GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

CCN
CENTRO CRIPTOLÓGICO NACIONAL

GUÍA DE SEGURIDAD
(CCN-STIC 804)

ESQUEMA NACIONAL DE SEGURIDAD
GUÍA DE IMPLANTACIÓN

ens
Esquema Nacional de Seguridad

MARZO 2013

Edita:

Fecha de Edición: marzo de 2013

El Sr. José Antonio Mañas ha elaborado el presente documento y sus anexos.

El Ministerio de Hacienda y Administraciones Públicas ha financiado el desarrollo 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.

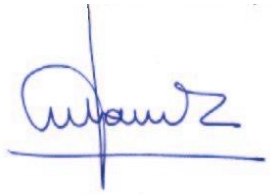
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia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

Marzo de 2013



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. Esta guía establece unas pautas de carácter general que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad sin entrar en casuísticas particulares. Se espera que cada organización las particularice para adaptarlas a su entorno singular.
2. El Esquema Nacional de Seguridad establece una serie de medidas de seguridad en su Anexo II que están condicionadas a la valoración (Anexo III) del nivel de seguridad en cada dimensión, y a la categoría (artículo 43) del sistema de información de que se trate. A su vez, la categoría del sistema se calcula en función del nivel de seguridad en cada dimensión.
3. Estas medidas constituyen un mínimo que se debe implementar, o justificar los motivos por los cuales no se implementan o se sustituyen por otras medidas de seguridad que alcancen los mismos efectos protectores sobre la información y los servicios.
4. Esta guía busca ayudar a los responsables de los sistemas para que puedan implantar rápida y efectivamente las medidas requeridas, sin perjuicio de que empleen recursos propios o recurran a proveedores y productos externos.
5. Para cada medida se proporciona:
   - una descripción más amplia que la proporcionada en el ENS,
   - referencias externas que ayuden a su comprensión y realización,
   - relación con medidas o controles en otros esquemas de seguridad,
   - relación con los principios básicos recogidos en el ENS,
   - indicaciones de lo que se considerará evidencia suficiente de cara a una evaluación de la seguridad

2. NIVELES DE MADUREZ

6. Es habitual el empleo de niveles de madurez para caracterizar la implementación de un proceso. El modelo de madurez1 permite describir las características que hacen un proceso efectivo, midiendo el grado o nivel de profesionalización de la actividad.
7. Los niveles identificados son los siguientes:

nivel	descripción
L0	Inexistente. Esta medida no está siendo aplicada en este momento.
L1	Inicial / ad hoc. Cuando la organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas. Pese a un naturaleza caótica, es más que no tener nada; pero es difícil prever la reacción ante una situación de emergencia.
L2	Repetible, pero intuitivo. Cuando existe un mínimo de planificación que, acompañada de la buena voluntad de las personas proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas.

[1] CMM - Capability Maturity Model, Carnegie Mellon University, CMU.

L3	Proceso definido. Se dispone un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general. Una diferencia importante entre el nivel 2 y el nivel 3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel 2, y que se gestiona en el nivel 3.
L4	Gestionado y medible. Cuando se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida.
L5	Optimizado. En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores.

8. Como regla general, se exigirá un nivel de madurez en las medidas en proporción al nivel de las dimensiones afectadas o de la categoría del sistema:

nivel	**categoría**	**nivel de madurez mínimo**
BAJO	BÁSICA	L2 - Repetible, pero intuitivo
MEDIO	MEDIA	L3 - Proceso definido
ALTO	ALTA	L4 - Gestionado y medible

3. [ORG] MARCO ORGANIZATIVO

9. Toda Organización necesita organizarse para poder asegurar el alcance de sus objetivos, definiendo funciones y estableciendo responsabilidades y canales de coordinación. Esta estructura permite la gestión día a día de las actividades rutinarias y la resolución ordenada de los incidentes que puedan sobrevenir.

10. Toda estructura organizativa necesita una evaluación constante y un análisis de la respuesta a los incidentes de forma que se aprende de la experiencia, se corrigen defectos o debilidades y se busca la excelencia por medio de la mejora continua.

11. La organización en materia de seguridad no puede sino estar alineada y servir a la misión del organismo, ajustándose a las necesidades de los servicios que se prestan.

