

A program that monitors a computer to identify spyware and prevent or contain spyware incidents. [NIST-SP800-83:2005]

2.985.6 (EN) SPYWARE

Type of malicious software that when installed, intercepts or takes partial control of the user’s computer without the user’s consent.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.985.7 (EN) SPYWARE

Software that (usually covertly) monitors the use of a computer. A business might use spyware to capture every keystroke of an employee suspected of fraud; a malicious website might also attempt to install spyware on every browser that visits that site in order to keep track of its users and/or capture data from their computers.

http://www.csoonline.com/glossary/

2.985.8 (EN) SPYWARE

refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

In simpler terms, spyware is a type of program that watches what users do with their computer and then sends that information over the Internet. Spyware can collect many different types of information about a user. More benign programs can attempt to track what types of websites a user visits and send this information to an advertisement agency. More malicious versions can try to record what a user types to try to intercept passwords or credit card numbers. Yet other versions simply launch popup advertisements.

http://en.wikipedia.org/wiki/Spyware

2.985.9 (EN) SPYWARE

Unwanted software that secretly monitors a user's activity, scans for private information or gives outsiders control of a computer.

http://www.getsafeonline.org/

2.985.10 (EN) SPYWARE

Programs that have the ability to scan systems or monitor activity and relay information to other computers or locations in cyber-space. Among the information that may be actively or passively gathered and disseminated by Spyware: passwords, log-in details, account numbers, personal information, individual files or other personal documents. Spyware may also gather and distribute information related to the user's computer, applications running on the computer, Internet browser usage or other computing habits.

Spyware frequently attempts to remain unnoticed, either by actively hiding or by simply not making its presence on a system known to the user. Spyware can be downloaded from Web sites (typically in shareware or freeware), email messages, and instant messengers. Additionally, a user may unknowingly receive and/or trigger spyware by accepting an End User License Agreement from a software program linked to the spyware or from visiting a website that downloads the spyware with or without an End User License Agreement.

http://www.symantec.com/avcenter/refa.html

2.985.11 (FR) SPYWARE

Le logiciel espion est un type de logiciel malveillant qui, une fois installé, intercepte ou prend partiellement le contrôle d’un ordinateur à l’insu de son utilisateur.

http://fr.pcisecuritystandards.org/

2.985.12 (FR) SPYWARE

Programme ou un sous-programme conçu dans le but de collecter des données personnelles sur ses utilisateurs et de les envoyer à son concepteur ou à un tiers via Internet ou tout autre réseau informatique, sans avoir obtenu au préalable une autorisation explicite et éclairée desdits utilisateurs.

http://www.secuser.com/glossaire/

2.986 SRS

Acrónimos: SRS, SSRS, SISRS

Ver:

- *Declaración de Requisitos de Seguridad*

2.986.1 (EN) SRS - SECURITY REQUIREMENTS STATEMENT

It is the core document for system accreditation. It describes completely and thoroughly the security priciples that apply, and the security requirements to be implemented. Every aspect must be based on a previous risk analysis.

2.987 SSH - SECURE SHELL

Acrónimos: SSH

Ver:

- http://www.ssh.org/
- http://www.ietf.org/rfc/rfc4819
- http://www.ietf.org/rfc/rfc4254
- http://www.ietf.org/rfc/rfc4253
- http://www.ietf.org/rfc/rfc4252
- http://www.ietf.org/rfc/rfc4251

2.987.1 SSH

Nombre de un protocolo y del programa que lo implementa. Este protocolo sirve para acceder a máquinas remotas a través de una red, de forma similar a como se hace con "telnet" con la diferencia principal de que SSH usa técnicas de cifrado en el intercambio de información. [CCN-STIC-641:2006]

2.987.2 (EN) SECURE SHELL

SSH a protocol that provides secure remote login utilising an insecure network. SSH is proprietary but will become an IETF standard in the near future. SSH was originally developed by SSH Communications Security. [ISO-18028-4:2005]

2.987.3 (EN) SECURE SHELL (SSH)

A program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.

http://www.sans.org/security-resources/glossary-of-terms/

2.987.4 (FR) SSH

SSH est un protocole de communication sécurisé. Le protocole de connexion impose un échange de clé de chiffrement en début de connexion, ce qui permet ensuite à des machines de dialoguer de façon chiffrée et donc de protéger la confidentialité des informations.

http://www.cases.public.lu/functions/glossaire/

2.987.5 (FR) SSH - SECURE SHELL.

Secure Shell est un protocole de communication sécurisée permettant l'accès distant à des machines Unix (notamment pour les commandes telles que rlogin, rsh et rcp). SSH permet de pallier les faiblesses de sécurité des accès distants aux systèmes Unix (ex.: telnet, X11) en fournissant les services de sécurité essentiels: authentification du serveur, confidentialité des flux (notamment des mots de passe).

SSH repose sur la technique de cryptographie asymétrique RSA. SSH utilise les algorithmes symétrique IDEA (par défaut), Blowfish et DES pour la confidentialité des données.

http://securit.free.fr/glossaire.htm

2.988 SSL - SECURE SOCKETS LAYER

Acrónimos: SSL

Ver:

- *TLS - Transport Layer Security*
- http://wp.netscape.com/eng/ssl3/
- http:www.schneier.com/paper-ssl-revised.pdf

2.988.1 SSL

Acrónimo de “secure sockets layer” (capa de conexión segura). Norma industrial establecida que cifra el canal entre un explorador web y un servidor web para garantizar la privacidad y confiabilidad de los datos transferidos por este canal. Consulte TLS

http://es.pcisecuritystandards.org

2.988.2 SSL - SECURE SOCKETS LAYER

Canal privado virtual entre dos puertos IP. Opcionalmente, asegura la autenticidad de una o ambas partes y la confidencialidad de los datos transmitidos.

Es el predecesor de TLS.

2.988.3 (EN) SSL

Acronym for “Secure Sockets Layer.” Established industry standard that encrypts the channel between a web browser and web server to ensure the privacy and reliability of data transmitted over this channel. See TLS.

https://www.pcisecuritystandards.org/security_standards/glossary.php

Secure Socket Layer (SSL)

A protocol used for protecting private information during transmission via the Internet.

Note: SSL works by using a public key to encrypt data that's transferred over the SSL connection. Most web browsers support SSL and many web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with “https:” instead of “http:.”

[CNSSI_4009:2010]

2.988.4 (EN) SECURE SOCKETS LAYER (SSL)

(N) An Internet protocol (originally developed by Netscape Communications, Inc.) that uses connection-oriented end-to-end encryption to provide data confidentiality service and data integrity service for traffic between a client (often a web browser) and a server, and that can optionally provide peer entity authentication between the client and the server. (See: Transport Layer Security.) [RFC4949:2007]

2.988.5 (EN) SECURE SOCKETS LAYER

SSL a protocol located between the network layer and the application layer provides authentication of clients and server and integrity and confidentiality services. SSL was developed by Netscape and builds the basis for TLS. [ISO-18028-4:2005]

2.988.6 (EN) SECURE SOCKETS LAYER (SSL)

A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection.

2.988.7 (FR) SSL

Acronyme de «Secure Sockets Layer», protocole SSL. Norme établie du secteur, cryptant le canal entre un navigateur et un serveur Web, afin de garantir la confidentialité et la fiabilité des données transmises sur ce canal. Voir TLS.

http://fr.pcisecuritystandards.org/

2.988.8 (FR) SSL (SECURE SOCKET LAYER)

Protocole de sécurité introduit par Netscape en 1995 permettant d'authentifier et de chiffrer une connexion entre un client et le serveur. SSL est le protocole de sécurité mis en place pour sécuriser les connexions HTTP en HTTPS.

http://www.cases.public.lu/functions/glossaire/

2.988.9 (FR) SSL - SECURE SOCKET LAYER

SSL est un protocole de communication sécurisée fournissant des services de sécurité basés sur les techniques de cryptographie symétriques (DES, 3-DES, RCx) et asymétriques (RSA):

- Authentification (unidirectionnelle ou mutuelle).
- Confidentialité des données.
- Intégrité des données.

SSL a été développé par Netscape (1ère version testée en interne, version 2.0 publiée en 1994, version actuelle 3.0 publié dans un draft IETF en 1996). SSL est en cours de standardisation par l'IETF sous le nom TLS (Transport Layer Security).

SSL est une couche supplémentaire au système OSI située entre la couche transport (TCP) et la couche des services applicatifs (niveau 7).

SSL est composé de deux niveaux:

- 1er niveau: protocole au dessus de TCP/IP: Record Layer Protocol.

- 2nd niveau: 3 sous-protocoles: Handshake protocol, Change cipher spe protocol, Alert protocol.

http://securit.free.fr/glossaire.htm

2.989 STUXNET

Ver

- *scada*

2.989.1 (EN) STUXNET:

A computer worm that was designed to target software and equipment comprising Siemens Corporation developed Supervisory Control and Data Acquisition (SCADA) systems. The payload of the Stuxnet malware included a programmable logic

The Tallinn Manual, 2013

2.989.2 (EN) STUXNET

An advanced cyber-attack against an industrial control system, consisting of multiple zero-day exploits used for the delivery of malware that then targeted and infected specific industrial controls for the purposes of sabotaging an automated process. Stuxnet is widely regarded as the first cyber-attack to specifically target an industrial control system.[knapp:2014]

2.989.3 (EN) STUXNET

Stuxnet is a computer worm discovered in June 2010 that is believed to have been created by the United States and Israel to attack Iran's nuclear facilities. Stuxnet initially spreads via Microsoft Windows, and targets Siemens industrial control systems. While it is not the first time that hackers have targeted industrial systems, it is the first discovered malware that spies on and subverts industrial systems, and the first to include a programmable logic controller (PLC) rootkit.

http://en.wikipedia.org/wiki/Stuxnet

2.990 SUPERCIFRADO

2.990.1 CIFRADO PRODUCTO

Es el obtenido aplicando sucesivos algoritmos de cifra a partir del texto en claro. Cada algoritmo actúa sobre el texto cifrado obtenido por el algoritmo inmediato anterior. [Ribagorda:1997]

2.990.1 (EN) SUPERENCRYPTION

Process of encrypting encrypted information. Occurs when a message, encrypted off-line, is transmitted over a secured, on-line circuit, or when information encrypted by the originator is multiplexed onto a communications trunk, which is then bulk encrypted. [CNSSI_4009:2010]

2.990.2 (EN) SUPERENCRYPTION

(I) An encryption operation for which the plaintext input to be transformed is the ciphertext output of a previous encryption operation. (Compare: hybrid encryption.) [RFC4949:2007]

2.991 SUPERVISIÓN DE LA INTEGRIDAD DE ARCHIVOS

2.991.1 SUPERVISIÓN DE LA INTEGRIDAD DE ARCHIVOS

Técnica o tecnología utilizada para supervisar archivos o registros a fin de detectar si se modificaron. Si se modifican archivos o registros críticos, se debería enviar mensajes de alerta al personal de seguridad apropiado.

http://es.pcisecuritystandards.org/

2.991.2 (EN) FILE INTEGRITY MONITORING:

Technique or technology under which certain files or logs are monitored to detect if they are modified. When critical files or logs are modified, alerts should be sent to appropriate security personnel.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.991.3 (FR) CONTROLE DE L'INTEGRITE DES FICHIERS

Technique ou technologie selon laquelle certains fichiers ou journaux sont contrôlés afin de détecter une éventuelle modification. Lorsque des fichiers ou des journaux critiques sont modifiés, des alertes doivent être envoyées au personnel de sécurité approprié.

http://fr.pcisecuritystandards.org/

2.992 SUPLANTACIÓN

Ver:

- *Impostura*
- *Anti-spoof*

2.992.1 SUPLANTAR

Ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba.

DRAE. Diccionario de la Lengua Española.

2.992.2 SUPLANTACIÓN

(En inglés Spoofing) Técnica basada en la creación de tramas TCP/IP utilizando una dirección IP falseada; desde su equipo, un atacante simula la identidad de otra máquina de la red (que previamente ha obtenido por diversos métodos) para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del anfitrión suplantado.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.992.3 SPOOFING

En materia de seguridad de redes, el término spoofing es una técnica de suplantación de identidad a través de la Red, llevada a cabo por un intruso generalmente con usos de malware o de investigación. Los ataques de seguridad en las redes a través de técnicas de spoofing ponen en riesgo la privacidad de los usuarios que navegan por Internet, así como la integridad de sus datos.

De acuerdo a la tecnología utilizada se pueden diferenciar varios tipos de spoofing:

- IP spoofing: Consiste en la suplantación de la dirección IP de origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.
- ARP spoofing: Es la suplantación de identidad por falsificación de tabla ARP. Las tablas ARP (Address Resolution Protocol) son un protocolo de nivel de red que relaciona una dirección de hardware con la dirección IP del ordenador. Por lo tanto, al falsear la tabla ARP de la víctima, todo lo que ésta envíe, será direccionado al atacante.
- DNS spoofing: Es una suplantación de identidad por nombre de dominio, la cual consiste en una relación falsa entre IP y nombre de dominio.
- Web spoofing: Con esta técnica el atacante crea una falsa página web, muy similar a la que suele utilizar el afectado con el objetivo de obtener información de dicha víctima como contraseñas, información personal, datos facilitados, páginas que visita con frecuencia, perfil del usuario, etc.
- Mail spoofing: Suplantación de correo electrónico bien sea de personas o de entidades con el objetivo de llevar a cabo envío masivo de phising o spam.

http://www.inteco.es/glossary/Formacion/Glosario/Spoofing

2.992.4 (EN) SPOOFING

Impersonating a legitimate resource or user to gain unauthorized entry into an information system or to make it appear that some other organization or individual has initiated or undertaken certain cyber activity.

The Tallinn Manual, 2013

2.992.5 (EN) SPOOFING

1. Faking the sending address of a transmission to gain illegal entry into a secure system.

2. The deliberate inducement of a user or resource to take incorrect action.

Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing.

[CNSSI_4009:2010]

2.992.6 (EN) SPOOFING

impersonating a legitimate resource or user. [ISO-18028-1:2006]

2.992.7 (EN) SPOOF

Attempt by an unauthorized entity to gain access to a system by posing as an authorized user.

2.992.8 (EN) SPOOF

To make a transmission appear to come from a user other than the user who performed the action.

http://www.getsafeonline.org/

2.992.9 (EN) SPOOFING

For example forging email messages or scanning Internet packets to acquire a valid password, with which to hack into a computer.

http://www.getsafeonline.org/

2.992.10 (EN) CONTENT SPOOFING

An attack technique used to trick a user into thinking that fake web site content is legitimate data.

http://www.webappsec.org/projects/glossary/

2.992.11 (FR) SPOOFING

Méthode d'usurpation de l'identité d'une machine. Le spoofing peut porter sur l'usurpation de l'adresse IP, l'adresse MAC ou tout autre élément permettant d'identifier une machine sur un réseau, afin de pouvoir se faire passer pour la machine usurpée et agir soit en son nom pour atteindre des niveaux de privilèges et d'accès non autorisés autrement soit agir pour lui porter atteinte comme dans le cas d'attaques de type smurfing.

http://www.cases.public.lu/functions/glossaire/

2.993 SUPLANTACIÓN DE DNS

Ver:

- *Envenenamiento del DNS*
- *Pharming*
- *Secuestro de DNS*
- *Extensiones de seguridad para el DNS*

2.993.1 SUPLANTACIÓN DE DNS

Técnica de ataque contra un dominio Internet. El atacante logra que su servidor, fraudulento, responda a las peticiones de los clientes, engañando a estos últimos.

2.993.2 (EN) DNS SPOOFING

An attack technique where a hacker intercepts your system's requests to a DNS server in order to issue false responses as though they came from the real DNS server. Using this technique, an attacker can convince your system that an existing Web page does not exist, or respond to requests that should lead to a legitimate Web site, with the IP address of a malicious Web site. This differs

from DNS cache poisoning because in DNS spoofing, the attacker does not hack a DNS server; instead, he inserts himself between you and the server and impersonates the server.

http://www.watchguard.com/glossary/

2.994 SUPLANTACIÓN IP

Ver:

- *Spoof*

2.994.1 FALSIFICACIÓN DE DIRECCIÓN IP

Técnica de ataque utilizada para obtener acceso no autorizado a redes o computadoras. La persona malintencionada envía mensajes engañosos a una computadora. Los mensajes tienen una dirección IP que indica que el mensaje proviene de un host de confianza.

http://es.pcisecuritystandards.org

2.994.2 IP SPOOFING

Técnica de ataque en la que un usuario malintencionado toma la identidad de un host "confiable" (cambiando su dirección IP por la dirección de éste) y obtiene de este modo accesos no autorizados a otros sistemas. [CCN-STIC-641:2006]

2.994.3 IP SPOOFING

Técnica mediante la cual un atacante hace creer al servidor víctima del ataque que su IP de origen es diferente a la real. Normalmente, para conseguir acceso a zonas limitadas a determinadas IP. [CCN-STIC-612:2006] [CCN-STIC-671:2006]

2.994.4 (EN) IP ADDRESS SPOOFING:

Attack technique used by a malicious individual to gain unauthorized access to computers. The malicious individual sends deceptive messages to a computer with an IP address indicating that the message is coming from a trusted host.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.994.5 (EN) IP SPOOFING

The technique of supplying a false IP address.

http://www.sans.org/security-resources/glossary-of-terms/

2.994.6 (FR) USURPATION D'ADRESSE IP

Technique d'attaque utilisée pour obtenir un accès non autorisé à des réseaux ou des ordinateurs. L'individu malveillant envoie des messages trompeurs à un ordinateur avec une adresse IP indiquant que le message provient d'un hôte de confiance.

http://fr.pcisecuritystandards.org/

2.995 SUSTITUCIÓN

Ver:

- *Código*
- *Transposición*

2.995.1 SUSTITUCIÓN

Algoritmo criptográfico que reemplaza los símbolos (bits, caracteres o cadenas de éstos) del texto en claro por otros símbolos diferentes del mismo alfabeto u otro distinto. [Ribagorda:1997]

2.995.2 SUSTITUCIÓN HOMOFÓNICA (HOMOPHONIC SUBSTITUCION)

Método de sustitución consistente en el reemplazo de los caracteres del alfabeto del texto en claro por los caracteres (llamados homófonos de los anteriores) de otro alfabeto (alfabeto de homófonos) de cardinalidad mucho mayor que el primero. [Ribagorda:1997]

2.995.3 SUSTITUCIÓN MONOALFABETO (MONOALPHABETIC SUBTITUCION)

Método de sustitución que consta de un único alfabeto de cifrado que además coincide con el alfabeto en claro. [Ribagorda:1997]

2.995.4 SUSTITUCIÓN POLIALFABETO (POLYALPHABETIC SUBSTITUTION)

Método de sustitución que consta de varios alfabetos de cifrado, eligiéndose el adecuado a cada carácter en claro según la posición ocupada por éste en el texto en claro. [Ribagorda:1997]

2.995.5 SUSTITUCIÓN POLIGRÁMICA (POLYGRAMIC SUBSTITUTION)

Método de sustitución en el que los caracteres no se reemplazan uno a uno por otros sino por pares (llamados digramas o dígrafos), tríos (trigramas o trígrafos), etc., con lo cual se rompe el patrón de frecuencia de aparición de las letras aisladas de los lenguajes.

Ejemplos típicos de métodos de este tipo son los Playfair (en realidad ideado por Charles Wheatstone) y Hill (Lester S., Nueva York 1981-1961).

[Ribagorda:1997]

2.995.6 SUSTITUCIÓN

Sistema de cifrado que consiste en reemplazar los caracteres del texto claro por una representación distinta de la original.

Puede ser simple (de representación única cuando a cada carácter del claro le corresponde sólo un posible carácter en el criptograma y viceversa, o de representación múltiple si le pueden corresponder varios pero a cada uno del criptograma sólo uno del claro), o polialfabética (si a cada carácter del criptograma le pueden corresponder varios del claro y viceversa).

[CESID:1997]

2.995.7 (EN) SUBSTITUTION

1. (I) /cryptography/ A method of encryption in which elements of the plain text retain their sequential position but are replaced by elements of cipher text. (Compare: transposition.) [RFC4949:2007]

2.996 SYN FLOOD

Ver:

- *Inundación*
- *Denegación de servicio*

2.996.1 SYN FLOOD

Ataque de denegación de servicio realizando inundando de peticiones un servidor de conexiones TCP (SYN, de Synchronization) hasta la saturación. [CCN-STIC-611:2006] [CCN-STIC-614:2006]

2.996.2 TCP SYN ATTACK

Ataque por el que se inunda a un sistema de peticiones de conexión TCP, usualmente sin llegar a completarlas. Es un ataque de tipo DoS. [CCN-STIC-641:2006]

2.996.3 (EN) SYN FLOOD

(I) A denial-of-service attack that sends a large number of TCP SYN (synchronize) packets to a host with the intent of disrupting the operation of that host. (See: blind attack, flooding.) [RFC4949:2007]

2.996.4 (EN) SYN FLOOD

A denial of service attack that sends a host more TCP SYN packets (request to synchronize sequence numbers, used when opening a connection) than the protocol implementation can handle.

http://www.sans.org/security-resources/glossary-of-terms/

2.996.5 (EN) SYN FLOOD

SYN flooding is a method that the user of a hostile client program can use to conduct a denial-of-service (DOS) attack on a computer server. The hostile client repeatedly sends SYN (synchronization) packets to every port on the server, using fake IP addresses.

http://searchsoftwarequality.techtarget.com/glossary/

2.996.6 (FR) SYN FLOOD

Attaque ayant pour objectif le "Refus de Services" (DDoS) en inondant (flood) un serveur de demande de connexions TCP (SYN de synchronisation) jusqu'à sa saturation.

http://www.cases.public.lu/functions/glossaire/

2.997 TACACS - TERMINAL ACCESS CONTROLLER ACCESS CONTROL SYSTEM

Acrónimos: TACACS

Ver:

- *AAA - Autenticación, Autorización y Registro*
- *RADIUS - Remote Access Dial-In User Server*
- http://www.ietf.org/rfc/rfc1492

2.997.1 TACACS

Acrónimo de “terminal access controller access control system” (sistema de control de acceso del controlador de acceso aterminales). Protocolo de autenticación remoto que se utiliza generalmente en redes que se comunican entre un servidor de acceso remoto y un servidor de autenticación para determinar los derechos de acceso del usuario a la red. Este método de autenticación se puede utilizar con un token, tarjeta inteligente, etc., para proporcionar autenticación de dos factores.

http://es.pcisecuritystandards.org

2.997.2 TACACS

Protocolo estándar de AAA aunque en la práctica sólo es utilizado por todos los sistemas de control de accesos CISCO y compatibles. [CCN-STIC-641:2006]

2.997.3 (EN) TERMINAL ACCESS CONTROLLER (TAC) ACCESS CONTROL SYSTEM (TACACS)

(I) A UDP-based authentication and access control protocol [R1492] in which a network access server receives an identifier and password from a remote terminal and passes them to a separate authentication server for verification. (See: TACACS+.) [RFC4949:2007]

2.997.4 (EN) TACACS+

(I) A TCP-based protocol that improves on TACACS by separating the functions of authentication, authorization, and accounting and by encrypting all traffic between the network access server and authentication server. TACACS+ is extensible to allow any authentication mechanism to be used with TACACS+ clients. [RFC4949:2007]

2.997.5 (EN) TACACS

Acronym for “Terminal Access Controller Access Control System.” Remote authentication protocol commonly used in networks that communicates between a remote access server and an authentication server to determine user access rights to the network. This authentication method may be used with a token, smart card, etc., to provide two-factor authentication.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.997.6 (FR) TACACS

Acronyme de «Terminal Access Controller Access Control System», système de contrôle d’accès au contrôleur d’accès au terminal. Protocole d’authentification à distance, communément utilisé

dans les réseaux communiquant entre un serveur d'accès à distance et un serveur d'authentification, afin de déterminer les droits d'accès au réseau de l'utilisateur. Cette méthode d'authentification peut être utilisée avec un token, une carte à puce, etc., pour assurer une authentification à deux facteurs.

http://fr.pcisecuritystandards.org/

2.998 TARJETA CON CIRCUITOS INTEGRADOS

Acrónimos: ICC

Ver:

- *Tarjeta inteligente*

2.999 TARJETA INTELIGENTE

Ver:

- *Tarjeta con circuitos integrados*
- *Token criptográfico*

2.999.1 TARJETA INTELIGENTE

Dispositivo criptográfico de las dimensiones de una tarjeta de crédito. Contiene un microprocesador que realiza operaciones sobre datos almacenados internamente o proporcionados a través de la interfaz con el exterior.

Típicamente se usan para proporcionar servicios criptográficos tales como autenticación o cifrado de datos.

2.999.2 (EN) SMART CARD

(I) A credit-card sized device containing one or more integrated circuit chips that perform the functions of a computer's central processor, memory, and input/output interface. (See: PC card, smart token.)

Usage: Sometimes this term is used rather strictly to mean a card that closely conforms to the dimensions and appearance of the kind of plastic credit card issued by banks and merchants. At other times, the term is used loosely to include cards that are larger than credit cards, especially cards that are thicker, such as PC cards.

[RFC4949:2007]

2.999.3 (EN) SMART TOKEN

(I) A device that conforms to the definition of "smart card" except that rather than having the standard dimensions of a credit card, the token is packaged in some other form, such as a military dog tag or a door key. (See: smart card, cryptographic token.) [RFC4949:2007]

2.999.4 (FR) CARTE À PUCE

On définit la carte à puce de manière générale comme "un ordinateur personnel de la taille d'une carte de crédit" (Simon Davies). Il s'agit d'une carte disposant de moyens intelligents dont le but est de mettre en oeuvre des calculs cryptographiques permettant d'assurer les services de sécurité suivants: authentification, confidentialité, intégrité et preuve.

http://securit.free.fr/glossaire.htm

2.1000 TCSEC - TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

Acrónimos: TCSEC

Ver:

- *Criterios comunes*
- *ITSEC - Information Technology Security Evaluation Criteria*
- http://en.wikipedia.org/wiki/TCSEC

2.1000.1 TCSEC

Los TCSEC tiene por objetivo aplicar la política de seguridad del Departamento de Defensa estadounidense. Esta política se preocupa fundamentalmente del mantenimiento de la confidencialidad de la información clasificada a nivel nacional.

Los TCSEC definen siete conjuntos de criterios de evaluación denominados clases (D, C1, C2, B1, B2, B3 y A1). Cada clase de criterios cubre cuatro aspectos de la evaluación: política de seguridad, imputabilidad, aseguramiento y documentación. Los criterios correspondientes a estas cuatro áreas van ganando en detalle de una clase a otra, constituyendo una jerarquía en la que D es el nivel más bajo y A1 él más elevado. Todas las clases incluyen requisitos tanto de funcionalidad como de confianza.

A continuación se enumeran las siete clases:

- D Protección mínima. Sin seguridad.
- C1 Limitaciones de accesos a datos.
- C2 Acceso controlado al SI. Archivos de log y de auditoría del sistema.
- B1 Equivalente al nivel C2 pero con una mayor protección individual para cada fichero.
- B2 Los sistemas deben estar diseñados para ser resistentes al acceso de personas no autorizadas.
- B3 Dominios de seguridad. Los sistemas deben estar diseñados para ser altamente resistentes a la entrada de personas no autorizadas.
- A1 Protección verificada. En la práctica, es lo mismo que el nivel B3, pero la seguridad debe estar definida en la fase de análisis del sistema.

El Libro Naranja fue desarrollado por el NCSC (National Computer Security Center) de la NSA (National Security Agency) del Departamento de Defensa de EEUU. Actualmente, la responsabilidad sobre la seguridad de SI la ostenta un organismo civil, el NIST (National Institute of Standards and Technology).

http://www.csi.map.es/csi/silice/Segurd21.html

2.1000.2 TCSEC - TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

Criterios de evaluación de la seguridad de los sistemas de computación, conocidos también con el nombre de Orange Book (Libro naranja), definidos originalmente por el Ministerio de Defensa de los EE.UU.

http://www.iso27000.es/glosario.html

2.1000.3 (EN) DOD TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (TCSEC)

A document published by the National Computer Security Center containing a uniform set of basic requirements and evaluation classes for assessing degrees of assurance in the effectiveness of hardware and software security controls built into systems. These criteria are intended for use in the design and evaluation of systems that will process and/or store classified or Sensitive Unclassified data.

This document is Government Standard DoD 5200.28-STD and is frequently referred to as "The Criteria" or "The Orange Book."

[IRM-5239-8:1995]

2.1000.4 (EN) TCSEC

Trusted Computer System Evaluation Criteria (TCSEC) is a set of basic requirements for assessing the effectiveness of computer security controls built into a computer system which was evaluated for use by the United States Department of Defense (DoD). The TCSEC was used to classify and select computer systems being considered for the processing, storage and retrieval of sensitive or classified information. The TCSEC, frequently referred to as the Orange Book is the centerpiece of the DoD Rainbow Series publications. Initially issued by the National Computer Security Center (NCSC) an arm of the National Security Agency in 1983 and then updated in 1985, TCSEC was replaced with the development of the Common Criteria international standard originally published in 2005.

http://en.wikipedia.org/wiki/TCSEC

2.1001 TEARDROP

Ver:

- *Denegación de servicio*
- *Ataque*
- *Ping mortal*

2.1001.1 TEARDROP

Ataque de denegación de servicio. Consiste en enviar paquetes IP o fragmentos de paquetes IP que están indebidamente construidos. El propósito es provocar un fallo en el equipo destino.

2.1001.2 (EN) TEARDROP ATTACK

(D) /slang/ A denial-of-service attack that sends improperly formed IP packet fragments with the intent of causing the destination system to fail. [RFC4949:2007]

2.1002 TÉCNICAS AVANZADAS DE EVASIÓN

Acrónimos: AET

2.1002.1 TÉCNICAS AVAZANZADAS DE EVASIÓN

Se denomina técnicas de evasión avanzadas a la combinación de diferentes técnicas de evasión utilizando diferentes niveles de la red. El resultado dificulta enormemente la capacidad de detección del ataque.

2.1002.2 (EN) ADVANCED EVASION TECHNIQUE (AET)

An advanced evasion technique (AET) is a type of network attack that combines several different known evasion methods to create a new technique that's delivered over several layers of the network simultaneously. The code in the AET itself is not necessarily malicious; the danger is that it provides the attacker with undetectable access to the network.

http://searchsecurity.techtarget.com/

2.1003 TÉCNICA CRIPTOGRÁFICA ASIMÉTRICA

Ver:

- *Sistema de cifra asimétrica*
- *Sistema de firma asimétrica*
- *Criptografía de clave pública*
- *Par asimétrico de claves*

2.1003.1 TÉCNICAS CRIPTOGRÁFICAS ASIMÉTRICAS

Aquellas que usan dos algoritmos criptográficos, uno inverso del otro. De ellos, uno es de público conocimiento (determinado por la clave pública) y otro privado (determinado por la clave privada). Los dos algoritmos tienen la propiedad de que dado una de ellos es computacionalmente inviable obtener el otro. [ISO-11770-3:2008] [Ribagorda:1997]

2.1003.2 TÉCNICA CRIPTOGRÁFICA ASIMÉTRICA

1. Algoritmo de cifra basado en una función irreversible con trampa. Este algoritmo y su inverso dependen de dos claves diferentes, denominadas pública y privada, tales que el conocimiento de una no conduce a la otra. Tanto el algoritmo como su inverso, cada uno con su clave correspondiente, puede ser empleado para cifrar, descifrándose con el contrario.

2. Cifrado obtenido mediante técnicas criptográficas asimétricas.

[Ribagorda:1997]

2.1003.3 (EN) ASYMMETRIC CRYPTOGRAPHIC TECHNIQUE

a cryptographic technique that uses two related transformations; a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation in a given limited time and computing power. [ISO-19790:2006]

2.1003.4 (EN) ASYMMETRIC CRYPTOGRAPHIC TECHNIQUE

cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation [ISO/IEC ISO-11770-1:1996]. [ISO-18033-1:2005]

2.1003.5 (EN) ASYMMETRIC CRYPTOGRAPHIC TECHNIQUE

Cryptographic technique that uses two related operations: a public operation defined by a public data item, key or number, and a private operation defined by a private data item, key or number (the two operations have the property that, given the public operation, it is computationally infeasible to derive the private operation). [ISO-9798-5:2004]

2.1003.6 (EN) ASYMMETRIC CRYPTOGRAPHIC TECHNIQUE

A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation. [ISO-11770-3:2008]

2.1003.7 (EN) ASYMMETRIC CRYPTOGRAPHY TECHNIQUE

A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation.

NOTE. A system based on asymmetric cryptographic techniques can either be an encipherment system, a signature system, a combined encipherment and signature system, or a key agreement system. With asymmetric cryptographic techniques there are four elementary transformations: sign and verify for signature systems, encipher and decipher for encipherment systems. The signature and decipherment transformation are kept private by the owning entity, whereas the corresponding verification and encipherment transformation are published. There exist asymmetric cryptosystems (e.g. RSA) where the four elementary functions may be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one public transformation suffices for both verifying and encrypting messages.

However, since this is not the general case, throughout ISO/IEC ISO-9798 the four elementary transformations and the corresponding keys are kept separate.

[ISO-9798-1:1997]

2.1003.8 (FR) CHIFFREMENT ASYMÉTRIQUE

Technique de chiffrement, parfois dénommé chiffrement à clé publique, utilisant une paire de clés différentes, une clé privée et une clé publique, pour chiffrer et déchiffrer les données. Des propriétés mathématiques liant la clé publique et la clé privée permettent de garantir que les messages chiffrés avec une des deux clés ne peuvent être déchiffrés qu'avec l'autre clé de la paire. Ces propriétés mathématiques assurent de plus que la clé utilisée pour chiffrer n'est pas en mesure de déchiffrer ce qui vient d'être chiffré. Les deux clés, publiques et privées, qui constituent la paire

de clés sont donc intimement liées entre elles. La clé privée ne doit être uniquement connue que de son propriétaire, la clé publique est quant à elle vouée à être transmise publiquement à toute personne afin de permettre à quiconque de communiquer de manière confidentielle avec le propriétaire de la clé publique qui possède la clé privée liée à cette clé publique. La garantie du lien entre la clé publique et son propriétaire se fait à l'aide d'un certificat électronique.

http://www.cases.public.lu/functions/glossaire/

2.1004 TÉCNICA CRIPTOGRÁFICA SIMÉTRICA

Ver:

- *Cifrado*
- *Descifrado*
- *Criptografía de clave secreta*
- *Algoritmo criptográfico simétrico*

2.1004.1 TÉCNICA CRIPTOGRÁFICA SIMÉTRICA

Técnica criptográfica donde se usa la misma clave secreta para cifrar y para descifrar. Sin el conocimiento de la clave es [computacionalmente] imposible tanto cifrar como descifrar.

2.1004.2 (EN) SYMMETRIC CRYPTOGRAPHIC TECHNIQUE

cryptographic technique that uses the same secret key for both the encryption and the decryption transformations [ISO-19790:2006]

2.1004.3 (EN) SYMMETRIC CRYPTOGRAPHIC TECHNIQUE

cryptographic technique that uses the same secret key for both the originators and the recipients transformation. Without knowledge of the secret key, it is computationally infeasible to compute either the originators or the recipients transformation.

NOTE. Examples of symmetric cryptographic techniques include symmetric ciphers and Message Authentication Codes (MACs). In a symmetric cipher, the same secret key is used to encrypt and decrypt data. In a MAC scheme, the same secret key is used to generate and verify MACs.

[ISO-18033-1:2005]

2.1004.4 (EN) SYMMETRIC CRYPTOGRAPHIC TECHNIQUE

A cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation.

NOTE. Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation.

[ISO-9798-1:1997]

2.1004.5 (EN) SYMMETRIC CRYPTOGRAPHIC TECHNIQUE

A cryptographic technique that uses the same secret key for both the originators and the recipients transformation. Without knowledge of the secret key, it is computationally infeasible to compute either the originators or the recipients transformation. [ISO-11770-1:1996]

2.1004.6 (FR) TECHNIQUE CRYPTOGRAPHIQUE SYMÉTRIQUE

Technique cryptographique qui utilise la même clé secrète pour la transformation cryptographique de l'émetteur ou du destinataire. Sans connaissance de la clé secrète, il est impossible de calculer la transformation cryptographique de l'émetteur ou du destinataire. [ISO-11770-1:1996]

2.1005 TEMPEST

Acrónimos: TEMPEST

Ver:

- *Seguridad*
- *Seguridad de las emanaciones*
- *Emanaciones*
- *Emanaciones comprometedoras*

2.1005.1 TEMPEST

Término que hace referencia a las investigaciones y estudios de emanaciones comprometedoras (emisiones electromagnéticas no intencionadas, producidas por equipos eléctricos y electrónicos que, detectadas y analizadas, puedan llevar a la obtención de información) y a las medidas aplicadas a la protección contra dichas emanaciones. [CCN-STIC-150:2006]

2.1005.2 CERTIFICACIÓN TEMPEST

Certificación que se otorga a aquellos equipos físicos (básicamente terminales e impresoras) cuya emisión de radiaciones electromagnéticas se mantiene por debajo de un umbral que las hace indetectables incluso a corta distancia. [Ribagorda:1997]

2.1005.3 (EN) TEMPEST

A name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment. [CNSSI_4009:2010]

2.1005.4 (EN) TEMPEST ZONE

Designated area within a facility where equipment with appropriate TEMPEST characteristics (TEMPEST zone assignment) may be operated. [CNSSI_4009:2010]

2.1005.5 (EN) TEMPEST

1. (N) Short name for technology and methods for protecting against data compromise due to electromagnetic emanations from electrical and electronic equipment. [Army, Russ] (See: inspectable space, soft TEMPEST, TEMPEST zone. Compare: QUADRANT)

2. (O) /U.S. Government/ "Short name referring to investigation, study, and control of compromising emanations from IS equipment." [C4009]

[RFC4949:2007]

2.1005.6 (EN) TEMPEST

a name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment. [FIPS-140-2:2001]

2.1005.7 (EN) TEMPEST

The study and control of spurious electronic signals emitted from ADP equipment. [TCSEC:1985]

2.1006 TERCERA PARTE

Ver:

- *Tercera parte de confianza*

2.1006.1 TERCERO(S)

Una persona, grupo, o Negocio que no es parte del Acuerdo de Nivel de Servicio para un Servicio de TI, pero que es requerida para asegurar el éxito en la entrega de ese Servicio de TI. Por ejemplo, un Proveedor de software, una empresa de mantenimiento de hardware, o el departamento de .... Los requerimientos para los terceros están normalmente especificados en Contratos de Soporte o Acuerdos de Nivel Operacional. [ITIL:2007]

2.1006.2 (EN) THIRD PARTY

A person, group, or Business who is not part of the Service Level Agreement for an IT Service, but is required to ensure successful delivery of that IT Service. For example a software Supplier, a hardware maintenance company, or a facilities department. Requirements for Third Parties are typically specified in Underpinning Contracts or Operational Level Agreements. [ITIL:2007]

2.1006.3 (FR) TIERCE PARTIE

Une personne, un groupe ou un business qui ne fait pas partie de l'accord sur les niveaux de service d'un service des TI, mais est nécessaire pour assurer la fourniture réussie de ce service des TI. Par exemple un fournisseur de logiciels sous-traitant, une société de maintenance de matériel ou un département de l'équipement. Les exigences envers les tierces parties sont habituellement stipulées dans des contrats de sous-traitance ou des accords sur les niveaux opérationnels (OLA). [ITIL:2007]

2.1007 TERCERA PARTE DE CONFIANZA

Acrónimos: TTP

Ver:

- *Entidad de confianza*
- *Tercera parte*

- *Confianza*

2.1007.1 TERCERA PARTE FIABLE

Autoridad de seguridad, o agente suyo, confiable para otras entidades con respecto a actividades relativas a la seguridad. Una tercera parte fiable es de confianza para un demandante y/o verificador a efectos de autenticación (ISO/IEC ISO-9798-1).

A menudo se la conoce, informalmente, como Notario Electrónico.

[Ribagorda:1997]

2.1007.2 TERCERA PARTE CONFIABLE

Entidad que proporciona servicios y mecanismos de seguridad en los que las partes involucradas en un protocolo depositan su confianza, para la realización del protocolo y/o la resolución de conflictos relacionados con el mismo. [CESID:1997]

2.1007.3 TERCERA PARTE CONFIABLE

Autoridad de seguridad o su agente en la que se confía con respecto a algunas actividades pertinentes a la seguridad (en el contexto de una política de seguridad). [X.810:1995]

2.1007.4 (EN) TRUSTED THIRD PARTY

A security authority, or its agent, trusted by other entities with respect to security related activities (see ISO/IEC ISO-10181-1).

NOTE. In the context of this multipart International Standard, a trusted third party is trusted by the originator, the recipient, and/or the delivery authority for the purposes of non-repudiation, and by another party such as an adjudicator.

[ISO-13888-1:2004]

2.1007.5 (EN) TRUSTED THIRD PARTY (TTP)

A security authority, or its agent, trusted by other entities with respect to security related activities. [ISO-11770-3:2008]

2.1007.6 (EN) TRUSTED THIRD PARTY

a security authority or its agent, trusted by other entities with respect to security-related activities. In the context of ISO/IEC ISO-9798, a trusted third party is trusted by a claimant and/or a verifier for the purposes of authentication. [ISO-9798-1:1997]

2.1007.7 (EN) TRUSTED THIRD PARTY

security authority, or its agent, trusted by other entities with respect to security related activities. [ISO-10181-1:1996]

2.1007.8 (EN) TRUSTED THIRD PARTY

A security authority or its agent that is trusted with respect to some security-relevant activities (in the context of a security policy). [X.810:1995]

2.1007.9 (FR) TIERCE PARTIE DE CONFIANCE

autorité de sécurité ou son agent auquel il est fait confiance au regard de certaines activités liées à la sécurité (dans le contexte d'une politique de sécurité). [X.810:1995]

2.1008 TERCERO INTERPUESTO

Ver:

- *Ataque*

2.1008.1 MAN-IN-THE-MIDDLE

Técnica mediante la cual un tercero es capaz de interceptar, e incluso modificar, la comunicación entre dos extremos. [CCN-STIC-612:2006]

[CCN-STIC-671:2006]

2.1008.2 (EN) MAN-IN-THE-MIDDLE ATTACK (MITM)

An attack on the authentication protocol run in which the Attacker positions himself or herself in between the Claimant and Verifier so that he can intercept and alter data traveling between them. [NIST-SP800-63:2013]

2.1008.3 (EN) MAN-IN-THE-MIDDLE ATTACK (MITM)

A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association. [CNSSI_4009:2010]

2.1008.4 (EN) MAN-IN-THE-MIDDLE ATTACK

(I) A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association. (See: hijack attack, piggyback attack.) [RFC4949:2007]

2.1008.5 (EN) ACTIVE MAN-IN-THE-MIDDLE ATTACK (MITM)

Active man-in-the-middle (MitM) is an attack method that allows an intruder to access sensitive information by intercepting and altering communications between the user of a public network and any requested website.

http://searchsecurity.techtarget.in/

2.1008.6 (EN) MAN IN THE MIDDLE ATTACK

An attack where the message is intercepted and copied or modified before being transmitted to the intended recipient.

2.1008.7 (EN) MAN-IN-THE-MIDDLE

An attacker places a machine between the authorised user and the system under attack, captures the I&A transactions as they are sent over the communications line and subsequently resends them as his/her own.

2.1008.8 (EN) MAN-IN-THE-MIDDLE ATTACK

In phishing, refers to using a fraudulent website as an intermediary between the victim and the legitimate website. The victim enters his or her banking information into the fraudulent site and is then redirected to the legitimate site, with little or no indication that anything is amiss.

2.1008.9 (FR) MIDDLEPERSON (MAN IN THE MIDDLE)

Menace passive correspondant à une personne qui, au sein d'un réseau, capte des informations numériques échangées entre deux personnes. Le Man in the Middle peut également être assimilée à une menace active, le Man in the Middle peut intercepter les informations, les modifier avant de les transmettre aux destinataire(s) initial(s) de l'information. Dans les deux cas, le Man in the Middle est invisible pour les entités intervenant dans la communication.

http://www.cases.public.lu/functions/glossaire/

2.1009 TERMINACIÓN DE SOPORTES DE INFORMACIÓN

Ver:

- *Borrado*
- *Desmagnetizador*
- *Reutilización*
- *Soporte*

2.1009.1 TERMINACIÓN DE SOPORTES DE INFORMACIÓN

Eliminación deliberada, completa e irreversible de los contenidos de un sistema o un soporte de información. Se aplica cuando el soporte contiene o ha contenido información sensible.