12. La carencia de una organización formal y efectiva se traduce en unas prestaciones inciertas, cuyo resultado depende de la fortuna y el buen tino de los miembros de la organización, sin poder asegurar que se vayan a alcanzar los objetivos propuestos, ni tan siquiera pueda decirse que la Organización está bajo control.

13. Referencias

- Guía CCN-STIC 801 – Roles y funciones.
- Guía CCN-STIC 402 – Organización y Gestión para la Seguridad de los Sistemas TIC

- Guía CCN-STIC 201 – Organización y Gestión para la Seguridad de las STIC

- NIST SP 800-37 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST SP 800-39 - Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-53 rev3:
  - PM-2 - Senior Information Security Officer
- NIST SP 800-13 - An Introduction to Computer Security: The NIST Handbook
  - Chapter 3 – Roles and Responsibilities

- ISO/IEC 27002:2005:
  - 6 Organización para la seguridad de la información
  - 6.1 Organización interna
- ISO/IEC 27003 – ISMS Implementation Guidance
  - Annex B – Roles and responsibilities for Information Security

3.1. [ORG.1] POLÍTICA DE SEGURIDAD

14. La guía CCN-STIC 805 trata esta sección en detalle.

15. Son de especial relevancia los siguientes principios básicos:

- Artículo 5. La seguridad como un proceso integral.
- Artículo 9. Revaluación periódica.

16. También son dignos de mención los siguientes principios recogidos de la guía NIST SP800-27 (Rev. A):

- Principle 1. Establish a sound security policy as the “foundation” for design.
- Principle 24. Strive for simplicity.

17. Referencias:

- Guía CCN-STIC 805 – Política de Seguridad

- NIST SP 800-12 - An Introduction to Computer Security: The NIST Handbook
  - Chapter 5 – Computer Security Policy

- NIST SP 800-53 rev3:
  - [PM-2] Senior Information Security Officer
  - [PM-11] Mission / business Process Definition

- ISO/IEC 27002:2005:
  - 5.1 Política de seguridad de la información
  - 6.1.1 Compromiso de la Dirección con la seguridad de la información
  - 6.1.3 Asignación de responsabilidades relativas a la seguridad de la información
  - 15.1.1 Identificación de legislación aplicable

3.2. [ORG.2] NORMATIVA DE SEGURIDAD

18. Conjunto de documentos que, sin entrar en detalles, establecen la forma de afrontar un cierto tema en materia de seguridad. Definen la posición del organismo en aspectos concretos y sirven para indicar cómo se debe actuar en caso de que una cierta circunstancia no esté recogida en un procedimiento explícito o que el procedimiento pueda ser impreciso o contradictorio en sus términos.

19. A veces se denominan “policies” (en inglés).

20. A veces se denominan “standards” (en inglés).

21. Las normas deben centrarse en los objetivos que se desean alcanzar, antes que en la forma de lograrlo. Los detalles los proporcionarán los procedimientos. Las normas ayudan a tomar la decisión correcta en caso de duda.

22. Las normas deben describir lo que se considera uso correcto, así como lo que se considera uso incorrecto.

23. La normativa tiene carácter de obligado cumplimiento. Esto debe destacarse, así como las consecuencias derivadas de su incumplimiento (medidas disciplinarias).

24. Cada norma debe indicar la forma de localizar los procedimientos que se han desarrollado en la materia tratada. Es difícil que la norma cubra todos los procedimientos desarrollados.

25. Las normas deben escribirlas personas expertas en la materia, conocedoras de la postura de la Dirección, de las posibilidades y limitaciones de la tecnología correspondiente y con experiencia en los incidentes o situaciones típicas que pueden encontrarse los usuarios. Las normas deben ser revisadas por el departamento de asesoría legal, tanto para evitar el incumplimiento de alguna norma de rango superior, como para introducir registros que puedan ser requeridos como pruebas fehacientes en caso de conflicto.

26. Las normas deben ser realistas y viables. Deben ser concisas (sin perder precisión) y sin ambigüedades. Deben estar motivadas, ser descriptivas y definir puntos de contacto para su interpretación correcta.