2.1009.2 (EN) MEDIA SANITIZATION

The actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. [CNSSI_4009:2010]

2.1009.3 (EN) SANITIZATION

A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. [CNSSI_4009:2010]

2.1009.4 (EN) SANITIZE

1. (I) Delete sensitive data from a file, device, or system. (See: erase, zeroize.) 2. (I) Modify data so as to be able either (a) to completely declassify it or (b) to downgrade it to a lower security level. [RFC4949:2007]

2.1009.5 (EN) MEDIA SANITIZATION

A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. [NIST-SP800-53:2013] [NIST-SP800-88:2006]

2.1009.6 (EN) SANITIZE

Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs. [FIPS-200:2006] [NIST-SP800-88:2006]

2.1009.7 (EN) DISINTEGRATION

A physically destructive method of sanitizing media; the act of separating into component parts. [NIST-SP800-88:2006]

2.1009.8 (EN) INCINERATION

A physically destructive method of sanitizing media; the act of burning completely to ashes. [NIST-SP800-88:2006]

2.1009.9 (EN) MELTING

A physically destructive method of sanitizing media; to be changed from a solid to a liquid state generally by the application of heat. [NIST-SP800-88:2006]

2.1009.10 (EN) OVERWRITE

Writing patterns of data on top of the data stored on a magnetic medium. NSA has researched that one overwrite is good enough to sanitize most drives. See comments on clear/purge convergence. [NIST-SP800-88:2006]

2.1009.11 (EN) PHYSICAL DESTRUCTION

A sanitization method for optical media, such as CDs. [NIST-SP800-88:2006]

2.1009.12 (EN) PULVERIZATION

A physically destructive method of sanitizing media; the act of grinding to a powder or dust. [NIST-SP800-88:2006]

2.1009.13 (EN) SECURE ERASE

An overwrite technology using firmware based process to overwrite a hard drive. Is a drive command defined in the ANSI ATA and SCSI disk drive interface specifications, which runs inside

drive hardware. It completes in about 1/8 the time of 5220 block erasure. It was added to the ATA specification in part at CMRR request. For ATA drives manufactured after 2001 (Over 15 GB) have the Secure Erase command and successfully pass secure erase validation testing at CMRR. A standardized internal secure erase command also exists for SCSI drives, but it is optional and not currently implemented in SCSI drives tested by CMRR. SCSI drives are a small percentage of the worlds hard disk drives, and the command will be implemented when users demand it. [NIST-SP800-88:2006]

2.1009.14 (EN) SHRED

A method of sanitizing media; the act of cutting or tearing into small particles. [NIST-SP800-88:2006]

2.1010 TEXTO CIFRADO

Ver:

- *Criptograma*

2.1010.1 TEXTO CIFRADO

1. Datos ininteligibles producidos mediante cifrado (ISO-7498-2).

2. Datos que no pueden ser interpretados como la expresión de un lenguaje natural o artificial sin el uso de la criptografía.

Aunque usualmente se considera sinónimo de criptograma, este último pone el acento en la transmisión, mientras que texto cifrado enfatiza el simple resultado de cifrar sin ulterior preparación para la transmisión.

[Ribagorda:1997]

2.1010.2 TEXTO CIFRADO O CRIPTO

Texto resultante de aplicar un procedimiento de cifrado a un texto claro. [CESID:1997]

2.1010.1 (EN) CIPHER TEXT / CIPHERTEXT

Data in its encrypted form. [CNSSI_4009:2010]

2.1010.2 (EN) CIPHER TEXT

1. (I) /noun/ Data that has been transformed by encryption so that its semantic information content (i.e., its meaning) is no longer intelligible or directly available. (See: ciphertext. Compare: clear text, plain text.)

2. (O) "Data produced through the use of encipherment. The semantic content of the resulting data is not available." [ISO-7498-2]

[RFC4949:2007]

2.1010.3 (EN) CIPHERTEXT

Data in its encrypted form. [NIST-SP800-57:2007]

2.1010.4 (EN) CIPHERTEXT

data which has been transformed to hide its information content. [ISO/IEC ISO-9798-1:1997] [ISO-18033-2:2006] [ISO-18033-3:2005]

2.1010.5 (EN) CIPHERTEXT

Data which has been transformed to hide its information content. [ISO-9798-1:1997]

2.1010.6 (EN) CIPHERTEXT

Data produced through the use of encipherment. The semantic content of the resulting data is not available.

NOTE. Ciphertext may itself be input to encipherment, such that super-enciphered output is produced.

[ISO-7498-2:1989]

2.1011 TEXTO CIFRADO ELEGIDO DINÁMICAMENTE

Ver:

- *Ataques a la criptografía*
- *Criptoanálisis*

2.1011.1 TEXTO CIFRADO ELEGIDO DINÁMICAMENTE

Variante del ataque por "texto cifrado elegido" donde el atacante va eligiendo dinámicamente el texto.

2.1011.2 (EN) ADAPTIVE CHOSEN CIPHERTEXT

A version of the chosen-ciphertext attack where the cryptanalyst can choose ciphertexts dynamically. A cryptanalyst can mount an attack of this type in a scenario in which he or she has free use of a piece of decryption hardware, but is unable to extract the decryption key from it.

http://www.rsasecurity.com/rsalabs/faq

2.1012 TEXTO EN CLARO

2.1012.1 TEXTO EN CLARO

1. Datos inteligibles, que pueden ser leídos o procesados sin la aplicación de ningún descifrador (ISO-7498-2).

2. Datos interpretables como expresión de un lenguaje natural o artificial.

En general, el adjetivo "en claro" se predica de aquella información, de cualquier naturaleza, que no ha sido cifrada, o si lo ha sido se ha descifrado posteriormente.

Así, se habla de símbolos, caracteres, números, datos etc., en claro.

[Ribagorda:1997]

2.1012.2 TEXTO CLARO

Texto o señales con significado propio en el idioma o código público que se emplee en cada caso. [CESID:1997]

2.1012.3 TEXTO CLARO

Datos inteligibles, cuyo contenido semántico está disponible. [ISO-7498-2:1989]

2.1012.4 (EN) CLEAR TEXT

1. (I) /noun/ Data in which the semantic information content (i.e., the meaning) is intelligible or is directly available, i.e., not encrypted. (See: cleartext, in the clear. Compare: cipher text, plain text.)

2. (O) /noun/ "Intelligible data, the semantic content of which is available." [ISO-7498-2]

3. (D) /noun/ Synonym for "plain text".

[RFC4949:2007]

2.1012.5 (EN) CLEARTEXT

alternative term for plaintext. [ISO-18033-1:2005]

2.1012.6 (EN) CLEARTEXT

Intelligible data, the semantic content of which is available. [ISO-7498-2:1989]

2.1012.7 (FR) TEXTE EN CLAIR

Données intelligibles dont la sémantique est compréhensible. [ISO-7498-2:1989]

2.1013 TEXTO EN CLARO ELEGIDO DINÁMICAMENTE

Ver:

- *Ataques a la criptografía*
- *Criptoanálisis*

2.1013.1 TEXTO EN CLARO ELEGIDO DINÁMICAMENTE

Variante del ataque por "texto en claro elegido" donde el atacante va eligiendo dinámicamente el texto.

2.1013.2 (EN) ADAPTIVE CHOSEN PLAINTEXT

A special case of the chosen-plaintext attack in which the cryptanalyst is able to choose plaintexts dynamically, and alter his or her choices based on the results of previous encryptions.

http://www.rsasecurity.com/rsalabs/faq

2.1014 TKIP - TEMPORAL KEY INTEGRITY PROTOCOL

Acrónimos: TKIP

Ver:

- *WPA - Wi-Fi Protected Access*

2.1014.1 TKIP - TEMPORAL KEY INTEGRITY PROTOCOL

TKIP es también llamado "hashing" de Clave WEP. WPA incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricos. WPA tiene TKIP, que utiliza el mismo algoritmo que WEP, pero construye claves en una forma diferente. Estas tecnologías son fácilmente implementadas usando la interfaz gráfica de usuario (GUI) del AP de Cisco, y recibió inicialmente el nombre WEP2. TKIP es una solución temporal que soluciona el problema de reutilización de clave de WEP. WEP utiliza periódicamente la misma clave para cifrar los datos. El proceso de TKIP comienza con una clave temporal de 128 bits que es compartida entre los clientes y los "access points". TKIP combina la clave temporal con la dirección MAC del cliente. Luego agrega un vector de inicialización relativamente largo, de 16 octetos, para producir la clave que cifrará los datos. Este procedimiento asegura que cada estación utilice diferentes claves para cifrar los datos. El "hashing" de clave WEP protege a los Vectores de Inicialización (IVs) débiles para que no sean expuestos haciendo "hashing" del IV por cada paquete.

http://es.wikipedia.org/wiki/TKIP

2.1014.2 (EN) TKIP (TEMPORAL KEY INTEGRITY PROTOCOL)

A security protocol used in Wi-Fi Protected Access (WPA). WPA is used for WiFi networks to correct deficiencies in the older Wired Equivalent Privacy (WEP) standard. TKIP (pronounced "tee-kip") was designed to replace WEP without replacing legacy hardware. This was necessary because the breaking of WEP had left WiFi networks without viable link-layer security, and the solution to this problem could not wait for the replacement of deployed hardware. For this reason, TKIP, like WEP, uses a key scheme based on RC4, but unlike WEP, TKIP provides per-packet key mixing, a message integrity check and a rekeying mechanism. TKIP ensures that every data packet is sent with its own unique encryption key.

http://en.wikipedia.org/wiki/TKIP

2.1015 TLS - TRANSPORT LAYER SECURITY

Acrónimos: TLS

Ver:

- *SSL - Secure Sockets Layer*
- http://www.ietf.org/rfc/rfc4346

2.1015.1 TLS

Acrónimo de “transport layer security” (seguridad de capa de transporte). Diseñado para brindar integridad y confidencialidad de datos en la comunicación entre dos aplicaciones. TLS es el sucesor de SSL.

http://es.pcisecuritystandards.org

2.1015.2 TLS - TRANSPORT LAYER SECURITY

Circuito privado virtual entre dos puertos IP. Opcionalmente, asegura la autenticidad de una o ambas partes y la confidencialidad de los datos transmitidos.

Es el sucesor de SSL.

2.1015.3 (EN) TLS

Acronym for “Transport Layer Security.” Designed with goal of providing data secrecy and data integrity between two communicating applications. TLS is successor of SSL.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.1015.4 (EN) TRANSPORT LAYER SECURITY PROTOCOL - TLS

The successor of SSL is an official Internet Protocol. [ISO-18028-4:2005]

2.1015.5 (EN) TRANSPORT LAYER SECURITY (TLS)

A protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer.

2.1015.6 (FR) TLS

Acronyme de «Transport Layer Security», protocole TLS. Conçu dans le but d’assurer la confidentialité et l’intégrité des données entre deux applications de communication. Le protocole TLS a remplacé le protocole SSL.

http://fr.pcisecuritystandards.org/

2.1016 TOKEN

Ver:

- *Token criptográfico*
- *Token de seguridad*
- *Token de autentificación*
- *Mochila*

2.1016.1 TOKEN

Componente hardware o software diseñado para almacenar y proteger información criptográfica. [CCN-STIC-430:2006]

2.1016.2 TOKEN

En el contexto de las autenticaciones y del control de acceso, un token es un valor proporcionado por un hardware o software que suele funcionar con un servidor de autenticación o VPN para realizar autenticaciones dinámicas o de dos factores.. Consulte RADIUS, TACACS y VPN.

http://es.pcisecuritystandards.org

2.1016.1 (EN) TOKEN

A value provided by hardware or software that usually works with an authentication server or VPN to perform dynamic or two-factor authentication.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.1016.2 (EN) TOKEN

Something that the claimant possesses and controls (such as a key or password) that is used to authenticate a claim. See also cryptographic token. [CNSSI_4009:2010]

2.1016.3 (EN) TOKEN

1. (I) /cryptography/ See: cryptographic token. (Compare: dongle.)

2. (I) /access control/ An object that is used to control access and is passed between cooperating entities in a protocol that synchronizes use of a shared resource. Usually, the entity that currently holds the token has exclusive access to the resource. (See: capability token.)

Usage: This term is heavily overloaded in the computing literature; therefore, IDOCs SHOULD NOT use this term with any definition other than 1 or 2.

3a. (D) /authentication/ A data object or a physical device used to verify an identity in an authentication process.

3b. (D) /U.S. Government/ Something that the claimant in an authentication process (i.e., the entity that claims an identity) possesses and controls, and uses to prove the claim during the verification step of the process. [SP63]

NIST defines four types of claimant tokens for electronic authentication in an information system [SP63]. IDOCs SHOULD NOT use these four NIST terms; they mix concepts in potentially confusing ways and duplicate the meaning of better-established terms. These four terms can be avoided by using more specifically descriptive terms as follows:

- NIST "hard token": A hardware device that contains a protected cryptographic key. (This is a type of "cryptographic token", and the key is a type of "authentication information".)
- NIST "one-time password device token": A personal hardware device that generates one-time passwords. (One-time passwords are typically generated cryptographically. Therefore, this is a type of "cryptographic token", and the key is a type of "authentication information".)
- NIST "soft token": A cryptographic key that typically is stored on disk or some other magnetic media. (The key is a type of "authentication information"; "authentication key" would be a better description.)

- NIST "password token": A secret data value that the claimant memorizes. (This is a "password" that is being used as "authentication information".)

[RFC4949:2007]

2.1016.4 (FR) TOKEN

Également dénommé jeton, un token est un mot de passe non re-jouable émis par un dispositif électronique. Il s'agit en général d'une calculette capable de dérouler un algorithme identique à celui déroulé par le serveur d'authentification. La calculette génère ainsi des mots de passe en même temps que le serveur. L'utilisateur se contente de recopier le mot de passe présenter sur l'écran de la calculette à un instant donné. Ce type de dispositif nécessite en général une synchronisation temporelle du serveur et du token.

Les token SecurID de la société RSA Security et ActivCard One et la société ActivCard sont les plus connus et utilisés.

http://securit.free.fr/glossaire.htm

2.1016.5 (FR) TOKEN

Dans le contexte de l'authentification et du contrôle d'accès, un token est une valeur fournie par un matériel ou un logiciel qui fonctionne avec un serveur d'authentification ou un VPN pour effectuer une authentification dynamique ou à deux facteurs. Voir RADIUS, TACACS et VPN.

http://fr.pcisecuritystandards.org/

2.1017 TOKEN CRIPTOGRÁFICO

Ver:

- *Token*
- *Dispositivo criptográfico*

2.1017.1 TOKEN CRIPTOGRÁFICO

Pequeño dispositivo, fácilmente transportable por un usuario, que almacena información criptográfica y permite realizar funciones criptográficas.

2.1017.2 TOKEN CRIPTOGRÁFICO

Dispositivo de seguridad que utiliza un usuario para autenticarse al acceder a un sistema informático.

Suele tener una pantalla donde se muestra un código de acceso que, junto con una contraseña, el usuario debe introducir en un formulario de acceso, para probar su identidad de un cliente ante un servicio web como puede ser la banca en línea.

http://www.inteco.es/glossary/Formacion/Glosario/

2.1017.3 (EN) CRYPTOGRAPHIC TOKEN

A token where the secret is a cryptographic key. [NIST-SP800-63:2013]

2.1017.4 (EN) CRYPTOGRAPHIC TOKEN

1. (I) A portable, user-controlled, physical device (e.g., smart card or PCMCIA card) used to store cryptographic information and possibly also perform cryptographic functions. (See: cryptographic card, token.) [RFC4949:2007]

2.1018 TOKEN DE AUTENTIFICACIÓN

Ver:

- *Autenticación*
- *Token*

2.1018.1 TESTIGO DE AUTENTICACIÓN; TESTIGO

Información transportada durante un intercambio de autenticación fuerte, que se puede utilizar para autenticar a quien la envió. [X.509:2005]

2.1018.2 TOKEN DE AUTENTIFICACIÓN

Información transmitida durante un intercambio de autenticación fuerte, que puede ser usada para autenticar su remitente (ISO/IEC 9594-8, ITU-T X.509). [Ribagorda:1997]

2.1018.3 (EN) IDENTITY TOKEN

Smart card, metal key, or other physical object used to authenticate identity. [CNSSI_4009:2010]

2.1018.4 (EN) AUTHENTICATION TOKEN

Information conveyed during a strong authentication exchange, which can be used to authenticate its sender. [X.509:2005]

2.1018.5 (FR) JETON D'AUTHENTIFICATION (JETON)

information véhiculée pendant un échange d'authentification forte et pouvant être utilisée pour authentifier son émetteur. [X.509:2005]

2.1019 TOKEN DE SEGURIDAD

Ver:

- *Token*

2.1019.1 TESTIGO DE SEGURIDAD

Conjunto de datos protegido por uno o más servicios de seguridad, junto con la información de seguridad utilizada para prestar esos servicios de seguridad, que se transfiere entre entidades comunicantes. [X.810:1995]

2.1019.2 (EN) SECURITY TOKEN

A set of data protected by one or more security services, together with security information used in the provision of those security services, that is transferred between communicating entities. [X.810:1995]

2.1019.3 (FR) JETON DE SÉCURITÉ

ensemble de données protégé par un ou plusieurs services de sécurité, ainsi que les informations de sécurité utilisées pour la fourniture de ces services de sécurité, qui est transféré entre les entités communicantes. [X.810:1995]

2.1020 TOKENIZATION

2.1020.1 TOKENIZATION

Procedimiento empleado por sistemas financieros para disociar identificadores de la transacción referenciada. De esta forma, los robs de información proporcionan escasa información al atacante, pero el propietario auténtico puede establecer la relación debida con la transacción correspondiente.

2.1020.2 (EN) TOKENIZATION

Tokenization is the process of substituting a sensitive data element with an "easily" reversible benign substitute. Easily means with regards to the data owner - the algorithm used shouldn't be easy to guess and is the key security strength indicator of tokenization. Tokenization can be used to safeguard sensitive data involving, for example, bank accounts, financial statements, medical records, criminal records, driver's licenses, loan applications, stock trades, voter registrations, and other types of personally identifiable information (PII).

http://en.wikipedia.org/wiki/Tokenization_%28data_security%29

2.1020.3 (EN) TOKENIZATION

Tokenization is a process by which the primary account number (PAN) is replaced with a surrogate value called a “token”. De-tokenization is the reverse process of redeeming a token for its associated PAN value. The security of an individual token relies predominantly on the infeasibility of determining the original PAN knowing only the surrogate value.

PCI Data Security Standard (PCI DSS) -- Information Supplement: PCI DSS Tokenization Guidelines

2.1020.4 (EN) TOKENIZATION

Tokenization is the process of replacing sensitive data with unique identification symbols that retain all the essential information about the data without compromising its security. Tokenization seeks to minimize the amount of data a business needs to keep on hand.

http://searchsecurity.techtarget.com/

2.1021 TOLERANCIA A FALLOS

2.1021.1 TOLERANCIA A FALLOS

Capacidad de un programa o sistema de operar correctamente incluso en caso de fallar sus componentes físicos o lógicos. [Ribagorda:1997]

2.1021.2 (EN) FAULT TOLERANCE

Redundant components in storage system provide security against system failure

http://www.datastorex.com/common/glossary.asp

2.1022 TOLERANCIA AL RIESGO

Ver:

- *Riesgo*

2.1022.1 ACTITUD ANTE EL RIESGO

Enfoque de la organización para apreciar un riesgo y eventualmente buscarlo, retenerlo, tomarlo o rechazarlo. [UNE Guía 73:2010]

2.1022.2 APETITO POR EL RIESGO

Cantidad y tipo de riesgo que una organización está preparada para buscar o retener. [UNE Guía 73:2010]

2.1022.3 AVERSIÓN AL RIESGO

Actitud de rechazar el riesgo.[UNE Guía 73:2010]

2.1022.4 TOLERANCIA AL RIESGO

Disponibilidad de una organización o de las partes interesadas para soportar el riesgo después del tratamiento del riesgo con objeto de conseguir sus objetivos.

NOTA. La tolerancia al riesgo puede estar influenciada por requisitos legales o reglamentarios.

[UNE Guía 73:2010]

2.1022.5 (EN) RISK APPETITE

amount and type of risk that an organization is willing to pursue or retain [ISO Guide 73:2009]

2.1022.6 (EN) RISK ATTITUDE

organization's approach to assess and eventually pursue, retain, take or turn away from risk [ISO Guide 73:2009]

2.1022.7 (EN) RISK AVERSION

attitude to turn away from risk [ISO Guide 73:2009]

2.1022.8 (EN) RISK TOLERANCE

organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives

NOTE. Risk tolerance can be influenced by legal or regulatory requirements.

[ISO Guide 73:2009]

2.1022.9 (EN) RISK TOLERANCE

The defined impacts to an enterprise’s information systems that an entity is willing to accept. [CNSSI_4009:2010]

2.1022.10 (EN) RISK APPETITE

The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission. [RiskIT-PG:2009]

2.1022.11 (EN) RISK TOLERANCE

The acceptable level of variation that management is willing to allow for any particular risk as it pursues objectives. the defined risk tolerance. [RiskIT-PG:2009]

2.1022.12 (EN) RISK TOLERANCE

degree to which an entity is willing to accept risk

DHS Risk Lexicon, September 2008

2.1022.13 (FR) ATTITUDE FACE AU RISQUE

approche d'un organisme pour apprécier un risque avant, éventuellement, de saisir ou préserver une opportunité ou de prendre ou rejeter un risque [ISO Guide 73:2009]

2.1022.14 (FR) AVERSION POUR LE RISQUE

attitude de rejet du risque [ISO Guide 73:2009]

2.1022.15 (FR) GOÛT DU RISQUE

importance et type de risque qu'un organisme est prêt à saisir ou à préserver [ISO Guide 73:2009]

2.1022.16 (FR) TOLÉRANCE AU RISQUE

disposition d'un organisme ou d'une partie prenante à supporter le risque après un traitement du risque afin d'atteindre ses objectifs

NOTE. La tolérance au risque peut être régie par des obligations légales ou réglementaires.

[ISO Guide 73:2009]

2.1023 TRANSEC - SEGURIDAD DE LAS TRANSMISIONES

Acrónimos: TRANSEC

Ver:

- *Seguridad en las comunicaciones*
- *Seguridad*

2.1023.1 SEGURIDAD DE LAS TRANSMISIONES (TRANSEC)

Conjunto de medidas destinadas a evitar la interceptación, el análisis de tráfico y la decepción imitativa. [CESID:1997]

2.1023.2 (EN) TRANSMISSION SECURITY (TRANSEC)

Measures (security controls) applied to transmissions in order to prevent interception, disruption of reception, communications deception, and/or derivation of intelligence by analysis of transmission characteristics such as signal parameters or message externals.

Note: TRANSEC is that field of COMSEC which deals with the security of communication transmissions, rather than that of the information being communicated.

[CNSSI_4009:2010]

2.1023.3 (EN) TRANSMISSION SECURITY (TRANSEC)

(I) COMSEC measures that protect communications from interception and exploitation by means other than cryptanalysis. Example: frequency hopping. (Compare: anti-jam, traffic flow confidentiality.) [RFC4949:2007]

2.1024 TRANSPORTE DE CLAVES

Ver:

- *Clave*
- *Clave criptográfica*

2.1024.1 TRANSPORTE DE CLAVES

Transferencia de claves entre módulos criptográficos. Típicamente la transferencia se realiza cifrada.

2.1024.2 (EN) KEY TRANSPORT (ALGORITHM OR PROTOCOL)

1. (I) A key establishment method by which a secret key is generated by a system entity in a communication association and securely sent to another entity in the association. (Compare: key agreement.)

2. (O) "The procedure to send a symmetric key from one party to other parties. As a result, all legitimate participants share a common symmetric key in such a way that the symmetric key is determined entirely by one party." [A9042]

[RFC4949:2007]

2.1024.3 (EN) KEY TRANSPORT

A key establishment procedure whereby one party (the sender) selects and encrypts the keying material and then distributes the material to another party (the receiver).