27. Normativa típica:

    - control de acceso
    - protección de los autenticadores (contraseñas, tarjetas, etc)
    - puesto de trabajo despejado y equipos desatendidos
    - protección frente a software malicioso: virus, spyware, adware, …
    - desarrollo de aplicaciones (software)
    - instalación de aplicaciones (software)
    - acceso remoto
    - tele-trabajo
    - uso de portátiles
    - gestión de soportes de información removibles (tales como CD, llaves USB, etc)
    - tratamiento de la información impresa: copias, almacenamiento y destrucción
    - uso del correo electrónico
    - uso de la web
    - problemas de ingeniería social
    - criterios de clasificación de la información
    - copias de respaldo (*backups*)
    - …
    - relaciones con terceros (proveedores externos)

- acuerdos de confidencialidad
- cooperación preventiva
- resolución de incidencias

28. Son de especial relevancia los siguientes principios básicos:

- Artículo 7. Prevención, reacción y recuperación.
- Artículo 9. Revaluación periódica.

29. También son dignos de mención los siguientes principios recogidos de la guía NIST SP800-27 (Rev. A):

- Principle 13. Use common language in developing security requirements.
- Principle 24. Strive for simplicity.

30. Referencias:

- Guía CCN-STIC 821 – Normas de Seguridad

- The SANS Security Policy Project
  http://www.sans.org/resources/policies/

- NIST SP 800-53 rev3:
  - todos los capítulos incluyen un apartado sobre este asunto
  - [PL-4] Rules of Behavior
  - [SA-8] Security Engineering Principles
- NIST SP800-12 - An Introduction to Computer Security: The NIST Handbook

- ISO/IEC 27002:2005:
  - 7.1.3 Condiciones de uso de los activos
  - 11.4.1 Política de uso de los servicios de red
  - 11.7.2 Teletrabajo
  - 12.3.1 Política de uso de controles criptográficos
  - 15.1.2 Derechos de propiedad intelectual (IPR)
- ISO/IEC 27003 – ISMS Implementation Guidance
  - Annex D – Structure of documentation

Is it a Policy, a Standard or a Guideline?

What's in a name? We frequently hear people use the names "policy", "standard", and "guideline" to refer to documents that fall within the policy infrastructure. So that those who participate in this consensus process can communicate effectively, we'll use the following definitions.

A policy is typically a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point-specific, covering a single area. For example, an "Acceptable Use" policy would cover the rules and regulations for appropriate use of the computing facilities.

A standard is typically collections of system-specific or procedural-specific requirements that must be met by everyone. For example, you might have a standard that describes how to harden a Windows NT workstation for placement on an external (DMZ) network. People must follow this standard exactly if they wish to install a Windows NT workstation on an external network segment.

A guideline is typically a collection of system specific or procedural specific "suggestions" for best practice. They are not requirements to be met, but are strongly recommended. Effective security policies make frequent references to standards and guidelines that exist within an organization.

http://www.sans.org/security-resources/policies/

3.3. [ORG.3] PROCEDIMIENTOS OPERATIVOS DE SEGURIDAD

31. Conjunto de documentos que describen paso a paso cómo realizar una cierta actividad. Facilitan las tareas rutinarias evitando que se olviden pasos importantes. Lo que nunca debe ocurrir es que una cierta actividad sólo sepa hacerla una determinada persona; debe estar escrito cómo se hace para que la persona pueda ser remplazada.
32. A veces se denominan “guías”.
33. Cada procedimiento debe detallar:
    - en qué condiciones debe aplicarse
    - quién es el que debe llevarlo a cabo
    - qué es lo que hay que hacer en cada momento, incluyendo el registro de la actividad realizada
    - cómo identificar situaciones anómalas y cuál es mecanismo para escalar la situación
    - cómo se reportan deficiencias en los procedimientos
34. El conjunto de procedimientos debe cubrir un alto porcentaje (al menos el 80%) de las actividades rutinarias, así como aquellas tareas que se realizan con poca frecuencia pero exigen seguir unos pasos determinados muy precisos.
35. Nunca se puede decir que hay demasiados procedimientos. Cuantos más, mejor.
36. No obstante, es mejor no tener un procedimiento que tener un procedimiento erróneo o anticuado.
37. Debe existir un mecanismo para que los usuarios accedan rápidamente a la una versión actualizada de los procedimientos que les afectan. El uso de la intranet como repositorio de documentos es muy eficaz, aunque hay que prever algunas copias en papel para aquellas actividades que hay que realizar cuando falla intranet.