When used in conjunction with a public key (asymmetric) algorithm, the keying material is encrypted using the public key of the receiver and subsequently decrypted using the private key of the receiver. When used in conjunction with a symmetric algorithm, the keying material is wrapped with a key encrypting key shared by the two parties.

[NIST-SP800-57:2007]

2.1024.4 (EN) KEY TRANSPORT

the process of transferring a key from one entity to another entity. [ISO-19790:2006]

2.1024.5 (EN) ELECTRONIC KEY TRANSPORT

the transfer of cryptographic keys, usually in encrypted form, using electronic means such as a computer network. [ISO-19790:2006]

2.1024.6 (EN) KEY TRANSPORT

secure transport of cryptographic keys from one cryptographic module to another module. [FIPS-140-2:2001]

2.1025 TRANSPOSICIÓN

Ver:

- *Sustitución*

2.1025.1 TRANSPOSICIÓN

Algoritmo criptográfico consistente en la reordenación de los símbolos (bits, caracteres o cadena de éstos) del texto en claro. Usualmente, esta reordenación se ejecuta según un patrón geométrico.

Paradigma de este método criptográfico es la transposición columna, en la cual el texto en claro se dispone según las filas de una matriz y se extrae columna tras columna.

Es término sinónimo de "permutación".

[Ribagorda:1997]

2.1025.2 TRANSPOSICIÓN O PERMUTACIÓN

Sistema de cifrado que consiste en alterar el orden de los caracteres del texto claro. [CESID:1997]

2.1025.3 (EN) TRANSPOSITION

(I) /cryptography/ A method of encryption in which elements of the plain text retain their original form but undergo some change in their sequential position. (Compare: substitution.) [RFC4949:2007]

2.1025.4 (EN) TRANSPOSITION

The cryptographic strategy of changing message-element positions, instead of changing message-element values, as is done in substitution.

http://www.ciphersbyritter.com/GLOSSARY.HTM

2.1025.5 (EN) TRANSPOSITION CIPHER

A method of encrypting a message where the character positions are changed but the characters themselves stay the same.

http://www.nsa.gov/kids/ciphers/ciphe00006.cfm

2.1026 TRATAMIENTO DEL RIESGO

Ver:

- *Riesgo*

2.1026.1 TRATAMIENTO DEL RIESGO:

Proceso destinado a modificar el riesgo. [UNE-ISO Guía 73:2010]

NOTA 1 El tratamiento del riesgo puede implicar:

− evitar el riesgo, decidiendo no iniciar o continuar con la actividad que motiva el riesgo;

− aceptar o aumentar el riesgo con objeto de buscar una oportunidad;

− eliminar la fuente de riesgo;

− cambiar la probabilidad;

− cambiar las consecuencias;

− compartir el riesgo con otra u otras partes [incluyendo los contratos y la financiación del riesgo]; y

− mantener el riesgo en base a una decisión informada.

NOTA 2 Los tratamientos del riesgo que conducen a consecuencias negativas, en ocasiones se citan como "mitigación del riesgo", "eliminación del riesgo", "prevención del riesgo" y "reducción del riesgo".

NOTA 3 El tratamiento del riesgo puede originar nuevos riesgos o modificar los riesgos existentes.

[PNE-ISO/IEC 27000:2014]

2.1026.2 TRATAMIENTO DEL RIESGO

Proceso destinado a modificar el riesgo.

NOTA 1. El tratamiento del riesgo puede implicar:

- evitar el riesgo, decidiendo no iniciar o continuar con la actividad que motiva el riesgo;
- aceptar o aumentar el riesgo con objeto de buscar una oportunidad;
- eliminar la fuente de riesgo;
- cambiar la probabilidad;
- cambiar las consecuencias;
- compartir el riesgo con otra u otras partes [incluyendo los contratos y la financiación del riesgo]; y
- mantener el riesgo en base a una decisión informada.

NOTA 2. Los tratamientos del riesgo que conducen a consecuencias negativas, en ocasiones se citan como "mitigación del riesgo", "eliminación del riesgo", "prevención del riesgo" y "reducción del riesgo".

NOTA 3. El tratamiento del riesgo puede originar nuevos riesgos o modificar los riesgos existentes.

[UNE Guía 73:2010]

2.1026.3 TRATAMIENTO DE RIESGOS

El proceso de selección e implantación de las medidas o salvaguardas para prevenir, impedir, reducir o controlar los riesgos identificados. [UNE-71504:2008]

2.1026.4 EVITACIÓN DE RIESGOS

Decisión resultante del tratamiento de los riesgos encaminada a que la organización no se vea envuelta en una situación de riesgo o bien se pueda retirar de una situación de riesgo. [UNE-71504:2008]

2.1026.5 OPTIMIZACIÓN DE RIESGOS

Proceso de toma de decisiones para reducir los efectos negativos de los riesgos y, en su caso, aprovechar sus aspectos positivos. [UNE-71504:2008]

2.1026.6 TRANSFERENCIA DE RIESGOS

Acción por la que se comparten los riesgos: perjuicios y beneficios. [UNE-71504:2008]

2.1026.7 EVITACIÓN DEL RIESGO

Decisión argumentada de no implicarse en una actividad o de retirarse de ella, con objeto de no estar expuesto a un riesgo particular. [UNE Guía 73:2010]

2.1026.8 REPARTO DEL RIESGO

Forma de tratamiento del riesgo que implica una distribución acordada del riesgo con otras partes.

NOTA 2. El reparto del riesgo se puede realizar mediante seguros u otras formas de contratos.

NOTA 4. La transferencia del riesgo es una forma de reparto del riesgo.

[UNE Guía 73:2010]

2.1026.9 FINANCIACIÓN DEL RIESGO

Forma de tratamiento del riesgo que implica la gestión de contingentes para la previsión de fondos, a fin de hacer frente o a modificar las consecuencias financieras que se pudiesen presentar. [UNE Guía 73:2010]

2.1026.10 RETENCIÓN DEL RIESGO

Aceptación de los beneficios potenciales de una ganancia o de las cargas por pérdida motivadas por un riesgo particular.

NOTA 1. La retención del riesgo incluye la aceptación de los riesgos residuales.

[UNE Guía 73:2010]

2.1026.11 (EN) RISK TREATMENT

process to modify risk [ISO Guide 73:2009]

NOTE 1: Risk treatment can involve:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;
- sharing the risk with another party or parties (including contracts and risk financing); and
- retaining the risk by informed choice.

NOTE 2: Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

NOTE 3: Risk treatment can create new risks or modify existing risks.

[ISO/IEC 27000:2014]

2.1026.12 (EN) RISK TREATMENT

process to modify risk

NOTE 1. Risk treatment can involve:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;

- sharing the risk with another party or parties [including contracts and risk financing]; and
- retaining the risk by informed decision.

NOTE 2. Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

NOTE 3. Risk treatment can create new risks or modify existing risks.

[ISO Guide 73:2009]

2.1026.13 (EN) RISK AVOIDANCE

informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk [ISO Guide 73:2009]

2.1026.14 (EN) RISK AVOIDANCE

strategies or measures taken that effectively remove exposure to a risk

Annotation: Avoidance is one of a set of four commonly used risk management strategies, along with risk control, risk acceptance, and risk transfer.

DHS Risk Lexicon, September 2008

2.1026.15 (EN) RISK SHARING

form of risk treatment involving the agreed distribution of risk with other parties

NOTE 2. Risk sharing can be carried out through insurance or other forms of contract.

NOTE 4. Risk transfer is a form of risk sharing.

[ISO Guide 73:2009]

2.1026.16 (EN) RISK FINANCING

form of risk treatment involving contingent arrangements for the provision of funds to meet or modify the financial consequences should they occur

2.1026.17 (EN) RISK RETENTION

acceptance of the potential benefit of gain, or burden of loss, from a particular risk

NOTE 1. Risk retention includes the acceptance of residual risks.

[ISO Guide 73:2009]

2.1026.18 (FR) TRAITEMENT DU RISQUE

processus destiné à modifier un risque

NOTE 1. Le traitement du risque peut inclure

- un refus du risque en décidant de ne pas démarrer ou poursuivre l'activité porteuse du risque,

- la prise ou l'augmentation d'un risque afin de saisir une opportunité,
- l'élimination de la source de risque,
- une modification de la vraisemblance
- une modification des conséquences,
- un partage du risque avec une ou plusieurs autres parties [incluant des contrats et un financement du risque], et
- un maintien du risque fondé sur une décision argumentée.

NOTE 2. Les traitements du risque portant sur les conséquences négatives sont parfois appelés «atténuation du risque», «élimination du risque», «prévention du risque» et «réduction du risque».

NOTE 3. Le traitement du risque peut créer de nouveaux risques ou modifier des risques existants.

[ISO Guide 73:2009]

2.1026.19 (FR) REFUS DU RISQUE

décision argumentée de ne pas s'engager dans une activité, ou de s'en retirer, afin de ne pas être exposé à un risque particulier [ISO Guide 73:2009]

2.1026.20 (FR) PARTAGE DU RISQUE

forme de traitement du risque impliquant la répartition consentie du risque avec d'autres parties

NOTE 2. Le partage du risque peut intervenir sous forme d'assurances ou autres types de contrats.

NOTE 4. Le transfert du risque est une forme de partage du risque.

[ISO Guide 73:2009]

2.1026.21 (FR) FINANCEMENT DU RISQUE

forme de traitement du risque mettant en jeu des arrangements contingents pour provisionner des fonds afin de faire face à d'éventuelles conséquences financières ou de les modifier [ISO Guide 73:2009]

2.1026.22 (FR) PRISE DE RISQUE

acceptation de l'avantage potentiel d'un gain ou de la charge potentielle d'une perte découlant d'un risque particulier

NOTE 1. La prise de risque comprend l'acceptation des risques résiduels.

[ISO Guide 73:2009]

2.1026.23 (FR) TRAITEMENT DES RISQUES

Sous-processus de la gestion des risques permettant de choisir et de mettre en œuvre des mesures de sécurité visant àmodifier les risques de sécurité de l'information. [EBIOS:2010]

2.1026.24 (FR) TRANSFERT DE RISQUES

Choix de traitement consistant à partager les pertes consécutives à la réalisation de risques. [EBIOS:2010]

2.1027 TRAZABILIDAD (IMPUTABILIDAD)

2.1027.1 IMPUTABILIDAD

La responsabilidad de una entidad por sus acciones y decisiones.

2.1027.2 TRAZABILIDAD

Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE-71504:2008]

2.1027.3 RESPONSABILIDAD

Propiedad de una entidad que garantiza que las acciones de ésta (como violaciones o intentos de violación de la seguridad) queden asociadas inequívocamente a ella. (ISO-7498-2) [Ribagorda:1997]

2.1027.4 RESPONSABILIDAD

Cualidad que permite que todas las acciones realizadas sobre un sistema de tecnología de la información sean asociadas de modo inequívoco a un individuo o entidad. [CESID:1997]

2.1027.5 TRAZABILIDAD

capacidad para seguir la historia, la aplicación o la localización de todo aquello que está bajo consideración [ISO-9000_es:2000]

2.1027.6 IMPUTABILIDAD

Propiedad que garantiza que las acciones de una entidad puedan ser rastreadas de una manera inequívoca para imputarlas a esa entidad. [ISO-7498-2:1989]

2.1027.1 (EN) ACCOUNTABILITY

Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information. [CNSSI_4009:2010]

2.1027.2 (EN)INDIVIDUAL ACCOUNTABILITY

Ability to associate positively the identity of a user with the time, method, and degree of access to an information system. [CNSSI_4009:2010]

2.1027.3 (EN) ACCOUNTABILITY

(I) The property of a system or system resource that ensures that the actions of a system entity may be traced uniquely to that entity, which can then be held responsible for its actions. [Huff] (See: audit service.) [RFC4949:2007]

2.1027.4 (EN) ACCOUNTABILITY

The property that ensures that the actions of an entity may be traced uniquely to the entity. [NIST-SP800-57:2007]

2.1027.5 (EN) ACCOUNTABILITY

The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and afteraction recovery and legal action. [NIST-SP800-27:2004]

2.1027.6 (EN) ACCOUNTABILITY

The security objective that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. [NIST-SP800-33:2001]

2.1027.7 (EN) ACCOUNTABILITY

The property that ensures that the actions of an entity may be traced uniquely to the entity. [ISO-7498-2:1989]

2.1027.8 (FR) IMPUTABILITÉ

La propriété qui assure qu'une action d'une entité peut être tracée et liée de manière unique et sans équivoque à l'entité qui l'a effectuée. [ISO-7498-2:1989]

2.1028 TRIPLE DES

Acrónimos: TDEA, TDES, 3DES

Ver:

- *DES - Data Encryption Standard*
- [ISO-18033-3:2005]

2.1028.1 TRIPLE DES

Algoritmo de cifra que realiza 3 cifrados DES consecutivos. Cifra el texto en bloques de 64 bits. Utiliza claves de 112 o 160 bits (correspondientes a 2 o 3 claves de 56 bits).

2.1028.2 TRIPLE DES

Procedimiento que aumenta la fortaleza del DES consistente en efectuar, en su modo estándar (E-D-E DES), sucesivamente un cifrado, un descifrado y otro cifrado DES usando dos claves, una para los procesos de cifrado y la otra para el de descifrado. [CESID:1997]

2.1028.3 (EN) TRIPLE DES (3DES)

An implementation of the Data Encryption Standard (DES) algorithm that uses three passes of the DES algorithm instead of one as used in ordinary DES applications. Triple DES provides much stronger encryption than ordinary DES but it is less secure than AES. [CNSSI_4009:2010]

2.1028.4 (EN) TRIPLE DATA ENCRYPTION ALGORITHM

(I) A block cipher that transforms each 64-bit plaintext block by applying the DEA three successive times, using either two or three different keys for an effective key length of 112 or 168 bits. [A9052, SP67] [RFC4949:2007]

2.1028.5 (EN) TRIPLE DES

Triple DES is implemented by running the symmetric DES algorithm three times with two or three different keys. The first and the third execution is done in encrypt mode and the second execution is in decrypt mode.

2.1029 TROYANO

Ver:

- *Caballo de Troya*

2.1030 TRUECRYPT

2.1030.1 TRUECRYPT

TrueCrypt es un programa de código abierto multiplataforma para cifrado de archivos y de disco completo (FDE) .

En mayo de 2014, el sitio web de TrueCrypt publicó un anuncio de que el programa había sido retirado. El anuncio advirtió que TrueCrypt podría contener problemas de seguridad no solucionados y ya no era seguro de usar después del fin del soporte para Windows XP. El sitio web recomienda que los usuarios migren de TrueCrypt a BitLocker y proporciona instrucciones paso a paso sobre cómo hacerlo.

http://searchdatacenter.techtarget.com/es/

2.1030.2 (EN) TRUECRYPT

TrueCrypt is a cross-platform open source program for file and full disk encryption (FDE).

In May 2014, the TrueCrypt website posted an announcement that the program had been retired. The announcement warned that TrueCrypt may contain unfixed security issues and was no longer safe to use following the end of support for Windows XP. The website recommends that users migrate from TrueCrypt to BitLocker and provides step-by-step directions for how to do so.

http://searchsecurity.techtarget.com/

2.1031 TRUNCAMIENTO

2.1031.1 TRUNCAMIENTO

Método mediante el cual se elimina definitivamente un segmento de datos del PAN, con lo cual todo el PAN se vuelve ilegible. El truncamiento se relaciona con la protección del PAN cuando está almacenado en archivos, bases de datos, etc. Consulte Ocultamiento para protección del PAN cuando aparece en pantallas, recibos impresos, etc.

http://es.pcisecuritystandards.org

2.1031.2 (EN) TRUNCATION:

Method of rendering the full PAN unreadable by permanently removing a segment of PAN data. Truncation relates to protection of PAN when stored in files, databases, etc. See Masking for protection of PAN when displayed on screens, paper receipts, etc.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.1031.3 (FR) TRONCATURE

Méthode permettant de rendre la totalité du PAN illisible en supprimant en permanence un segment de ses données. La troncature concerne la protection du PAN lorsqu'il est stocké dans des fichiers, bases de données, etc. Voir Masquage pour la protection du PAN lorsqu'il est affiché sur des écrans, des reçus papier, etc.

http://fr.pcisecuritystandards.org/

2.1032 TÚNEL

2.1032.1 TÚNEL

Enlace virtual entre dos dispositivos utilizando una infraestructura previa. Hay diferentes técnicas para crear un túnel: encapsular el protocolo, conmutar por etiquetas, o crear circuitos virtuales. El túnel permite que las entidades conectadas utilicen protocolos que soporta la red subyacente.

2.1032.2 (EN) TUNNELING

Technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network. [CNSSI_4009:2010]

2.1032.3 (EN) TUNNEL

1. (I) A communication channel created in a computer network by encapsulating (i.e., layering) a communication protocol's data packets in (i.e., above) a second protocol that normally would be carried above, or at the same layer as, the first one. (See: L2TP, tunnel mode, VPN. Compare: covert channel.) [RFC4949:2007]

2.1032.4 (EN) TUNNEL

Data path between networked devices which is established across an existing network infrastructure by using techniques such as protocol encapsulation, label switching, or virtual circuits. [ISO-18028-1:2006]

2.1032.5 (EN) TUNNEL

A communication channel created in a computer network by encapsulating a communication protocol's data packets in (on top of) a second protocol that normally would be carried above, or at the same layer as, the first one. Most often, a tunnel is a logical point-to-point link - i.e., an OSI

layer 2 connection - created by encapsulating the layer 2 protocol in a transport protocol (such as TCP), in a network or Internetwork layer protocol (such as IP), or in another link layer protocol. Tunneling can move data between computers that use a protocol not supported by the network connecting them.

http://www.sans.org/security-resources/glossary-of-terms/

2.1032.6 (FR) TUNNELING

Le principe de tunneling consiste à utiliser un réseau public non sécurisé (ex.: Internet) comme élément/extension d'un réseau privé sécurisé. On utilise ainsi les capacités de télécommunication de l'Internet en ajoutant une couche de sécurité afin d'établir un VPN. Sont souvent utilisés les protocoles PPTP, L2TP ou IPSEC pour établir cette couche supplémentaire de sécurité.

http://securit.free.fr/glossaire.htm

2.1033 TWOFISH

Ver:

- http://www.schneier.com/twofish.html
- *Blowfish*
- *AES - Advanced Encryption Standard*

2.1033.1 TWOFISH

En criptografía, Twofish es un método de criptografía simétrica con cifrado por bloques desarrollado por Counterpane Labs y presentado al concurso del NIST que buscaba un sustituto para DES (el concurso AES). El tamaño de bloque en Twofish es de 128 bits y el tamaño de clave puede llegar hasta 256 bits. Twofish llegó a la ronda final del concurso del NIST, pero no fue elegido para la estandarización. TwoFish quedó tercero, tras Rijndael y Serpent.

2.1033.2 (EN) TWOFISH

(O) A symmetric, 128-bit block cipher with variable key length (128, 192, or 256 bits), developed by Counterpane Labs as a candidate for the AES. (See: Blowfish.) [RFC4949:2007]

2.1033.3 (EN) TWOFISH

In cryptography, Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but was not selected for standardisation. Twofish is related to the earlier block cipher Blowfish.

http://en.wikipedia.org/wiki/Twofish

2.1034 VACUNA

Ver:

- *Virus*

2.1034.1 VACUNA

Programa de prevención de ataques de los virus informáticos. [Ribagorda:1997]

2.1034.2 VACUNACIÓN

Mediante esta técnica el programa antivirus almacena información sobre cada uno de los ficheros. En caso de haberse detectado algún cambio entre la información guardada y la información actual del fichero, el antivirus avisa de lo ocurrido. Existen dos tipos de vacunaciones: Interna (la información se guarda dentro del propio fichero, de tal forma que al ejecutarse él mismo comprueba si ha sufrido algún cambio) y Externa (la información se guarda en un fichero especial y desde él se contrasta la información).

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.1034.3 (EN) VACCINE

A technique to fight virus. The anti-virus software registers some summary information of prtected files. When a change is detected, a virus may be the cause.

2.1035 VALIDACIÓN

Ver:

- *verificación*

2.1035.1 VALIDACIÓN

«validación», el proceso de verificar y confirmar la validez de una firma o sello electrónicos. [PE-CONS 60/14]

2.1035.2 VALIDACIÓN

confirmación mediante la aportación de evidencia objetiva de que se han cumplido los requisitos para una utilización o aplicación específica prevista [ISO 9000:2005]

2.1035.3 (EN) VALIDATION

'validation' means the process of verifying and confirming that an electronic signature or a seal is valid. [PE-CONS 60/14]

2.1035.4 (EN) VALIDATION

Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled (e.g., a trustworthy credential has been presented, or data or information has been formatted in accordance with a defined set of rules, or a specific process has demonstrated that an entity under consideration meets, in all respects, its defined attributes or requirements). [CNSSI_4009:2010]

2.1035.5 (EN) VALIDATION

confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled [ISO 9000:2005]

2.1035.6 (FR) VALIDATION

"validation", le processus de vérification et de confirmation de la validité d'une signature ou d'un cachet électronique. [PE-CONS 60/14]

2.1036 VALIDACIÓN DE CERTIFICADOS

Ver:

- *Certificado X.509*
- *Cadena de certificación*
- http://www.ietf.org/rfc/rfc3280

2.1036.1 VALIDACIÓN DE CERTIFICADO

Proceso para asegurar que un certificado era válido en un momento determinado, con posible inclusión de la construcción y el procesamiento de un trayecto de certificación, y que asegura que todos los certificados en dicho trayecto eran válidos (es decir, no habían caducado ni estaban revocados) en un determinado momento. [X.509:2005]

2.1036.2 (EN) CERTIFICATE VALIDATION

1. (I) An act or process by which a certificate user establishes that the assertions made by a digital certificate can be trusted. (See: valid certificate, validate vs. verify.)

2. (O) "The process of ensuring that a certificate was valid at a given time, including possibly the construction and processing of a certification path [R4158], and ensuring that all certificates in that path were valid (i.e. were not expired or revoked) at that given time." [X509] [RFC4949:2007]

2.1036.3 (EN) CERTIFICATE VALIDATION

The process of ensuring that a certificate was valid at a given time, including possibly the construction and processing of a certification path, and ensuring that all certificates in that path were valid (i.e. were not expired or revoked) at that given time. [X.509:2005]

2.1036.4 (EN) PATH VALIDATION

(I) The process of validating (a) all of the digital certificates in a certification path and (b) the required relationships between those certificates, thus validating the contents of the last certificate on the path. (See: certificate validation.) [RFC4949:2007]

2.1036.5 (FR) VALIDATION DE CERTIFICAT

processus consistant à s'assurer qu'un certificat était valide à un instant donné, impliquant éventuellement la construction et le traitement d'un itinéraire de certification avec la garantie que tous

les certificats de l'itinéraire étaient valides (c'est-à-dire, non caducs ou révoqués) à l'instant donné. [X.509:2005]

2.1037 VALIDAR

Ver:

- *Verificar*

2.1037.1 VALIDACIÓN

(Transición del Servicio) Una Actividad que asegura que un Servicio de TI, Proceso, Plan u otro Entregable nuevo o cambiado satisface las necesidades del Negocio. La Validación asegura que los Requerimientos de Negocio son satisfechos incluso aunque estos sean cambiados desde su diseño original.

Ver Verificación, Aceptación, Cualificación, Validación y Prueba del Servicio.

[ITIL:2007]

2.1037.2 VALIDACIÓN

confirmación mediante el suministro de evidencia objetiva de que se han cumplido los requisitos para una utilización o aplicación específica prevista [ISO-9000_es:2000]

2.1037.3 (EN) VALIDATE

1. (I) Establish the soundness or correctness of a construct. Example: certificate validation. (See: validate vs. verify.)

2. (I) To officially approve something, sometimes in relation to a standard. Example: NIST validates cryptographic modules for conformance with [FP140].

[RFC4949:2007]

2.1037.4 (EN) VALIDATION

(Service Transition) An Activity that ensures a new or changed IT Service, Process, Plan, or other Deliverable meets the needs of the Business. Validation ensures that Business Requirements are met even though these may have changed since the original Design.

See Verification, Acceptance, Qualification, Service Validation and Testing.

[ITIL:2007]

2.1038 VALOR

Ver:

- *Activo*

2.1038.1 VALOR

Cualidad que poseen algunas realidades, consideradas bienes, por lo cual son estimables.

DRAE. Diccionario de la Lengua Española.

2.1038.2 VALOR (DE UN ACTIVO)

Es una estimación del coste inducido por la materialización de una amenaza. [Magerit:2012]

2.1038.3 VALOR ACUMULADO

Considera tanto el valor propio de un activo como el valor de los activos que dependen de él. [Magerit:2012]

2.1038.4 (EN) VALUE

The quality of being useful or important.

Oxford Advanced Learner's Dictionary.

2.1038.5 (EN) VALUE

relative worth, utility, or importance.

Merriam-Webster's.

2.1038.6 (EN) INFORMATION VALUE

A qualitative measure of the importance of the information based upon factors such as: level of robustness of the Information Assurance controls allocated to the protection of information based upon: mission criticality, the sensitivity (e.g., classification and compartmentalization) of the information, releasability to other countries, perishability/longevity of the information (e.g., short life data versus long life intelligence source data), and potential impact of loss of confidentiality and integrity and/or availability of the information. [CNSSI_4009:2010]

2.1038.7 (EN) ASSET VALUE

The perceived or intrinsic worth of an asset.

http://www.symantec.com/avcenter/refa.html

2.1039 VALORACIÓN

Ver:

- *Estimar*
- *Valoración*
- *Auditoría*

2.1039.1 EVALUACIÓN

Inspección y análisis para verificar si un Estándar o un conjunto de Guías se está siguiendo, que sus Registros son precisos, o que las metas de Eficiencia y Efectividad se están cumpliendo. Ver Auditoría. [ITIL:2007]

2.1039.2 VALORAR

Reconocer, estimar o apreciar el valor o mérito de alguien o algo.

2.1039.3 (EN) ASSESSMENT

Inspection and analysis to check whether a Standard or set of Guidelines is being followed, that Records are accurate, or that Efficiency and Effectiveness targets are being met. See Audit. [ITIL:2007]

2.1039.4 (EN) ASSESSMENT

Verification of a product, system, or service against a standard using the corresponding assessment method to establish compliance and determine the assurance. [ISO-15443-1:2005]

2.1039.5 (EN) ASSESSMENT

Verification of a deliverable against a standard using the corresponding method to establish compliance and determine the assurance. [ISO-15443-1:2005]

2.1039.6 (FR) ÉVALUATION

Inspection et analyse permettant de vérifier qu'un standard ou un ensemble de principes a bien été suivi, que les enregistrements sont précis ou que les objectifs d'efficience et d'efficacité ont été atteints. Voir Audit. [ITIL:2007]

2.1040 VALOR DE INICIALIZACIÓN

Acrónimos: IV

2.1040.1 VALOR DE INICIALIZACIÓN

Valor usado para establecer las condiciones de arranque de un proceso de cifrado.

Esto incrementa la seguridad al establecer una variable adicional. Así mismo, facilita la sincronización de los equipos criptográficos (ISO 8372).

Este valor debe ser conocido por emisor y receptor con anterioridad a la transmisión de informaciones cifradas.

[Ribagorda:1997]

2.1040.2 VECTOR DE INICIALIZACIÓN

Es término sinónimo de "valor de inicialización". [Ribagorda:1997]

2.1040.3 (EN) INITIALIZATION VALUE (IV)

(I) /cryptography/ An input parameter that sets the starting state of a cryptographic algorithm or mode. (Compare: activation data.) [RFC4949:2007]

2.1040.4 (EN) INITIALIZATION VECTOR (IV)

A vector used in defining the starting point of a cryptographic process. [NIST-SP800-57:2007]

2.1040.5 (EN) INITIALIZATION VALUE

a vector used in defining the starting point of an encryption process within a cryptographic algorithm. [FIPS-140-2:2001]

2.1041 VALOR RESUMEN

Ver:

- *Hash code*
- *Resumen criptográfico*
- *Función resumen*
- *Hash*

2.1041.1 VALOR RESUMEN

Resultado de aplicar una función resumen determinada a una cierta información.

2.1041.2 (EN) HASH VALUE

The result of applying a hash function to information. [NIST-SP800-57:2007]

2.1041.3 (EN) HASH-VALUE

string of bits which is the output of a hash-function [ISO-10118-1:2000]

2.1042 VERIFICACIÓN

Ver:

- *validación*

2.1042.1 VERIFICACIÓN

confirmación mediante la aportación de evidencia objetiva de que se han cumplido los requisitos especificados. [ISO 9000:2005]

2.1042.2 (EN) VERIFICATION

Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome. [CNSSI_4009:2010]

2.1042.3 (EN) VERIFICATION

confirmation, through the provision of objective evidence, that specified requirements have been fulfilled [ISO-9000:2005]

2.1043 VERIFICACIÓN DE FIRMA

Ver:

- *Firma digital*
- *Datos de verificación de firma*
- *Dispositivo de verificación de firma*

2.1043.1 VERIFICACIÓN DE FORMA

Proceso que toma como entrada el mensaje firmado, la clave de verificación y los parámetros del dominio, y que da como salida el resultado de la verificación de firma: válida o inválida.

2.1043.2 (EN) VERIFICATION PROCESS

A process which takes as input the signed message, the verification key and the domain parameters, and which gives as output the result of the signature verification: valid or invalid. [ISO/IEC ISO-14888-1] [ISO-15946-2:2002]

2.1043.3 (EN) MESSAGE SIGNATURE VERIFICATION

A process which takes as input the signed message, the verification key and the domain parameters, and which gives as output the result of the signature verification: valid or invalid. [ISO-14888-1:1998]

2.1044 VERIFICACIÓN VISUAL

Ver:

- *CAPTCHA*
- *Anti automatización*
- *Autenticación*

2.1044.1 VERIFICACIÓN VISUAL

Método visual anti automatización. Consiste en requerir del aspirante que demuestre una habilidad visual fácil para un ser humano pero difícil para un robot, permitiendo así distinguir unos de otros.

2.1044.2 (EN) VISUAL VERIFICATION

Visual oriented method of anti-automation that prevents automated programs from exercising web site functionality by determining if there is presence of mind.

http://www.webappsec.org/projects/glossary/

2.1045 VERIFICADOR

2.1045.1 VERIFICADOR

Una entidad que es, o representa, la entidad solicitante de una autenticación de identidad. Un verificador incluye las funciones necesarias de conexión en un intercambio de autenticación (ISO/IEC ISO-10181-2). [Ribagorda:1997]

2.1045.2 (EN) VERIFIER

entity including the functions necessary for engaging in authentication exchanges on behalf of an entity requiring an entity authentication [ISO-9798-5:2004]

2.1045.3 (EN) VERIFIER

An entity that verifies evidence. [ISO-13888-1:2004]

2.1045.4 (EN) VERIFIER

an entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges. [ISO-9798-1:1997]

2.1045.5 (EN) VERIFIER

An entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges. [ISO-9798-1:1997]

2.1046 VERIFICADOR DEL SELLO DE TIEMPO

Ver:

- *Sello de tiempo*

2.1046.1 VERIFICADOR DEL SELLO DE TIEMPO

entidad que tiene unos datos y dessea verificar que disfrutan de un sello de tiempo ligado a ellos

NOTA. La verificación puede llevarla a cabo el propio verificador u una tercera parte de confianza

[traducción de ISO/IEC 18014-1]

2.1046.2 (EN) TIME-STAMP VERIFIER

entity which possesses data and wants to verify that it has a valid time-stamp bound to it

NOTE. The verification process may be performed by the verifier itself or by a Trusted Third Party.

[ISO-18014-1:2002]

2.1047 VERIFICADOR DE PRIVILEGIOS

Ver:

- *Privilegio*

2.1047.1 VERIFICADOR DE PRIVILEGIOS

Entidad que verifica certificados a partir de una política de privilegios. [X.509:2005]

2.1047.2 (EN) PRIVILEGE VERIFIER

An entity verifying certificates against a privilege policy. [X.509:2005]

2.1047.3 (FR) VÉRIFICATEUR DE PRIVILÈGE

entité effectuant la vérification de certificats conformément à une politique de privilège. [X.509:2005]

2.1048 VERIFICAR

Ver:

- *Validar*

2.1048.1 VERIFICACIÓN

(Transición del Servicio) Una Actividad que asegura que un Servicio de TI, Proceso, Plan u otro Entregable nuevo o cambiado, es completo, preciso, Confiable y está de acuerdo con su Especificación de Diseño.

Ver Validación, Aceptación, Validación y Prueba del Servicio.

[ITIL:2007]

2.1048.2 VERIFICACIÓN

confirmación mediante la aportación de evidencia objetiva de que se han cumplido los requisitos especificados [ISO-9000_es:2000]

2.1048.3 (EN) VERIFY

(I) To test or prove the truth or accuracy of a fact or value. (See: validate vs. verify, verification. Compare: authenticate.) [RFC4949:2007]

2.1048.4 (EN) VERIFICATION

1. (I) /authentication/ The process of examining information to establish the truth of a claimed fact or value. (See: validate vs. verify, verify. Compare: authentication.)

2. (N) /COMPUSEC/ The process of comparing two levels of system specification for proper correspondence, such as comparing a security model with a top-level specification, a top-level specification with source code, or source code with object code. [NCS04]

[RFC4949:2007]

2.1048.5 (EN) VERIFICATION

(Service Transition) An Activity that ensures a new or changed IT Service, Process, Plan, or other Deliverable is complete, accurate, Reliable and matches its Design Specification.

See Validation, Acceptance, Service Validation and Testing.

[ITIL:2007]

2.1049 VIRUS

Ver:

- *Firma de un virus*
- *Código dañino*
- http://en.wikipedia.org/wiki/Computer_virus

2.1049.1 VIRUS

Programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros. [CCN-STIC-430:2006]

2.1049.2 VIRUS

Segmento de código que puede copiarse, tras la satisfacción de alguna condición lógica o temporal, para infectar otros programas, a los que ataca modificándolos, destruyéndolos, etc. [Ribagorda:1997]

2.1049.3 VIRUS POLIMÓRFICO

Virus que muta con cada nueva infección, haciendo así su detección mediante una firma imposible.

Los más sofisticados usan técnicas de cifrado con claves criptográficas aleatorias que varían de infección en infección. El segmento de código encargado de esta generación aleatoria se denomina motor de mutaciones.

[Ribagorda:1997]

2.1049.4 VIRUS SOLAPADO

Virus que oculta su presencia incluso a los productos antivirus. Por ejemplo, puede cambiar el código de detección de errores para engañar a un programa de detección. [Ribagorda:1997]

2.1049.5 (EN) VIRUS

Self-replicating, malicious code that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence.

The Tallinn Manual, 2013

2.1049.6 (EN) VIRUS

A self-replicating program that spreads to other users by inserting copies of itself into other executable code or documents. [CSS NZ:2011]

2.1049.7 (EN) VIRUS

A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. [CNSSI_4009:2010]

2.1049.8 (EN) VIRUS

(I) A self-replicating (and usually hidden) section of computer software (usually malicious logic) that propagates by infecting -- i.e., inserting a copy of itself into and becoming part of -- another program. A virus cannot run by itself; it requires that its host program be run to make the virus active. [RFC4949:2007]

2.1049.9 (EN) VIRUS

A form of malware that is designed to self-replicatemake copies of itselfand distribute the copies to other files, programs, or computers. [NIST-SP800-83:2005]

2.1049.10 (EN) VIRUS

A self-replicating program that runs and spreads by modifying other programs or files. [NIST-SP800-61:2004]

2.1049.11 (EN) VIRUS

A computer program with the ability to replicate itself usually by attaching itself to other programs to the detriment of security and integrity.

May or may not be introduced through a Trojan Horse.

[IRM-5239-8:1995]

2.1049.12 (EN) VIRUS

A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting - i.e., inserting a copy of itself into and becoming part of - another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

http://www.sans.org/security-resources/glossary-of-terms/

2.1049.13 (EN) VIRUS

A malicious program that replicates itself and may cause damage to a computer system by attacking or attaching itself to boot information, another program or a document that uses macros.

http://www.csoonline.com/glossary/

2.1049.14 (EN) VIRUSES

A virus is a program or code that replicates itself onto other files with which it comes in contact; that is, a virus can infect another program, boot sector, partition sector, or a document that supports macros, by inserting itself or attaching itself to that medium. Most viruses only replicate, though many can do damage to a computer system or a user's data as well.

http://www.symantec.com/avcenter/refa.html

2.1049.15 (EN) MACRO VIRUS

A program or code segment written in the internal macro language of an application. Some macros replicate, while others infect documents.

http://www.symantec.com/avcenter/refa.html

2.1049.16 (EN) POLYMORPHIC VIRUS

A virus that can change its byte pattern when it replicates; thereby, avoiding detection by simple string-scanning techniques.

http://www.symantec.com/avcenter/refa.html

2.1049.17 (EN) RETROVIRUS

A computer virus that actively attacks an antivirus program or programs in an effort to prevent detection.

http://www.symantec.com/avcenter/refa.html

2.1049.18 (FR) VIRUS INFORMATIQUE

Un virus est un logiciel ou un morceau de logiciel qui, pour pouvoir se propager, s'attache à tout type de fichier ou autre logiciel, et qui a pour vocation l'infection et sa propagation d'une machine à une autre, à l'insu des utilisateurs. Son code exécutable se greffe au code exécutable de son programme hôte lui permettant ainsi de se propager et de s'exécuter à l'aide de programmes hôtes. Un virus ne peut s'exécuter que par l'exécution d'un programme hôte à la différence du ver qui possède son propre moteur de propagation. Pour chaque virus apparu, de nombreuses variantes sont écrites.

http://www.cases.public.lu/functions/glossaire/

2.1049.19 (FR) MÉTAMORPHIQUE (VIRUS)

Type de virus qui se transforme en se reproduisant pour rendre sa détection plus difficile. Contrairement aux virus polymorphes, les virus métamorphiques se désintègrent et se reconstruisent entièrement quand ils se reproduisent.

http://www.cases.public.lu/functions/glossaire/

2.1049.20 (FR) POLYMORPHE (VIRUS)

virus qui peut prendre plusieurs formes et est capable de modifier sa signature à chaque nouvelle génération, le rendant difficilement détectable pour les anti-virus, notamment ceux se basant uniquement sur des bases de données de signatures.

http://www.cases.public.lu/functions/glossaire/

2.1050 VULNERABILIDAD

Ver:

- *Exploit*

- *Daño*
- *Exposición*
- *Gestión de vulnerabilidades*
- *Evaluación de vulnerabilidad*
- *Escáner de vulnerabilidades*
- *Análisis de vulnerabilidades*

2.1050.1 VULNERABLE

Que puede ser herido o recibir lesión, física o moralmente.

DRAE. Diccionario de la Lengua Española.

2.1050.2 VULNERABILIDAD:

Debilidad de un activo o de un control que puede ser explotada por una o más amenazas. [UNE-ISO/IEC 27000:2014]

2.1050.3 VULNERABILIDAD:

Propiedades intrínsecas de que algo produzca como resultado una sensibilidad a una fuente de riesgo que puede conducir a un suceso con una consecuencia [UNE Guía 73:2010]

2.1050.4 VULNERABILIDAD

Una debilidad que puede ser aprovechada por una Amenaza. Por ejemplo un puerto abierto en el cortafuegos, una clave de acceso que no se cambia, o una alfombra inflamable. También se considera una Vulnerabilidad un Control perdido. [ITIL:2007]

2.1050.5 VULNERABILIDAD

Debilidad o falta de control que permitiría o facilitaría que una amenaza actuase contra un objetivo o recurso del Sistema.

2.1050.6 VULNERABILIDAD

Debilidad de seguridad de un sistema que le hace susceptible de poder ser dañado al ser aprovechada por una amenaza. [CCN-STIC-400:2006]

2.1050.7 VULNERABILIDAD

Error en un programa o un fallo en la configuración que puede permitir a un atacante obtener acceso no autorizado al sistema. [CCN-STIC-431:2006]

2.1050.8 VULNERABILIDAD

Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza. [Magerit:2012]

2.1050.9 VULNERABILIDAD

Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. [UNE-71504:2008]

2.1050.10 VULNERABILIDAD

Error o debilidad que, de llegar a explotarse, puede ocasionar una exposición a riesgos del sistema, intencionalmente o no.

http://es.pcisecuritystandards.org

2.1050.11 VULNERABILIDAD

Característica de una entidad que puede ser una debilidad o una falla desde el punto de vista de la seguridad de los sistemas de información. [EBIOS:2005]

2.1050.12 VULNERABILIDAD

1. Debilidad del Objeto de Evaluación (debido a errores en su análisis, diseño, implementación u operación) (ITSEC).

2. Debilidad en el sistema de protección de un activo.

3. Susceptibilidad de un sistema o producto a sufrir daños ante ataques específicos.

[Ribagorda:1997]

2.1050.13 VULNERABILIDAD

Debilidad en la seguridad de un sistema de información. Puede ser:

- Explotable: Vulnerabilidad que puede ser explotada en la práctica para romper un objetivo de seguridad.
- Potencial: Vulnerabilidad supuesta que puede ser utilizada para romper un objetivo de seguridad, pero cuya posibilidad, explotación o existencia no ha sido aún demostrada.

[CESID:1997]

2.1050.14 (EN) VULNERABILITY

weakness of an asset or control that can be exploited by one or more threats [ISO/IEC 27000:2014]

2.1050.1 (EN) VULNERABILITY:

A vulnerability refers to a weakness in a system that can be utilized by an attacker to damage the system. obtain unauthorized access. execute arbitrary code. or otherwise exploit the system. [knapp:2014]

2.1050.2 (EN) VULNERABILITY ASSESSMENT:

The process of scanning networks to find hosts or assets. and probing those hosts to determine vulnerabilities. Vulnerability assessment can be automated using a vulnerability assessment scanner, which will typically examine a host to determine the version of the operating system and all running applications. which can then be compared against a repository of known software vulnerabilities to determine where patches should be applied. [knapp:2014]

2.1050.3 (EN) VULNERABILITY

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. [CNSSI_4009:2010]

2.1050.4 (EN) VULNERABILITY ANALYSIS

See vulnerability assessment. [CNSSI_4009:2010]

2.1050.5 (EN) VULNERABILITY ASSESSMENT

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. [CNSSI_4009:2010]

2.1050.6 (EN) VULNERABILITY

intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence [ISO Guide 73:2009]

2.1050.7 (EN) VULNERABILITY

physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard

Example: Installation of vehicle barriers may remove a vulnerability related to attacks using vehicle-borne improvised explosive devices.

Extended Definition: characteristic of design, location, security posture, operation, or any combination thereof, that renders an asset, system, network, or entity susceptible to disruption, destruction, or exploitation

Annotation: In calculating risk of an intentional hazard, the common measurement of vulnerability is the likelihood that an attack is successful, given that it is attempted.

DHS Risk Lexicon, September 2008

2.1050.8 (EN) VULNERABILITY ASSESSMENT

process for identifying physical features or operational attributes that render an entity, asset, system, network, or geographic area susceptible or exposed to hazards

Example: The team conducted a vulnerability assessment on the ship to determine how it might be exploited or attacked by an adversary.

Annotation: Vulnerability assessments can produce comparable estimates of vulnerabilities across a variety of hazards or assets, systems, or networks.

DHS Risk Lexicon, September 2008

2.1050.9 (EN) VULNERABILITY:

Flaw or weakness which, if exploited, may result in an intentional or unintentional compromise of a system..

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.1050.10 (EN) VULNERABILITY

A weakness in design, implementation, operation or internal control [RiskIT-PG:2009]

2.1050.11 (EN) VULNERABILITY EVENT

Any event where a material increase in vulnerability results. Note that this increase in vulnerability can result from changes in control conditions or from changes in threat capability/force. [RiskIT-PG:2009]

2.1050.12 (EN) VULNERABILITY

(I) A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy. (See: harden.) [RFC4949:2007]

2.1050.13 (EN) VULNERABILITY

A weakness that could be exploited by a Threat. For example an open firewall port, a password that is never changed, or a flammable carpet. A missing Control is also considered to be a Vulnerability. [ITIL:2007]

2.1050.14 (EN) VULNERABILITY

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [FIPS-200:2006] [NIST-SP800-53:2013]

2.1050.15 (EN) VULNERABILITY

Flaw, weakness or property of the design or implementation of an information system (including its security controls) or its environment that could be intentionally or unintentionally exploited to adversely effect an organization's assets or operations. [ISO-19790:2006]

2.1050.16 (EN) VULNERABILITY

a weakness in the TOE that can be used to violate the SFRs in some environment.

TOE - Target of Evaluation

SFR - Security Functional Requirement

[CC:2006]

2.1050.17 (EN) RESIDUAL VULNERABILITY

weakness that cannot be exploited in the operational environment for the TOE, but that could be used to violate the SFRs by an attacker with greater attack potential than is anticipated in the operational environment for the TOE.

TOE - Target of Evaluation

SFR - Security Functional Requirement

[CC:2006]

2.1050.18 (EN) VULNERABILITY

A defect or weakness in system security procedure, design, implementation, or internal control that an attacker can exploit. A vulnerability can exist in one or more of the components making up a system, even if those components aren't necessarily involved with security functionality.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/risk/248-BSI.html

2.1050.19 (EN) VULNERABILITY

Characteristic of an entity that can constitute a weakness or flaw in terms of information systems security. [EBIOS:2005]

2.1050.20 (EN) VULNERABILITY

A weakness in a system, application, or network that is subject to exploitation or misuse. [NIST-SP800-61:2004]

2.1050.21 (EN) VULNERABILITY

A weakness or lack of controls that would allow or facilitate a threat actuation against a specific asset or target. [CRAMM:2003]

2.1050.22 (EN) VULNERABILITY

An information security "vulnerability" is a mistake in software that can be directly used by a hacker to gain access to a system or network.