38. Debe existir un proceso para que los usuarios puedan reportar errores, inexactitudes o carencias en los procedimientos y se proceda a la revisión y actualización del procedimiento.

39. Son de especial relevancia los siguientes principios básicos:

    - Artículo 9. Revaluación periódica.

40. También son dignos de mención los siguientes principios recogidos de la guía NIST SP800-27 (Rev. A):

    - Principle 11. Protect against all likely classes of "attacks."
    - Principle 15. Strive for operational ease of use.
    - Principle 18. Provide assurance that the system is, and continues to be, resilient in the face of expected threats.
    - Principle 23. Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.
    - Principle 28. Ensure proper security in the shutdown or disposal of a system.

41. Referencias:

    - Guía CCN-STIC 822 – Procedimientos Operativos de Seguridad

    - NIST SP 800-53 rev3
        - todos los capítulos incluyen un apartado sobre este asunto

    - ISO/IEC 27002:2005:
        - 10.1.1 Documentación de los procedimientos de operación

3.4. [ORG.4] PROCESO DE AUTORIZACIÓN

42. Ningún sistema de información con responsabilidades sobre la información que maneja o los servicios que presta debería admitir elementos no autorizados por cuanto la libre incorporación de elementos socavaría de raíz la confianza en el sistema.

43. El ENS singulariza una serie de elementos, sin perjuicio de que se aplique siempre la regla de 'se requiere autorización previa':

    a. Utilización de instalaciones, habituales y alternativas.

    b. Entrada de equipos en producción, en particular, equipos que involucren criptografía.

    c. Entrada de aplicaciones en producción.

    d. Establecimiento de enlaces de comunicaciones con otros sistemas.

    e. Utilización de medios de comunicación, habituales y alternativos.

    f. Utilización de soportes de información.

    g. Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, PDA, u otros de naturaleza análoga.

    h. Utilización de equipos propiedad del usuario (BYOD – *Bring Your Own Device*)

44. El proceso de autorización requiere:

- que esté definido en la normativa de seguridad la persona o punto de contacto para autorizar un determinado componente o actuación
- que exista un formulismo (o sea, un formulario) para solicitar la autorización, indicando lo que se desea y la motivación; esta solicitud deberá incorporar los siguientes elementos:
    - descripción precisa del elemento o actuación para el que se solicita autorización
    - descripción precisa de las actividades para las que se requiere el nuevo componente
    - justificación de que nuevo componente no afecta a otras funcionalidades del sistema
    - si el nuevo componente introduce posibles vulnerabilidades (es decir, si expone al sistema a nuevas o renovadas amenazas), deberá anexarse un análisis de riesgos y las medidas que se toman para gestionarlo; este análisis de riesgos tendrá la intensidad proporcionada a la categoría del sistema, como se establece en [op.pl.1]
    - justificación de que no se viola ninguna normativa de seguridad
    - información de los procedimientos de seguridad que son aplicables al caso o, si fuere necesario, la necesidad de desarrollar algún nuevo procedimiento específico
- que se requiera la aprobación formal de la petición (o sea, la firma del responsable) antes de la actuación

45. Si se requieren nuevos procedimientos, la autorización puede ser temporal con un plazo límite para desarrollar los nuevos procedimientos y formalizar la autorización definitiva.

46. La autorización sólo cubrirá la utilización de los nuevos recursos para los objetivos explícitamente aprobados.

47. Son de especial relevancia los siguientes principios básicos:

- Artículo 9. Revaluación periódica.

48. También son dignos de mención los siguientes principios recogidos de la guía NIST SP800-27 (Rev. A):

- Principle 7. Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness
- Principle 15. Strive for operational ease of use.