CVE considers a mistake a vulnerability if it allows an attacker to use it to violate a reasonable security policy for that system (this excludes excluding entirely "open" security policies in which all users are trusted, or where there is no consideration of risk to the system).

http://www.cve.mitre.org/

2.1050.23 (EN) VULNERABILITY

The susceptibility of information to exploitation by an adversary.

http://www.ioss.gov/docs/definitions.html

2.1050.24 (EN) TECHNICAL VULNERABILITY

A hardware, firmware, communication, or software flaw that leaves a computer processing system open for potential exploitation, either externally or internally, thereby resulting in risk for the owner, user, or manager of the system. [IRM-5239-8:1995]

2.1050.25 (EN) VULNERABILITY

A flaw or weakness in the design or implementation of an information system (including security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely affect an agencys operations (including missions, functions, and public confidence in the agency), an agencys assets, or individuals (including privacy) through a loss of confidentiality, integrity, or availability. [NIST-SP800-60V2:2004]

2.1050.26 (EN) VULNERABILITY

A weakness in system security requirements, design, implementation, or operation, that could be accidentally triggered or intentionally exploited and result in a violation of the systems security policy. [NIST-SP800-27:2004]

2.1050.27 (EN) VULNERABILITY

a security weakness in a Target of Evaluation (for example, due to failures in analysis, design, implementation or operation). [ITSEC:1991]

2.1050.28 (EN) POTENTIAL VULNERABILITY

a weakness the existence of which is suspected (by virtue of a postulated attack path), but not confirmed, to violate the SFRs.

SFR - Security Functional Requirement

[CC:2006]

2.1050.29 (EN) ENCOUNTERED POTENTIAL VULNERABILITIES

potential weakness in the TOE identified by the evaluator while performing evaluation activities that could be used to violate the SFRs.

TOE - Target of Evaluation

SFR - Security Functional Requirement

[CC:2006]

2.1050.30 (EN) RESIDUAL VULNERABILITY

a weakness that cannot be exploited in the operational environment for the TOE, but that could be used to violate the SFRs by an attacker with greater attack potential than is anticipated in the operational environment for the TOE.

TOE - Target of Evaluation

SFR - Security Functional Requirement

[CC:2006]

2.1050.31 (EN) EXPLOITABLE VULNERABILITY

a weakness in the TOE that can be used to violate the SFRs in the operational environment for the TOE.

TOE - Target of Evaluation

SFR - Security Functional Requirement

[CC:2006]

2.1050.32 (EN) VULNERABILITY

A weakness in system security procedures, design, implementation, internal controls, etc., that could be accidentally triggered or intentionally exploited and result in a violation of the systems security policy. [NIST-SP800-33:2001]

2.1050.33 (EN) VULNERABILITY

A security vulnerability is a flaw or weakness in a systems design, implementation or operation that could be exploited to violate the systems security (RFC 2828). A security vulnerability is not a risk, a threat, or an attack.

Vulnerabilities can be of four types.

- Threat Model vulnerabilities originate from the difficulty to foresee future threats (e.g. Signalling System No.7).
- Design & Specification vulnerabilities come from errors or oversights in the design of the protocol that make it inherently vulnerable (e.g. WEP in IEEE 802.11b a.k.a. WiFi).
- Implementation vulnerabilities are vulnerabilities that are introduced by errors in a protocol implementation.
- Finally, Operation and Configuration vulnerabilities originate from improper usage of options in implementations or weak deployment policies (e.g. not enforcing use of encryption in a WiFi network, or selection of a weak stream cipher by the network administrator).

2.1050.34 (EN) VULNERABILITY

A (universal) vulnerability is a state in a computing system (or set of systems) which either:

- Allows an attacker to execute commands as another user
- Allows an attacker to access data that is contrary to the specified access restrictions for that data
- Allows an attacker to pose as another entity
- Allows an attacker to conduct a denial of service

http://www.symantec.com/avcenter/refa.html

2.1050.35 (EN) VULNERABILITY

A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

http://www.sans.org/security-resources/glossary-of-terms/

2.1050.36 (EN) VULNERABILITIES

A vulnerability is a software weakness that can be exploited by an attacker. Bugs and flaws collectively form the basis of most software vulnerabilities.

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/attack/590-BSI.html

2.1050.37 (EN) VULNERABILITY

An inadequacy related to security that could increase susceptibility to compromise or injury.

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

2.1050.38 (FR) VULNÉRABILITÉ

propriétés intrinsèques de quelque chose entraînant une sensibilité à une source de risque pouvant induire un événement avec une conséquence

[ISO Guide 73:2009]

2.1050.39 (FR) VULNÉRABILITÉ

Défaut ou faiblesse qui, s'il est exploité, peuvent compromettre un système, intentionnellement ou non.

http://fr.pcisecuritystandards.org/

2.1050.40 (FR) VULNÉRABILITÉ

Une faiblesse qui pourrait être exploitée par une menace. Par exemple, un pare-feu ouvert, un mot de passe qui n'est jamais changé ou une moquette inflammable. Un contrôle manquant est également considéré comme une vulnérabilité. [ITIL:2007]

2.1050.41 (FR) VULNÉRABILITÉ

Caractéristique d'un bien support qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information. [EBIOS:2010]

2.1050.42 (FR) VULNÉRABILITÉ

Insuffisance liée à la sécurité qui pourrait accroître la susceptibilité à la compromission ou au préjudice.

http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578

2.1051 WAR CHALKING

2.1051.1 WAR CHALKING

Es la práctica de dibujar símbolos con tiza en paredes o pisos para indicar la existencia de puntos de acceso desprotegidos que permitan el acceso inalámbrico a redes. Luego todos podrán ver desde el exterior que en ese lugar hay nodos abiertos sin ningún tipo de protección.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.1051.2 (EN) WAR CHALKING

War chalking is marking areas, usually on sidewalks with chalk, that receive wireless signals that can be accessed.

http://www.sans.org/security-resources/glossary-of-terms/

2.1052 WAR DIALER

2.1052.1 WAR DIALER

Barrido automatizado de números de teléfono. Se buscan números a los que respondan equipos informáticos, con ánimo de identificar puntos de ataque para intentar penetrar en el sistema.

2.1052.2 (EN) WAR DIALER

(I) /slang/ A computer program that automatically dials a series of telephone numbers to find lines connected to computer systems, and catalogs those numbers so that a cracker can try to break the systems. [RFC4949:2007]

2.1052.3 (EN) WAR DIALER

A computer program that automatically dials a series of telephone numbers to find lines connected to computer systems, and catalogs those numbers so that a cracker can try to break into the systems.

http://www.sans.org/security-resources/glossary-of-terms/

2.1052.4 (EN) WAR DIALING

War dialing is a simple means of trying to identify modems in a telephone exchange that may be susceptible to compromise in an attempt to circumvent perimeter security.

http://www.sans.org/security-resources/glossary-of-terms/

2.1053 WAR DRIVING

2.1053.1 WAR DRIVING

Técnica difundida donde individuos equipados con material apropiado (dispositivo inalámbrico, antena, software de rastreo y unidad GPS) tratan de localizar en coche puntos inalámbricos desprotegidos. Existen otras modalidades dependiendo de cómo se realice el rastreo: a pie, bicicleta, patines, etc...

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.1053.2 (EN) WAR DRIVING

War driving is the process of traveling around looking for wireless access point signals that can be used to get network access.

2.1053.3 (FR) WARDRIVING

Méthode consistant à repérer les points d'accès de réseaux sans fil (localisation physique et mémorisation de leur configuration) en se déplaçant sur un territoire donné. La cartographie s'effectue généralement à partir d'un véhicule et d'un dispositif électronique (ordinateur portable, agenda électronique doté d'une carte WIFI) pour tenter de découvrir les zones géographiques publiques couvertes par un point d'accès privé.

http://www.cases.public.lu/functions/glossaire/

2.1054 WAREZ

Ver:

- *Piratería*

2.1054.1 WAREZ

Programas pirateados.

2.1054.2 (EN) WAREZ

Pirated software.

2.1055 WARM_STANDBY

Ver:

- *Opción de recuperación*
- *Warm site*

2.1055.1 (EN) WARM STANDBY

Synonym for Intermediate Recovery. [ITIL:2007]

2.1055.2 (EN) INTERMEDIATE RECOVERY

(Service Design) A Recovery Option which is also known as Warm Standby. Provision is made to Recover the IT Service in a period of time between 24 and 72 hours. Intermediate Recovery typically uses a shared Portable or Fixed Facility that has computer Systems and network Components. The hardware and software will need to be configured, and data will need to be restored, as part of the IT Service Continuity Plan. [ITIL:2007]

2.1056 WARM SITE

Ver:

- *Sede alternativa*

2.1056.1 WARM SITE

Sede alternativa que está parcialmente equipada con sistemas y comunicaciones para soportar operaciones durante un desastre.

2.1056.2 (EN) WARM SITE

Backup site which typically contains the data links and pre-configured equipment necessary to rapidly start operations, but does not contain live data. Thus commencing operations at a warm site will (at a minimum) require the restoration of current data. [CNSSI_4009:2010]

2.1056.3 (EN) WARM SITE

An environmentally conditioned workspace that is partially equipped with IT and telecommunications equipment to support relocated IT operations in the event of a significant disruption. [NIST-SP800-34:2002]

2.1056.4 (EN) WARM SITE

Backup site which is somewhere between a Hot Site and a Cold Site.

Typically contains the data links and pre-configured equipment necessary to rapidly start operations, but does not contain live data. Thus commencing operations at a warm site will (at a minimum) require the restoration of current data.

2.1057 WEB SERVICES SECURITY

Acrónimos: WS-Security

2.1057.1 WEB SERVICES SECURITY

Propuesta de un grupo de industrias para añadir elementos de seguridad a las transacciones web-services.

2.1057.2 (EN) WS-SECURITY

WS-Security (Web Services Security) is a proposed IT industry standard that addresses security when data is exchanged as part of a Web service. WS-Security is one of a series of specifications from an industry group that includes IBM, Microsoft, and Verisign. Related specifications include the Business Process Execution Language (BPEL), WS-Coordination, and WS-Transaction.

http://searchsoftwarequality.techtarget.com/glossary/

2.1058 WATERING HOLE

Ver

- *Phishing*

2.1058.1 WATERING HOLE

Estrategia de ataque informático. El atacante quiere atacar a un grupo en particular (organización, sector o región). El ataque consiste en tres fases:

1. Adivinar (u observar) los sitios web que el grupo utiliza a menudo.
2. Infectar uno o más de estos sitios web con *malware*.
3. Con el tiempo, algunos miembros del grupo objetivo se infectarán.

Esta estrategia basa su eficacia en la confianza que el grupo ha depositado en las páginas web que sus miembros visitan con asiduidad. Es eficaz incluso con grupos concienciados que son resistentes a *spear phishing* y otras formas de *phishing*.

2.1058.2 (EN) WATERING HOLE

Watering Hole is a computer attack.

The attacker wants to attack a particular group (organization, industry, or region). The attack consists of three phases:

1. Guess (or observe) which websites the group often uses.
2. Infect one or more of these websites with malware.
3. Eventually, some member of the targeted group will get infected.

Relying on websites the group trusts makes this strategy efficient even with groups that are resistant to spear phishing and other forms of phishing.

http://en.wikipedia.org/wiki/Watering_Hole

2.1059 WEP - WIRED EQUIVALENT PRIVACY

Acrónimos: WEP

Ver:

- *WPA - Wi-Fi Protected Access*
- *IEEE 802.11i*

2.1059.1 WEP - WIRED EQUIVALENT PRIVACY

Protocolo de cifrado de canales inalámbricos IEEE 802.11.

2.1059.2 WEP

Acrónimo de “wired equivalent privacy” (privacidad equivalente por cable). Algoritmo débil utilizado en el cifrado de redes inalámbricas. Expertos de la industria han informado que la conexión WEP presenta varias debilidades tan serias que puede descifrarse en minutos utilizando herramientas de software comunes. Consulte WPA.

http://es.pcisecuritystandards.org

2.1059.3 WEP

(Wired Equivalent Privacy) Protocolo para la transmisión de datos 'segura'. El cifrado puede ser ajustado a 128 bits, 64 bits o deshabilitado. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de cifrado. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits, cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red. También decir que este protocolo no es 100% seguro. Hay software dedicado a violar este cifrado, aunque requiere tiempo.

http://www.inteco.es/glossary/Formacion/Glosario/

2.1059.4 WIRED EQUIVALENT PRIVACY

WEP, acrónimo de Wired Equivalent Privacy, 1999 - es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona cifrado a nivel 2. Está basado en el algoritmo de cifrado RC4, y utiliza claves de 64 bits (40 bits más 24 bits del vector de inicialización IV) o de 128 bits (104 bits más 24 bits del IV).

http://es.wikipedia.org/wiki/WEP

2.1059.5 (EN) WEP

Acronym for “Wired Equivalent Privacy.” Weak algorithm used to encrypt wireless networks. Several serious weaknesses have been identified by industry experts such that a WEP connection can be cracked with readily available software within minutes. See WPA.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.1059.6 (EN) WIRED EQUIVALENT PRIVACY (WEP)

(N) A cryptographic protocol that is defined in the IEEE 802.11 standard and encapsulates the packets on wireless LANs. Usage: a.k.a. "Wired Equivalency Protocol". [RFC4949:2007]

2.1059.7 (EN) WIRED EQUIVALENT PRIVACY - WEP

A cryptographic protocol offering stream cipher encryption with a key length of 128 bits; it is defined within the IEEE 802.11 Wireless LAN specifications. [ISO-18028-4:2005]

2.1059.8 (EN) WEP - WIRED EQUIVALENT PRIVACY

WEP is a protocol for the encryption of wireless LAN traffic, for those using the 802.11 range of networking protocols.

2.1059.9 (EN) WIRED EQUIVALENT PRIVACY

Wired Equivalent Privacy (WEP) is a scheme that is part of the IEEE 802.11 wireless networking standard to secure IEEE 802.11 wireless networks (also known as Wi-Fi networks). Because a wireless network broadcasts messages using radio, it is particularly susceptible to eavesdropping.

http://en.wikipedia.org/wiki/WEP

2.1059.10 (FR) WEP

Acronyme de «Wired Equivalent Privacy», protocole WEP. Algorithme peu complexe, utilisé pour crypter des réseaux sans fil. De nombreuses faiblesses ont été identifiées par les experts du secteur; en effet, une connexion WEP peut être piratée en quelques minutes avec un logiciel prêt à l'emploi. Voir WPA.

http://fr.pcisecuritystandards.org/

2.1059.11 (FR) WEP

Wired Equivalent Privacy: processus de chiffrement (en partie imparfait à cause de la longueur insuffisante de la clé de chiffrement utilisée) devant permettre de disposer d'un niveau de confidentialité équivalent à celui des réseaux filaires dans l'utilisation de réseaux wireless.

http://www.cases.public.lu/functions/glossaire/

2.1060 WHALING

2.1060.1 WHALING

Es un ataque de ingeniería social, variante del spear phishing, que se caracteriza porque el fraude está dirigido a miembros concretos de la organización, principalmente ejecutivos de alto nivel, con el objeto de obtener sus claves, contraseñas y todo tipo de información confidencial que permita a los atacantes el acceso y control de los sistemas de información de la empresa.

La forma en que se comete el ataque bajo esta figura, es muy similar a la de los ataques de phishing. Se procede mediante el envío de correos electrónicos falsos que contienen enlaces a sitios web fraudulentos, con la diferencia de que en el caso de phishing el afectado no es necesariamente un directivo o alto cargo de la organización.

http://www.inteco.es/glossary/Formacion/Glosario/

2.1060.2 (EN) WHALING

Whaling is a type of fraud that targets high-profile end users such as C-level corporate executives, politicians and celebrities.

As with any phishing endeavor, the goal of whaling is to trick someone into disclosing personal or corporate information through social engineering, email spoofing and content spoofing efforts. The attacker may send his target an email that appears as if it's from a trusted source or lure the target to a website that has been created especially for the attack. Whaling emails and websites are highly customized and personalized, often incorporating the target's name, job title or other relevant information gleaned from a variety of sources.

The term whaling is a play-on-words because an important person may also be referred to as a "big fish." In gambling, for examples, whales describe high-stakes rollers who are given special VIP treatment.

Due to their focused nature, whaling attacks are often harder to detect than standard phishing attacks. In the enterprise, security administrators can help prevent success whaling expeditions by encouraging corporate management staff to undergo information security awareness training.

http://searchsecurity.techtarget.com/

2.1061 WHIRLPOOL - ALGORITMO RESUMEN (HASH)

Ver:

- *Hash*
- https://www.cosic.esat.kuleuven.be/nessie/
- [ISO-10118-3:2004]

2.1061.1 WHIRLPOOL - ALGORITMO RESUMEN (HASH)

Algoritmo para calcular resúmenes criptográficos. Produce resúmenes de 512 bits. Fue diseñado en el programa europeo NESSIE (New European Schemes for Signatures, Integrity and Encryption).

2.1061.2 (EN) WHIRLPOOL - HASH ALGORITHM

The Whirlpool hash algorithm was designed by Vincent Rijmen (co-designer of the AES encryption algorithm) and Paulo S. L. M. Barreto. The size of the output of this algorithm is 512 bits. The first version of Whirlpool, now called Whirlpool-0, was published in November 2000. The second version, now called Whirlpool-T, was selected for the NESSIE (New European Schemes for Signatures, Integrity and Encryption) portfolio of cryptographic primitives (a project organized by the European Union, similar to the AES contest). The third (final) version of Whirlpool was adopted by the International Organization for Standardization (ISO) and the IEC in the ISO/IEC ISO-10118-3:2004 international standard.

http://www.truecrypt.org/docs/whirlpool.php

2.1062 WIRETAPPING

2.1062.1 WIRETAPPING

Acceso a los datos que circulan por una red de comunicaciones.

2.1062.2 (EN) PASSIVE WIRETAPPING

The monitoring or recording of data while it is being transmitted over a communications link, without altering or affecting the data. [CNSSI_4009:2010]

2.1062.3 (EN) WIRETAPPING

Monitoring and recording data that is flowing between two points in a communication system.

http://www.sans.org/security-resources/glossary-of-terms/

2.1062.4 (EN) WIRETAPPING

(I) An attack that intercepts and accesses information contained in a data flow in a communication system. (See: active wiretapping, end-to-end encryption, passive wiretapping, secondary definition under "interception".) [RFC4949:2007]

2.1062.5 (EN) PASSIVE WIRETAPPING

(I) A wiretapping attack that attempts only to observe a communication flow and gain knowledge of the data it contains, but does not alter or otherwise affect that flow. (See: wiretapping. Compare: passive attack, active wiretapping.) [RFC4949:2007]

2.1063 WPA - WI-FI PROTECTED ACCESS

Acrónimos: WPA

Ver:

- *WEP - Wired Equivalent Privacy*
- *IEEE 802.11i*

2.1063.1 WPA/WPA2

Acrónimo de “WiFi Protected Access” (acceso protegido WiFi). Protocolo de seguridad creado para asegurar las redes inalámbricas. WPA es la tecnología sucesora de WEP. También se lanzó WPA2, tecnología sucesora de WPA.

http://es.pcisecuritystandards.org

2.1063.2 WPA / WPA2

El sistema WPA (Wireless Protected Access o Acceso Protegido Inalámbrico) es un sistema utilizado en el ámbito de las comunicaciones inalámbricas destinado a evitar que cualquier persona no expresamente autorizada pueda acceder a la red. Es un algoritmo que cifra las comunicaciones inalámbricas WiFi para evitar el acceso no autorizado por parte de terceros. Fue desarrollado por la WiFi Alliance como medio para corregir los errores que presentaba el anterior sistema, el algoritmo WEP (Wired Equivalent Privacy).

El algoritmo WPA incluía algunas de las funcionalidades del estándar 802.11i, que no quedarían plenamente integradas hasta la evolución del algoritmo en el llamado WPA2.

http://www.inteco.es/glossary/Formacion/Glosario/

2.1063.3 WI-FI PROTECTED ACCESS

WPA (Wi-Fi Protected Access - 1995 - Acceso Protegido Wi-Fi) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo WEP (Wired Equivalent Privacy - Privacidad Equivalente a Cableado). Los investigadores han encontrado varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado.

WPA fue creado por "The Wi-Fi Alliance" (La Alianza Wi-Fi).

http://es.wikipedia.org/wiki/WPA

http://www.wi-fi.org/

2.1063.4 (EN) WPA/WPA2:

Acronym for “WiFi Protected Access.” Security protocol created to secure wireless networks. WPA is the successor to WEP. WPA2 was also released as the next generation of WPA.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.1063.5 (EN) WI-FI PROTECTED ACCESS-2 (WPA2)

The approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard. For Federal government use, the implementation must use FIPS approved encryption, such as AES. [CNSSI_4009:2010]

2.1063.6 (EN) WIFI PROTECTED ACCESS - WPA

A specification for a security enhancement to provide confidentiality and integrity for wireless communications; it includes the temporal key implementation protocol (TKIP). WPA is the successor of WEP. [ISO-18028-4:2005]

2.1063.7 (EN) WPA - WI-FI PROTECTED ACCESS

WPA is a subset of the security aspects of the 802.11i wireless networking protocol. Using a per-packet, rather than a static, encryption key, it is more resistant to attack than is WEP. WPA2 is the full implementation of the 802.11i standard and uses a stronger encryption algorithm.

2.1063.8 (EN) WI-FI PROTECTED ACCESS

Wi-Fi Protected Access (WPA and WPA2) is a class of systems to secure wireless (Wi-Fi) computer networks. It was created in response to several serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared.

http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

2.1063.9 (FR) WPA/WPA2

Acronyme de «WiFi Protected Access», accès WiFi protégé. Protocole de sécurité créé pour sécuriser les réseaux sans fil. Le protocole WPA a remplacé le protocole WEP. Le WPA2 est la dernière génération de WPA.

http://fr.pcisecuritystandards.org/

2.1064 XER - XML ENCODING RULES

Acrónimos: XER

Ver:

- *ASN.1 - Abstract Syntax Notation One*
- *BER - Basic Encoding Rules*
- *CER - Canonical Encoding Rules*
- *DER - Distinguished Encoding Rules*

- *PER - Packet Encoding Rules*

2.1064.1 XER - XML ENCODING RULES

Conjunto de reglas para formatear en XML datos descritos en ASN.1.