49. Referencias:

- NIST SP 800-53 rev3
    - [PM-10] Security Authorization Process
    - [CA-3] Information System Connections
    - [CA-6] Security Authorization

- ISO/IEC 27002:2005:
    - 6.1.4 Proceso de autorización de recursos para el tratamiento de la información
    - 11.4.6 Control de conexión a la red
    - 12.4.1Control del software en explotación

- Manageable Network Plan
    - Milestone 7: Manage Your Network, Part II (Baseline Management)

4. [OP] MARCO OPERACIONAL

50. Medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

4.1. [OP.PL] PLANIFICACIÓN

51. Actividades previas a la puesta en explotación.

52. Son de especial relevancia los siguientes principios básicos:

- Artículo 5. La seguridad como un proceso integral.
- Artículo 6. Gestión de la seguridad basada en los riesgos.

53. También son dignos de mención los siguientes principios recogidos de la guía NIST SP800-27 (Rev. A):

- Principle 1. Establish a sound security policy as the "foundation" for design.
- Principle 2. Treat security as an integral part of the overall system design.
- Principle 5. Reduce risk to an acceptable level.
- Principle 7. Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness
- Principle 8. Implement tailored system security measures to meet organizational security goals

54. Referencias

- NIST SP 800-53 rev3:
  - [CA-5] Plan of Action and Milestones

4.1.1. [OP.PL.1] ANÁLISIS DE RIESGOS

55. El análisis de riesgos permite

1. validar el conjunto de medidas de seguridad implantado,
2. detectar la necesidad de medidas adicionales y
3. justificar el uso de medidas de protección alternativas.

56. Todo análisis de riesgos debe identificar y priorizar los riesgos más significativos a fin de conocer los riesgos a los que estamos sometidos y tomar las medidas oportunas, técnicas o de otro tipo

57. El análisis de riesgos debe ser una actividad recurrente; es decir, se debe mantener actualizado.

58. El aspecto formal exige que el análisis esté documentado y aprobado. La documentación debe incluir los criterios utilizados para seleccionar y valorar activos, amenazas y salvaguardas.

59. Un análisis de riesgos debe ser realizado:

- durante la especificación de un nuevo sistema, para determinar los requisitos de seguridad que deben incorporarse a la solución
- durante el desarrollo de un nuevo sistema, para analizar opciones

- durante la operación del sistema, para ajustar a nuevos activos, nuevas amenazas, nuevas vulnerabilidades y nuevas salvaguardas

60. Todo sistema opera bajo una situación de cierto riesgo residual. El riesgo residual debe estar documentado y aprobado por el responsable de la información y del servicio correspondiente(s).

Categoría BÁSICA

61. El análisis de riesgos puede ser informal; es decir, un documento que describa la valoración del sistema (Anexo I), las principales amenazas que cabe esperar y las medidas que se han tomado para enfrentarlas. Por último se hará una estimación del riesgo residual.

Categoría MEDIA

62. El análisis de riesgos debe ser semiformal, introduciendo tablas para analizar las amenazas que cabe esperar, las salvaguardas implantadas y el riesgo residual.

Categoría ALTA

63. El análisis debe ser formal, valorando activos, amenazas y salvaguardas para deducir el nivel de riesgo residual en el que se opera. El formalismo debe plasmarse en un modelo matemático que esté reconocido internacionalmente. Es conveniente emplear alguna herramienta de soporte para afrontar la actualización regular de los cálculos ante nuevas amenazas o cambios en el sistema-

64. Referencias:

- Magerit v3:2012 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información; Ministerio de Administraciones Públicas; Consejo Superior de Administración Electrónica.
  http:// administracionelectronica.gob.es/
- PILAR – Herramienta de Análisis y Gestión de Riesgos
  https://www.ccn-cert.cni.es/
- Guía CCN-STIC 470 Manual Herramienta de Análisis de Riesgos PILAR 4.1
  https://www.ccn-cert.cni.es/

- UNE 71504 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información; AENOR Agencia Española de Normalización
  http://www.aenor.es/

- NIST SP 800-53 rev3:
  - [RA-3] Risk Assessment
  - [PM-9] Risk Management Strategy
- NIST SP 800-30 - Risk Management Guide for Information Technology Systems
- NIST SP 800-37 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST SP 800-39 - Managing Risk from Information Systems: An Organizational Perspective
  http://csrc.nist.gov/publications/PubsSPs.html

- ISO/IEC 27002:2005:
  - cláusula 4. Evaluación y tratamiento de los riesgos
  - 12.1.1 Análisis y especificación de los requisitos de seguridad

- ISO/IEC 27005 - Information security risk management
  http://www.iso.org/

4.1.2. [OP.PL.2] ARQUITECTURA DE SEGURIDAD

65. Esta medida es básicamente documental y descriptiva de cómo es el sistema de información y el sistema de gestión del mismo.