2.1064.2 (EN) XER - XML ENCODING RULES

a set of ASN.1 encoding rules for formatting data in XML.

http://en.wikipedia.org/wiki/XML_Encoding_Rules

2.1065 XPATH INJECTION

Ver:

- *Inyección SQL*
- *Null injection*
- *LDAP injection*
- *Meta-Character Injection*

2.1065.1 XPATH INJECTION

Ataque a servidores web mediante peticiones XPath. Se trata de desconcertar al servidor cuando analiza el sentido de la consulta XPath, provocando la revelación de contenido XML al cual el cliente no debería tener acceso.

2.1065.2 (EN) XPATH INJECTION

XPath injection is an attack targeting Web sites that create XPath queries from user-supplied data. If an application embeds unprotected data into an XPath query, the query can be altered so that it is no longer parsed in the manner originally intended. This can be done by bypassing the Web site authentication system and extracting the structure of one or more XML documents in the site.

http://searchsoftwarequality.techtarget.com/glossary/

2.1066 ZOMBI

Ver:

- http://en.wikipedia.org/wiki/Zombie_computer
- *Ataque distribuido*
- *Botnet*

2.1066.1 ZOMBI

Persona que se supone muerta y que ha sido reanimada por arte de brujería, con el fin de dominar su voluntad.

DRAE. Diccionario de la Lengua Española.

2.1066.2 ZOMBIE

Es el nombre que se da a los ordenadores que han sido infectados de manera remota por un usuario malicioso con algún tipo de software que, al infiltrarse dentro del propio ordenador manipulado y sin consentimiento del propio usuario, un tercero puede hacer uso del mismo ejecutando actividades ilícitas a través de la Red. Su uso más frecuente es el envío de comunicaciones electrónicas no deseadas, así como la propagación de otros "virus informáticos", conocidos así en el lenguaje cotidiano, que constituyen uno de los grandes problemas de seguridad informática.

http://www.inteco.es/glossary/Formacion/Glosario/

2.1066.3 ZOMBI

Un ordenador generalmente infectado con un troyano de acceso remoto, capaz de recibir órdenes externas, y de actuar, generalmente en actividades maliciosas, sin el conocimiento de sus dueños.

http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

2.1066.4 (EN) ZOMBIE

(I) /slang/ An Internet host computer that has been surreptitiously penetrated by an intruder that installed malicious daemon software to cause the host to operate as an accomplice in attacking other hosts, particularly in distributed attacks that attempt denial of service through flooding. [RFC4949:2007]

2.1066.5 (EN) ZOMBIE

A program that is installed on a system to cause it to attack other systems. [NIST-SP800-83:2005]

2.1066.6 (EN) ZOMBIE COMPUTER

A computer attached to the Internet that has been compromised by a security cracker, a computer virus, or a trojan horse. Generally, a compromised machine is only one of many in a "botnet", and will be used to perform malicious tasks of one sort or another under remote direction. Most owners of zombie computers are unaware that their system is being used in this way. Because the vector tends to be unconscious, these computers are metaphorically compared to a zombie.

http://en.wikipedia.org/wiki/Zombie_computer

2.1066.7 (EN) ZOMBIE

In the West Indies, a zombie is a will-less, automaton-like person who is said to have been revived from the dead and must now do the will of the living. There are at least three usages of the term related to computers and the Internet.

1) In one form of denial of service attack, a zombie is an insecure Web server on which malicious people have placed code that, when triggered at the same time as other zombie servers, will launch an overwhelming number of requests toward an attacked Web site, which will soon be unable to service legitimate requests from its users. A pulsing zombie is one that launches requests intermittently rather than all at once.

A more recent use of zombies is to use them as an army of unwitting spam purveyors.

2) On the World Wide Web, a zombie is an abandoned and sadly out-of-date Web site that for some reason has been moved to another Web address. It's a ghost site that appears to have moved. Zombies contribute to linkrot.

3) In the Unix operating system world, developers sometimes use the term to refer to a program process that has died but hasn't yet given its process table entry back to the system.

http://searchsoftwarequality.techtarget.com/glossary/

2.1067 ZONA

2.1067.1 ZONA

Conjunto físico o lógico de elementos dentro de un mismo perímetro de seguridad. Los elementos de una zona disfrutan de una seguridad colectiva frente a agentes externos a su perímetro.

2.1067.2 (EN) ZONE

A zone refers to a logical boundary or enclave containing assets of like function and/or criticality, for the purposes of facilitating the security of common systems and services. See also: Enclave. [knapp:2014]

2.1067.3 (EN) ENCLAVE:

A logical grouping of assets. systems and/or services that defines and contains one (or more) functional groups. Enclaves represent network "zones" that can be used to isolate certain functions in order to more effectively secure them. [knapp:2014]

2.1067.4 (EN) ENCLAVE

Collection of information systems connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location. [CNSSI_4009:2010]

2.1067.5 (EN) ENCLAVE BOUNDARY

Point at which an enclave’s internal network service layer connects to an external network’s service layer, i.e., to another enclave or to a Wide Area Network (WAN). [CNSSI_4009:2010]

2.1068 ZONA DESMILITARIZADA (DMZ)

Acrónimos: DMZ

Ver:

- *Zona intermedia*

2.1068.1 DMZ

Abreviatura de “demilitarized zone” (zona desmilitarizada). Subred física o lógica que proporciona una capa de seguridad adicional a la red privada interna de una organización. La DMZ agrega una capa de seguridad de red adicional entre Internet y la red interna de una organización, de modo

que las partes externas sólo tengan conexiones directas a los dispositivos de la DMZ y no a toda la red interna.

http://es.pcisecuritystandards.org

2.1068.2 DMZ - ZONA DESMILITARIZADA

Zona con un nivel de protección intermedio entre dos áreas de seguridad diferentes. [CCN-STIC-400:2006]

2.1068.1 (EN) DEMILITARIZED ZONE (DMZ)

Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks. [CNSSI_4009:2010]

2.1068.2 (EN) DEMILITARIZED ZONE (DMZ)

(D) Synonym for "buffer zone". [RFC4949:2007]

2.1068.3 (EN) DEMILITARIZED ZONE (DMZ)

a perimeter network (also known as a screened sub-net) inserted as a neutral zone" between networks. It forms a security buffer zone. [ISO-18028-1:2006]

2.1068.4 (EN) DE-MILITARISED ZONE - DMZ

a separated area of a local or site network whose access is controlled by a specific policy using firewalls. A DMZ is not part of the internal network and is considered less secure. [ISO-18028-4:2005]

2.1068.5 (EN) DMZ

Abbreviation for "demilitarized zone." Physical or logical sub-network that provides an additional layer of security to an organization's internal private network. The DMZ adds an additional layer of network security between the Internet and an organization's internal network so that external parties only have direct connections to devices in the DMZ rather than the entire internal network.

https://www.pcisecuritystandards.org/security_standards/glossary.php

2.1068.6 (EN) DMZ (DEMILITARIZED ZONE)

A partially-protected zone on a network, not exposed to the full fury of the Internet, but not fully behind the firewall. This technique is typically used on parts of the network which must remain open to the public (such as a Web server) but must also access trusted resources (such as a database). The point is to allow the inside firewall component, guarding the trusted resources, to make certain assumptions about the impossibility of outsiders forging DMZ addresses.

http://www.watchguard.com/glossary/

2.1068.7 (EN) DMZ - DEMILITARIZED ZONE

A network segment taht is placed between the organization's network and a public network, usually the Internet.

2.1068.8 (EN) DEMILITARIZED ZONE (DMZ)

In computer security, in general a demilitarized zone (DMZ) or perimeter network is a network area (a subnetwork) that sits between an organization's internal network and an external network, usually the Internet. DMZ's help to enable the layered security model in that they provide subnetwork segmentation based on security requirements or policy. DMZ's provide either a transit mechanism from a secure source to an insecure destination or from an insecure source to a more secure destination. In some cases, a screened subnet which is used for servers accessbile form the outside is refered to as a DMZ.

http://www.sans.org/security-resources/glossary-of-terms/

2.1068.9 (FR) DMZ

Abréviation de «demilitarized zone», zone démilitarisée. Sous-réseau physique ou logique qui ajoute une couche de sécurité supplémentaire au réseau privé interne d'une organisation. La zone démilitarisée ajoute une couche supplémentaire de sécurité réseau entre Internet et le réseau interne d'une organisation, de sorte que les tiers externes puissent se connecter directement aux dispositifs de la zone démilitarisée, sans avoir accès à l'ensemble du réseau interne.

http://fr.pcisecuritystandards.org/

2.1068.10 (FR) ZONE DÉMILITARISÉE

Zone tampon d'un réseau située entre une zone de confiance, par exemple le réseau local, et une zone externe non digne de confiance, par exemple Internet. Les serveurs qui ne présentent pas d'informations sensibles et qui doivent accéder à Internet et être accessibles depuis Internet (par exemple les serveurs de mails, serveurs DNS, serveurs web, etc.) sont placés dans la DMZ. Le firewall gère et assure les contrôles sur cette zone.

http://www.cases.public.lu/functions/glossaire/

2.1068.11 (FR) DMZ - DEMILITARISED ZONE

Littéralement zone démilitarisée, zone intermédiaire (ou neutre) entre un réseau informatique interne sensible et devant être sécurisé et un réseau externe non maîtrisé (ex.: Internet). La DMZ est un sas dans lequel sont obligatoirement véhiculés les flux échangés entre les deux réseaux afin de garantir le caractère sain et inoffensif de ces flux.

Une DMZ est en général délimitée par un équipement de sécurité réseau (ex.: firewall).

Dans certains cas, on met en oeuvre des DMZs de nature différente:

- DMZ publique: recevant les flux en provenance de l'extérieur. Cette zone peut héberger le serveur de messagerie, le serveur Web et le DNS de l'entreprise.
- DMZ privée: recevant les flux en provenance du réseau interne et à destination de l'extérieur. Cette zone peut héberger un relais de messagerie sortant, un proxy-cache pour l'accès au Web.

2.1069 ZONA INTERMEDIA

Ver:

- *DMZ - Zona desmilitarizada*

2.1069.1 ZONA INTERMEDIA

Segmento de red que se interpone entre segmentos que operan bajo diferentes políticas de seguridad.

2.1069.2 (EN) BUFFER ZONE

(I) A neutral internetwork segment used to connect other segments that each operate under a different security policy. [RFC4949:2007]

3 ACRÓNIMOS

3DES	Triple DES
802.11i	IEEE 802.11i
A5	GSM voice encryption
AA	Attribute Authority
AAA	Authentication, Authorisation and Accounting
AaaS	Attack as a Service
AARL	Attribute Authority Revocation List
AC (es)	Autoridad de Certificación
AC (fr)	Autorité de Certification
AC	attribute certificate
ACL	Access Control List
ACRL	Attribute Certificate Revocation List
AES	Advanced Encryption Standard
AES-CCMP	AES – Counter Cipher Mode Protocol
AET	Advanced Evasion Technique
AfT	Authorization for Trial
AH	Authentication Header
ALARP	As Low As Reasonably Practical
ALE	Annualised Loss Expectancy
ANS (es)	Acuerdo de Nivel de Servicio
AOSTIC (es)	Autoridad Operativa del Sistema TIC
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threat
ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
ATO	Authorization to Operate
BCM	Business Continuity Management
BCP	Business Continuity Plan
BER	Basic Encoding Rules
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
BIOS	Basic Input Output System
Botnet	Robot net
BPC	Boundary Protection Component

BPD	Border Protection Device
BPS	Boundary Protection Service
BRP	Business Resumption plan
CA	Certification Authority
CAPEC	Common Attack Pattern Enumeration and Classification
CAPI	Cryptographic Application Programming Interface
CAPTCHA	Completely Automated Public Turing Test to tell Computers and Humans Apart
CARL	Certificate Authority Revocation List
CAST	Carlisle Adams and Stafford Tavares
CBC	Cipher Block Chaining
CC (es)	Criterios Comunes
CC	Common Criteria
CCE	Common Criteria Evaluation
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CEM	Common Evaluation Criteria
CER	Canonical Encoding Rules
CERT	Computer Emergency Response Team
CES (fr)	Contrat d´engagement de service
CFB	Cipher feedback mode
CHAP	Challenge-Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CIIP	Critical Information Infrastructure Protection
CIK	Crypto-Ignition Key
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIRC	Computer Incident Response Center
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CMAC	CBC-MAC
CMDB	Configuration Management Database
CMM	Capability Maturity Model
CMS	Cryptographic Message Syntax
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Explotation
CoF	Ciphering OFfset

COMPUSEC	Computers security
COMSEC	Communications security
CONOP	Concept of Operations
COOP	Continuity of Operations Plan
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSIRT	Computer Security Incident Response Team
CSMA/CD	Carrier Sense Multiple Access / Collision Detection
CSO	Chief Security Officer
CSRF	Cross-Site Request Forgery
CTAK	Cipher Text Auto-Key
CTR	Counter mode
CVE	Common Vulnerability and Exposures
CVSS	Common Vulnerability Scoring System
CWIN	Critical infrastructure Warning Information Network
DAC	Discretionary Access Control
DDoS	Distributed Denial of Service
DEA	Data Encryption Algorithm
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	Domain Name System Security Extension
DoS	Denial of Service
DRBG	Deterministic Random Bit Generator
DRES (es)	Declaración de Requisitos Específicos de Seguridad
DRM	Digital Rights Management
DRP	Disaster Recovery Plan
DRS (es)	Declaración de Requisitos de Seguridad
DRSI (es)	Declaración de Requisitos de Seguridad de la Interconexión
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
DTCC	Depository Trust and Clearing Corporation

EAC	Equivalent Annual Cost
EAL	Evaluation Assurance Level
EAR (es)	Esquema de Análisis de Riesgos
EAP	Extensible Authentication Protocol
ECB	Electronic codebook mode
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EGP	External Gateway Protocol
EMSEC	Emissions Security
ERC (es)	Equipo de Respuesta a Ciberincidentes
ERM	Enterprise Risk Management
ESP	Electronic Security Perimeter
ESP	Encapsulating Security Payload
ESSID	Extended Service Set Identifier
FAR	False Acceptance Rate
FDDI	Fiber Distributed Data Interface
FEAL	Fast Data Encipherment Algorithm
FHSS	Frequency Hoping Spread Spectrum
FIPS	Federal Information Processing Standard
FIRST	Forum of Incident Response and Security Teams
FISMA	Federal Information Security Management Act
FRAM IPSEC	Framework Internet Protocol Security
FRR	False Rejection Rate
GCM	Galois/Counter Mode
GIR (es)	Grupo Involucrado en la Resolución
GnuPG	GNU Privacy Guard
GPG	GNU Privacy Guard
GRC	Governance, Risk Management and Compliance
HDLC	High level Data Link Protocol
HIDS	Host Intrusion Detection System
HIPAA	Health Insurance Portability & Accountability Act of 1996
HIPS	Host Intrusion Prevention System
HMAC	Hash-based Message Authentication Code
HSM	Hardware Security Module
HTTPS	HTTP secure
I&A	Identification and Authentication
IANA	Internet Assigned Numbers Authority

IATO	Interim Approval to Operate
ICC	Integrated Circuit Card
ICMP	Internet Control Message Protocol
IDEA	International Data Encryption Algorithm
IDS	Intrusion Detection System
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
INFOSEC	INFormation SECurity
IOC	Indicator of Compromise
IODEF	Incident Object Description and Exchange Format
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol security
ISA	Interconnection Security Agreement
ISAKMP	Internet Security Association Key Management Protocol
ISMS	Information Security Management System
ISO	Information Security Officer
ITSEC	Information Technology Security Evaluation Criteria
IV	Initialization value
IV	Initialization vector
KAK	Key Auto-Key
KDC	Key Distribution Center
KDF	Key Derivation Function
KEK	Key Encrypting Key
KGC	Key Generation Centre
KMI	Key Management Infrastructure
KPK	Key Production Key
KRI	Key Risk Indicator
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LATO	Limited Authorization To Operate
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol

LLC	Logical Link Control
LOPD (es)	Ley Orgánica de Protección de Datos
MaaS	Malware as a Service
MAC	Message Authentication Code
MAC	Mandatory Access Control
MAC	Media Access Control
MAEC	Malware Attribute Enumeration and Characterization
Malware	malicious software
MAM	Mobile Application Management
MAN	Metropolitan Area Network
MCM	Mobile Content Management
MD2	Message Digest 2
MD4	Message Digest 4
MD5	Message Digest 5
MDM	Mobile Device Management
MEAM	Mobile Enterprise Application Management
MLS	Multilevel Security
MTA	Mail Transfer Address
MUA	Mail User Agent
NCSC	National CyberSecurity Center
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
NSA	National Security Agency
NTP	Network Time Protocol
NVD	National Vulnerability Database
NVRAM	Non Volatile Random Access Memory
OCSP	Online Certificate Status Protocol
OFB	Output feedback mode
OPSEC	Operations Security
OSPF	Open Shortest Path First
OTAR	On The Air Rekeying
OTP	One-time password
OWASP	Open Web Application Security Project
PAP	Password Authentication Protocol
PBAC	Policy Based Access Control
PCI	Peripheral Component Interconnect

PCI-DSS	Payment Card Industry Data Security Standard
PCMCIA	Personal Computer Memory Card International Association
PDCA	Plan Do Check Act
PEAP	Protected Extensible Authentication Protocol
PEM	Privacy Enhanced Mail
PenTest	Penetration Testing
PER	Packet Encoding Rules
PFS	Perfect Forward Secrecy
PFS	Public-Key Forward Secrecy
PGP	Pretty Good Privacy
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKC	Public Key Cryptography
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure
POP	Proof of Possession
POS (es)	Procedimientos Operativos de Seguridad
PP (es)	Perfil de protección
PP	Protection Profile
PPP	Point-to-Point Protocol
PPT (es)	Pliego de Prescripciones Técnicas
PPTP	Point-to-Point Tunneling Protocol
PRNG	Pseudo Random Number Generator
PSK	Pre-Shared Key
PUP	Potentially Unwanted Program
QoS	Quality of Service
RA	Registration Authority
RACF	Resource Access Control Facility
RADIUS	Remote Access Dial-In User Server
RAID	Redundant Arrays of Inexpensive Drives
RAID	Redundant Array of Independent Disks
RAID	Redundant Array of Inexpensive Disks
RAM	Random Access Memory
Ransomware	Ransom software
RARP	Reverse Address Resolution Protocol

RAT	Remote Access Tools
RBAC	Role-Based Access Control
RC-2	RC-2
RC-4	RC-4
RC-5	RC-5
RC-6	RC-6
RFI	Remote File Inclusion
RFID	Radio Frequency Identification
RIP	Routing Information Protocol
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RNG	Random Number Generator
Rogueware	Rogue software
ROM	Read Only Memory
RPF	Reverse Path Filtering
RPO	Recovery Point Objective
RPV (es)	Red Privada Virtual
RSA	Rivest Shamir Adelman
RSBAC	Rule Set Based Access Control
RT	Request Tracker
RT-IR	Request Tracker for Incident Response
RTO	Recovery Time Objective
RTTP	Real Time Transport Protocol
S/Key	Secure Key
S/MIME	Secure Multipurpose Mail Extension
SACM	Security Automation & Continuous Monitoring
SAFER	Secure And Fast Encryption Routine
SAI (es)	Sistema de Alimentación Ininterrumpida
SAML	Security Assertion Markup Language
SARA (es)	Sistema de Aplicaciones y Redes para las Administraciones
SATAN	Security Administrator Tool for Analyzing Networks
SECOPS	Security Operating Procedures
SEM	Security Event Manager
SEP	Search Engine Poisoning
SET	Secure Electronic Transactions
S-FTP	Secure-FTP
SFA	Security Fault Analysis
SFTP	Secure File Transfer Protocol

SGSI (es)	Sistema de Gestión de la Seguridad de la Información
SHA	Secure Hash Algorithm
SHIM	System Health and Intrusion Monitoring
SHS	Secure Hash Standard
SIEM	Security Information and Event Management
SIM	Security Information Management
SIM	Subscriber identification module
SISRS	system interconnection security requirements statement
SKIP	Simple Key Management for Internet Protocols
SLA	Service Level Agreement
SMB	Server Message Block
SMTP	Single Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOA	Source of Authority
SoA	Statement of Applicability
SOAP	Simple Object Access Protocol
SOC	Security Operations Center
SoD	Separation of Duties
SOX	Sarbanes-Oxley Act
SPKI	Simple Public Key Infrastructure
Spyware	Spy software
SQL	Structured Query Language
SRS	security requirements statement
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
SSO	System Security Officer
SSPR	Self-service password reset
SSRS	System-Specific Security Requirements Statement
ST	Security Target
STIC (es)	Seguridad de las Tecnologías de la Información y las Comunicaciones
STIX	Structured Thread Information eXpression
STP	Spanning Tree Protocol
TACACS	Terminal Access Controller Access Control System
TAN	Transaction Authentication Number

TAXII	Trusted Automated eXchange of Indicator Information
TCB	Trusted Computing Base
TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TDEA	Triple Data Encryption Algorithm
TDES	Triple DES
Telnet	Teletype Network
TEMPEST	Transient Electromagnetic Pulse Surveillance Technology
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TLP	Traffic Light Protocol
TLS	Transport Layer Security
TOE	Target Of Evaluation
TRANSEC	Transmissions security
TSA	Time-Stamping Authority
TSS	Time-Stamping Service
TTL	Time To Live
TTP	Trusted Third Party
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
UTM	Unified Threat Management
VA	Validation Authority
VPN	Virtual Private Network
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access (2)
WPAN	Wireless Personal Area Network
WS-Security	Web Services Security
XER	XML Encoding Rules
XML	eXtensible Markup Language
XSRF	Cross-Site Request Forgery
XSS	Cross-Site Scripting

4 REFERENCIAS

[BLP:1976]

Bell, D. E. and LaPadula, L. J., Secure Computer Systems: Unified Exposition and Multics Interpretation, MTR-2997 Rev. 1, MITRE Corp., Bedford, Mass., March 1976.

[BS25999-1:2006]

Business continuity management - Part 1: Code of practice. British Standard BS 25999-1:2006.

[CC:2006]

Common Criteria for Information Technology Security Evaluation, version 3.1, revision 1, September 2006.

Part 1 - Introduction and general model

Part 2 - Security functional requirements

Part 3 - Security assurance requirements

Also published as [ISO/IEC 15408].

[CCN-STIC-001:2006]

Políticas: Seguridad de las TIC en la Administración. Centro Criptológico Nacional, Guía STIC 001, 2006.

[CCN-STIC-002:2006]

Políticas: Definición de Criptología Nacional. Centro Criptológico Nacional, Guía STIC 002, 2006.

[CCN-STIC-003:2006]

Políticas: Uso Cifradores Certificados. Centro Criptológico Nacional, Guía STIC 003, 2006.

[CCN-STIC-101:2005]

Procedimientos: Procedimiento de Acreditación Nacional. Centro Criptológico Nacional, Guía STIC 101, 2005.

[CCN-STIC-103:2006]

Procedimientos: Catálogo de Productos con Certificación Criptológica Centro Criptológico Nacional, Guía STIC 103, 2006.

[CCN-STIC-150:2006]

Procedimientos: Evaluación y Clasificación Tempest de Cifradores con Certificación Criptológica. Centro Criptológico Nacional, Guía STIC 150 2006.

[CCN-STIC-151:2006]

Procedimientos: Evaluación y Clasificación Tempest de Equipos. Centro Criptológico Nacional, Guía STIC 151 2006.

[CCN-STIC-152:2006]

Procedimientos: Evaluación y Clasificación Zoning de Locales. Centro Criptológico Nacional, Guía STIC 152 2006.

[CCN-STIC-201:2006]

Normas: Organización y Gestión STIC. Centro Criptológico Nacional, Guía STIC 201 2006.

[CCN-STIC-202:2006]

Normas: Estructura y Contenido DRS. Centro Criptológico Nacional, Guía STIC 202 2006.

[CCN-STIC-203:2006]

Normas: Estructura y Contenido POS. Centro Criptológico Nacional, Guía STIC 203 2006.

[CCN-STIC-204:2006]

Normas: CO-DRS-POS Formulario Centro Criptológico Nacional, Guía STIC 204 2006.

[CCN-STIC-207:2006]

Normas: Estructura y Contenido del Concepto de Operación de Seguridad (COS). Centro Criptológico Nacional, Guía STIC 207 2006.

[CCN-STIC-301:2006]

Instrucciones Técnicas: Requisitos STIC. Centro Criptológico Nacional, Guía STIC 301 2006.

[CCN-STIC-302:2012]

Instrucciones Técnicas: Interconexión de CIS. Centro Criptológico Nacional, Guía STIC 302 2012.

[CCN-STIC-303:2006]

Instrucciones Técnicas: Inspección STIC. Centro Criptológico Nacional, Guía STIC 303 2006.

[CCN-STIC-400:2006]

Guías Generales: Manual de Seguridad de las TIC. Centro Criptológico Nacional, Guía STIC 400 2006.

[CCN-STIC-401:2007]

Guías Generales: Glosario y Abreviaturas. Centro Criptológico Nacional, Guía STIC 401 2007.

[CCN-STIC-403:2006]

Guías Generales: Gestión de Incidentes de Seguridad. Centro Criptológico Nacional, Guía STIC 403 2006.

[CCN-STIC-404:2006]

Guías Generales: Control de Soportes Informáticos. Centro Criptológico Nacional, Guía STIC 404 2006.

[CCN-STIC-405:2006]

Guías Generales: Algoritmos y Parmetros de Firma Electrnica Centro Criptológico Nacional, Guía STIC 405 2006.

[CCN-STIC-406:2006]

Guías Generales: Seguridad de Redes Inalámbricas. Centro Criptológico Nacional, Guía STIC 406 2006.

[CCN-STIC-407:2006]

Guías Generales: Seguridad de Telefonía Móvil. Centro Criptológico Nacional, Guía STIC 407 2006.

[CCN-STIC-408:2006]

Guías Generales: Seguridad Perimetral - Cortafuegos. Centro Criptológico Nacional, Guía STIC 408 2006.

[CCN-STIC-414:2006]

Guías Generales: Seguridad en Voz sobre IP. Centro Criptológico Nacional, Guía STIC 414 2006.

[CCN-STIC-430:2006]

Guías Generales: Herramientas de Seguridad. Centro Criptológico Nacional, Guía STIC 430 2006.

[CCN-STIC-431:2006]

Guías Generales: Herramientas de Análisis de Vulnerabilidades. Centro Criptológico Nacional, Guía STIC 431 2006.

[CCN-STIC-432:2006]

Guías Generales: Seguridad Perimetral - Detección de Intrusos. Centro Criptológico Nacional, Guía STIC 432 2006.

[CCN-STIC-435:2006]

Guías Generales: Herramientas de Monitorización de Tráfico en Red. Centro Criptológico Nacional, Guía STIC 435 2006.

[CCN-STIC-512:2006]

Guías para Entornos Windows: Gestin de Actualizaciones de Seguridad en Sistemas Windows. Centro Criptológico Nacional, Guía STIC 512 2006.

[CCN-STIC-611:2006]

Guías para otros entornos: Configuración Segura (SuSE Linux). Centro Criptológico Nacional, Guía STIC 611 2006.

[CCN-STIC-612:2006]

Guías para otros entornos: Configuración Segura (Debian). Centro Criptológico Nacional, Guía STIC 612 2006.

[CCN-STIC-614:2006]

Guías para otros entornos: Configuración Segura (RedHat Enterprise AS 4 y Fedora). Centro Criptológico Nacional, Guía STIC 614 2006.

[CCN-STIC-641:2006]

Guías para otros entornos: Plantilla configuración segura Routers CISCO. Centro Criptológico Nacional, Guía STIC 641 2006.

[CCN-STIC-642:2006]

Guías para otros entornos: Configuración Segura (Switches Enterasys). Centro Criptológico Nacional, Guía STIC 642 2006.

[CCN-STIC-671:2006]

Guías para otros entornos: Configuración Segura (Servidor Web Apache). Centro Criptológico Nacional, Guía STIC 671 2006.

[CCN-STIC-801:2010]

Esquema Nacional de Seguridad. Responsables y Funciones. 2010.

[CCN-STIC-903:2006]

Informes Técnicos: Centro Criptológico Nacional, Guía STIC 903 2006.

[CCN-STIC-951:2006]

Informes Técnicos: Centro Criptológico Nacional, Guía STIC 951 2006.

[CCN-STIC-952:2006]

Informes Técnicos: Centro Criptológico Nacional, Guía STIC 952 2006.

[CEM:2006]

Common Evaluation Methodology, version 3.1, revision 1, September 2006. Also published as [ISO/IEC 18405].

[CESID:1997]

Centro Superior de Información de la Defensa, Glosario de Términos de Criptología, Ministerio de Defensa, 3ª edición, 1997.

[CIAO:2000]

Critical Infrastructure Assurance Office, Practices for Securing Critical Information Assets, January 2000.

[CNSSI_4009:2010]

NATIONAL INFORMATION ASSURANCE (IA) GLOSSARY. Committee on National Security Systems. CNSS Instruction No. 4009. April 2010.

[COBIT:2006]

CobiT - Control Objectives, Management Guidelines, Maturity Models. IT Governance Institute. Version 4.0, 2006.

[CRAMM:2003]

CCTA Risk Analysis and Management Method (CRAMM), Version 5.0, 2003.

[CSS CA:2010]

Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada, Public Safety Canada/Sécurité publique Canada, Ottawa, Canada. 2010.

[CSS DE:2011]

Cyber Security Strategy for Germanu. Feb. 2011.

[CSS EU:2013]

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013.

[CSS NZ:2011]

New Zealand Cyber Security Strategy. June 2011.

[Directive-1999/93/EC:1999]

Directive 1999/93/EC of the European Parliament and the Council of 13 December 1999 on a Community framework for electronic signatures.

[DoD 5220:2006]

DoD 5220.22-M - NATIONAL INDUSTRIAL SECURITY PROGRAM, OPERATING MANUAL, February 2006

[EBIOS:2005]

EBIOS - Expression des Besoins et Identification des Objectifs de Sécurité

[ENS:2010]

Esquema Nacional de Seguridad. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. BOE de 29 de enero de 2010.

[ES EES:2011]

Estrategia Española de Seguridad. Una responsabilidad de todos. Gobierno de España. Madrid, 2011.

[FIPS-43-3:1999]

FIPS 43-3, Data Encryption Standard (DES), October 1999 (withdrawn May 19, 2005).

[FIPS-81:1980]

FIPS 81, DES Modes of Operation, December 1980 (withdrawn May 19, 2005).

[FIPS-140-2:2001]

FIPS 140-2, Security Requirements for Cryptographic Modules, May 2001.

[FIPS-186-2:2000]

FIPS 186-2, Digital Signature Standard (DSS), January, 2000.

[FIPS-199:2004]

FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004..

[FIPS-200:2006]

FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.

[H.235:2005]

ITU-T H.235, Implementors Guide for H.235 V3: Security and encryption for H-series (H.323 and other H.245- based) multimedia terminals. (5 August 2005).

[H.530:2002]

ITU-H H.530, Symmetric security procedures for H.323 mobility in H.510. (03/02).

[IRM-5239-8:1995]

IRM-5239-08A, U.S. Marine Corps, Compuer Security Procedures, 1995.

[ISDEFE-6:2009]

Seguridad Nacional y Ciberdefensa. Cuadernos Cátedra ISDEFE-UPM Nº 6. 2009.

[ISO Guide 73:2009]

Risk management -- Vocabulary, 2009.

[ISO-7498-2:1989]

ISO 7498-2:1989, ITU-T X.800, Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture, 1989.

[ISO-8732:1999]

ISO 8732:1988/Cor 1:1999, Banking - Key management (wholesale), 1999.

[ISO-8825-1:2002]

ISO/IEC 8825-1:2002, Information technology -- ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), 2002.

[ISO-9000_es:2000]

Sistemas de gestión de la calidad -- Conceptos y vocabulario, 2000.

[ISO-9594-8:2005]

ISO/IEC 9594-8:2005, Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks, 2005.

[ISO-9796-2:2002]

ISO/IEC 9796-2:2002, Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms, 2002.

[ISO-9797-1:1999]

ISO/IEC 9797-1:1999, Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher, 1999.

[ISO-9798-1:1997]

ISO/IEC 9798-1:1997, Information technology -- Security techniques -- Entity authentication -- Part 1: General, 1997.

[ISO-9798-5:2004]

ISO/IEC 9798-5:2004, Information technology -- Security techniques -- Entity authentication -- Part 5: Mechanisms using zero-knowledge techniques, 2004.

[ISO-10118-1:2000]

ISO/IEC 10118-1:2000, Information technology -- Security techniques -- Hash-functions -- Part 1: General, 2000.

[ISO-10118-3:2004]

ISO/IEC 10118-3:2004 Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions, 2004.

[ISO-10181-1:1996]

ISO/IEC 10181-1:1996, ITU-T X.810, Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview, 1996.

[ISO-10181-2:1996]

ISO/IEC 10181-2:1996, ITU-T X.811, Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework, 1996.

[ISO-11568:2005]

ISO 11568-1:2005, Banking -- Key management (retail) -- Part 1: Principles, 2005.

[ISO-11568-2:2005]

ISO 11568-2:2005, Banking -- Key management (retail) -- Part 2: Symmetric ciphers, their key management and life cycle, 2005.

[ISO-11568-4:2007]

ISO 11568-4:2007, Banking -- Key management (retail) -- Part 4: Asymmetric cryptosystems -- Key management and life cycle, 2007.

[ISO-11770-1:1996]

ISO/IEC 11770-1:1996, Information technology -- Security techniques -- Key management -- Part 1: Framework, 1996.

[ISO-11770-2:1996]

ISO/IEC 11770-2:1996, Information technology -- Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques, 1996.

[ISO-11770-3:2008]

ISO/IEC 11770-3:2008, Information technology -- Security techniques -- Key management -- Part 3: Mechanisms using asymmetric techniques, 2008.

[ISO-11770-4:2006]

ISO/IEC 11770-4:2006, Information technology -- Security techniques -- Key management -- Part 4: Mechanisms based on weak secrets, 2006.

[ISO-13335-1:2004]

ISO/IEC 13335-1:2004, Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management, 2004.

[ISO-13335-4:2000]

ISO/IEC 13335-4:2000, Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of safeguards, 2000.

[ISO-13888-1:2004]

ISO/IEC 13888-1:2004, IT security techniques -- Non-repudiation -- Part 1: General, 2004.

[ISO-14516:2002]

ISO/IEC TR 14516:2002, Information technology -- Security techniques -- Guidelines for the use and management of Trusted Third Party services, 2002.

[ISO-14888-1:1998]

ISO/IEC 14888-1:1998, Information technology -- Security techniques -- Digital signatures with appendix -- Part 1: General, 1998.

[ISO-14888-3:2006]

ISO/IEC 14888-3:2006, Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms, 2006.

[ISO-15292:2001]

ISO/IEC 15292:2001, Information technology - Security techniques - Protection Profile registration procedures, 2001.

[ISO-15443-1:2005]

ISO/IEC TR 15443:2005, Information technology -- Security techniques -- A framework for IT security assurance -- Part 1: Overview and framework, 2005.

[ISO-15782-1:2003]

ISO 15782-1:2003, Certificate management for financial services -- Part 1: Public key certificates, 2003.

[ISO-15816:2002]

ISO/IEC 15816:2002, Information technology -- Security techniques -- Security information objects for access control, 2002.

[ISO-15939:2002]

ISO/IEC 15939:2002, Software engineering -- Software measurement process, 2002.

[ISO-15945:2002]

ISO/IEC 15945:2002, Information technology -- Security techniques -- Specification of TTP services to support the application of digital signatures, 2002.

[ISO-15946-1:2002]

ISO/IEC 15946-1:2002, Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 1: General, 2002.

[ISO-15946-2:2002]

ISO/IEC 15946-2:2002, Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 2: Digital signatures, 2002.

[ISO-15946-3:2002]

ISO/IEC 15946-3:2002, Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 3: Key establishment, 2002.

[ISO-15946-4:2004]

ISO/IEC 15946-4:2004 Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 4: Digital signatures giving message recovery, 2004.

[ISO-15947:2002]

ISO/IEC TR 15947:2002, Information technology -- Security techniques -- IT intrusion detection framework, 2002.

[ISO-17799:2005]

ISO/IEC 17799:2005, Information technology -- Code of practice for information security management, 2005.

[ISO-18014-1:2002]

ISO/IEC IS 18014-2:2002, Information technology -- Security techniques -- Time-stamping services -- Part 1: Framework 2002.

[ISO-18014-2:2002]

ISO/IEC IS 18014-2:2002, Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens 2002.

[ISO-18028-1:2006]

ISO/IEC 18028-1:2006, Information technology -- Security techniques -- IT network security -- Part 1: Network security management, 2006.

[ISO-18028-2:2006]

ISO/IEC 18028-2:2006, Information technology -- Security techniques -- IT network security -- Part 1: Network security architecture, 2006.

[ISO-18028-3:2005]

ISO/IEC 18028-3:2005, Information technology -- Security techniques -- IT network security -- Part 3: Securing communications between networks using security gateways , 2005.

[ISO-18028-4:2005]

ISO/IEC 18028-4:2005, Information technology -- Security techniques -- IT network security -- Part 4: Securing remote access, 2005.

[ISO-18028-5:2006]

ISO/IEC 18028-5:2006, Information technology -- Security techniques -- IT network security -- Part 5: Securing communications across networks using virtual private networks, 2006.

[ISO-18031:2005]

ISO/IEC 18031:2005, Information technology -- Security techniques -- Random bit generation, 2005.

[ISO-18033-1:2005]

ISO/IEC 18033-1:2005, Information technology -- Security techniques -- Encryption algorithms -- Part 1: General, 2005.

[ISO-18033-2:2006]

ISO/IEC 18033-2:2006, Information technology -- Security techniques -- Encryption algorithms -- Part 2: Asymmetric ciphers 2006.

[ISO-18033-3:2005]

ISO/IEC 18033-3:2005, Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers 2005.

[ISO-18033-4:2005]

ISO/IEC 18033-4:2005, Information technology -- Security techniques -- Encryption algorithms -- Part 3: Stream ciphers 2005.

[ISO-18043:2006]

ISO/IEC 18043:2006, Information technology -- Security techniques -- Selection, deployment and operations of intrusion detection systems. 2006.

[ISO-18044:2004]

ISO/IEC TR 18044:2004, Information technology -- Security techniques -- Information security incident management, 2004.

[ISO-19790:2006]

ISO/IEC 19790:2006, Information technology -- Security techniques -- Security requirements for cryptographic modules. 2006.

[ISO-21827:2007]

ISO/IEC 21827:2002, Information technology -- Systems Security Engineering -- Capability Maturity Model (SSE-CMM), 2007.

[ISO-2382-8:1998]

ISO/IEC 2382-8:1998, Information technology -- Vocabulary -- Part 8: Security, 1998.

[ISO/IEC 27000:2014]

ISO/IEC 27000:2014, Information technology -- Security techniques -- Information security management systems – Overview and vocabulary, 2014.

[ISO-27032:2012]

ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity, 2012.

[ISO-27034-1:2011]

ISO/IEC 27034-1:2011, Information technology – Security techniques – Application security, 2011.

[ISO-27050:2015]

ISO/IEC CD 27050:2015, Information technology -- Security techniques -- Electronic discovery, 2015

[ITIL:2007]

ITIL V3 Glossary, 30 May 2007

[ITSEC:1991]

ITSEC - Information Technology Security Evaluation Criteria - Harmonized Criteria of France, Germany, the Netherlands, and the United Kingdom, Version 1.1, Published by Dept. of Trade and Industry, London, 1991.

[ITSEM:1993]

ITSEM - Information Technology Security Evaluation Manual. Commission of the European Communities. 1993.

[JP2-0:2013]

Joint Publication 2-0. Joint Intelligence. 22 October 2013.

[knapp:2014]

Knapp, Eric D.; Langill, Joel Thomas (2014-12-22). Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems (Kindle Locations 9173-9175). Elsevier Science.

[Ley 8/2011]

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

[Ley-59:2003]

Ley 59/2003, de 19 de diciembre, de firma electrónica.

[Magerit:1997]

Ministerio de Administraciones Públicas, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, MAP, versión 1.0, 1997.

[Magerit:2006]

Ministerio de Administraciones Públicas, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, MAP, versión 2.1, 2006.

[Magerit:2012]

Ministerio de Administraciones Públicas, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, MAP, versión 3.0, 2012.

[NATO AC/35-WP(2012)0007(IA)]

Glossary, 15 June, 2012.

[NERC:2014]

Glossary of Terms Used in NERC Reliability Standards, North American Electric Reliability Corporation, Updated October 1, 2014

[NIST-SP800-18:2006]

Guide for Developing Security Plans for Federal Information Systems. NIST Special Publication 800-18 Rev. 1, February 2006.

[NIST-SP800-27:2004]

Engineering Principles for Information Technology Security (A Baseline for Achieving Security), NIST Special Publication 800-27 Rev. A, June 2004.

[NIST-SP800-33:2001]

Underlying Technical Models for Information Technology Security, NIST Special Publication 800-33, December 2001.

[NIST-SP800-34:2002]

Contingency Planning Guide for Information Technology Systems, NIST Special Publication 800-34, June 2002.

[NIST-SP800-37:2004]

Guide for the Security Certification and Accreditation of Federal Information Systems, NIST Special Publication 800-37, May 2004.

[NIST-SP800-38A:2001]

Recommendation for Block Cipher Modes of Operation - Methods and Techniques, NIST Special Publication 800-38A, Dec 2001.

[NIST-SP800-38B:2005]

Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, May 2005.

[NIST-SP800-38C:2004]

Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, NIST Special Publication 800-38C, May 2004.

[NIST-SP800-38D:2007]

Recommendation for Block Cipher Modes of Operation: Galois/Counter, NIST Special Publication 800-38D, Nov 2007.

[NIST-SP800-53:2013]

Recommended Security Controls for Federal Information Systems, NIST Special Publication 800-53, Rev.4 April 2013.

[NIST-SP800-55:2003]

Security Metrics Guide for Information Technology Systems, NIST Special Publication 800-55, July 2003.

[NIST-SP800-57:2007]

Recommendation for Key Management - Part 1: General, NIST Special Publication 800-57, March 2007.

[NIST-SP800-60V2:2004]

Volume II: Appendixes to Guide for Mapping Types of Information and Information Systems to Security Categories, NIST Special Publication 800-60, June 2004.

[NIST-SP800-61:2004]

Computer Security Incident Handling Guide, NIST Special Publication 800-61, January 2004.

[NIST-SP800-63:2013]

Electronic Authentication Guideline, NIST Special Publication 800-63, Rev.2, 2013.

[NIST-SP800-77:2005]

Guide to IPsec VPNs NIST Special Publication 800-77, December 2005.

[NIST-SP800-83:2005]

Guide to Malware Incident Prevention and Handling, NIST Special Publication 800-83, November 2005.

[NIST-SP800-88:2006]

Guidelines for Media Sanitization, NIST Special Publication 800-88, September 2006.

[NIST-SP800-94:2007]

Guide to Intrusion Detection and Prevention Systems (IDPS) NIST Special Publication 800-94, February 2007.

[NIST-SP800-100:2006]

Information Security Handbook: A Guide for Managers, NIST Special Publication 800-100, October 2006.

[NIST7298:2011]

NIST IR 7298 Glossary of Key Information Security Terms, Revision 1, February, 2011.

[Octave:2003]

C. Alberts and A. Dorofee, Managing information Security Risks. The OCTAVE Approach, Addison Wesley, 2003.

[PE-CONS 60/14]

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93 CE, Bruselas, 16 de julio de 2014

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Brussels, 16 July 2014

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, Bruxelles, le 16 juillet 2014

[RFC4949:2007]

RFC4949, Internet Security Glossary, Version 2, August 2007

Each entry is preceded by a character -- I, N, O, or D -- enclosed in parentheses, to indicate the type of definition (as is explained further in Section 3):

"I" for a RECOMMENDED term or definition of Internet origin.

"N" if RECOMMENDED but not of Internet origin.

"O" for a term or definition that is NOT recommended for use in IDOCs but is something that authors of Internet documents should know about.

"D" for a term or definition that is deprecated and SHOULD NOT be used in Internet documents.

[Ribagorda:1997]

A. Ribagorda, Glosario de Términos de Seguridad de las T.I., Ediciones CODA, 1997.

[RiskIT-PG:2009]

The Risk IT Practitioner Guide. November 2009.

[TCSEC:1985]

TCSEC - Trusted Computer Systems Evaluation Criteria, DoD 5200.28-STD, Department of Defense, United States of America, 1985

[TDIR:2003]

Texas Department of Information Resources, Practices for Protecting Information Resources Assets, Revised September 2003.

[UNE Guía 73:2010]

Gestión del riesgo -- Vocabulario, 2010.

[UNE-71502:2004]

UNE 71502:2004, Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI), 2004.

[UNE-71504:2008]

UNE 71504:2008 - Metodología de análisis y gestión de riesgos de los sistemas de información, 2008.

[US-ESC:2012]

US ESC:2012, ELECTRICITY SUBSECTOR CYBERSECURITY. RISK MANAGEMENT PROCESS. U.S. Department of Energy. March 2012.

[US MSCO:2006]

US MSCO, The National Military Strategy for Cyberspace Operations. Dec. 2006.

[X.509:2005]

ITU-T X.509, ISI/IEC 9594-8, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. 08/2005.

[X.790:1995]

ITU-T X.790, X.790 Trouble management function for ITU-T applications. (11/95).

[X.805:2003]

ITU-T X.805, Security architecture for systems providing end-to-end communications, (10/03).

[X.810:1995]

ITU-T X.810, ISO/IEC 10181-1:1996, Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview. (11/95).