66. La arquitectura de seguridad es elaborada bajo la dirección del Responsable del Sistema, y es aprobada por el Responsable de Seguridad.

67. Son de especial relevancia los siguientes principios básicos:

    - Artículo 7. Prevención, reacción y recuperación.
    - Artículo 8. Líneas de defensa.

68. También son dignos de mención los siguientes principios recogidos de la guía NIST SP800-27 (Rev. A):

    - Principle 3. Clearly delineate the physical and logical security boundaries governed by associated security policies.
    - Principle 6. Assume that external systems are insecure.
    - Principle 9. Protect information while being processed, in transit, and in storage.
    - Principle 11. Protect against all likely classes of "attacks."
    - Principle 15. Strive for operational ease of use.
    - Principle 16. Implement layered security (Ensure no single point of vulnerability).
    - Principle 20. Isolate public access systems from mission critical resources (e.g., data, processes, etc.).
    - Principle 21. Use boundary mechanisms to separate computing systems and network infrastructures.
    - Principle 22. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.
    - Principle 24. Strive for simplicity.
    - Principle 25. Minimize the system elements to be trusted.
    - Principle 30. Implement security through a combination of measures distributed physically and logically.
    - Principle 31 (formerly 15). Formulate security measures to address multiple overlapping information domains.
    - Principle 32. Authenticate users and processes to ensure appropriate access control decisions both within and across domains.

69. Referencias:

    - NIST SP 800-53 rev3:
        - [CA-3] Information System Connections
        - [PM-3] Information Security Resources
        - [PM-7] Enterprise Architecture
        - [PM-8] Critical Infrastructure Plan
        - [SA-5] Information System Documentation
        - [SA-9] External Information System Services
        - [CM-8] Information System Component Inventory
        - [SI-10] Information Input Validation
        - [SI-11] Error Handling

    - ISO/IEC 27002:2005:

- 6.2.2 Tratamiento de la seguridad en las relaciones con los clientes
- 10.7.4 Seguridad en la documentación del sistema
- 11.1.1 Política de control de acceso
- 12.1 Requisitos de seguridad

- ISO/IEC 27001 Requisitos de un sistema de gestión de la información.

- Manageable Network Plan
  - Milestone 1: Prepare to Document
  - Milestone 2: Map Your Network
  - Milestone 3: Protect Your Network (Network Architecture)
  - Milestone 4: Reach Your Network (Device Accessibility)
  - Milestone 8: Document Your Network

4.1.3. [OP.PL.3] ADQUISICIÓN DE NUEVOS COMPONENTES

70. La adquisición de nuevos componentes debe

- tener en cuenta el análisis de riesgos [op.pl.1]
- ajustarse a la arquitectura de seguridad [op.pl.2]
- prever los recursos necesarios, esfuerzo y medios económicos para
  - la implantación inicial
  - el mantenimiento a lo largo de su vida útil
  - atender a la evolución de la tecnología
- en todo momento se atenderá tanto a las necesidades técnicas como a la necesaria concienciación y formación de las personas que van a trabajar con los componentes

71. Son de especial relevancia los siguientes principios básicos:

- Artículo 9. Reevaluación periódica.

72. También son dignos de mención los siguientes principios recogidos de la guía NIST SP800-27 (Rev. A):

- Principle 10. Consider custom products to achieve adequate security.
- Principle 12. Where possible, base security on open standards for portability and interoperability.
- Principle 13. Use common language in developing security requirements.
- Principle 14. Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.
- Principle 15. Strive for operational ease of use.
- Principle 16. Implement layered security (Ensure no single point of vulnerability).
- Principle 22. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.
- Principle 24. Strive for simplicity.
- Principle 25. Minimize the system elements to be trusted.

73. Referencias:

- NIST SP 800-53 rev3:
  - [PL-1] Security Planning Policy and Procedures
  - [PL-2] System Security Plan
  - [PL-3] System Security Plan Update (withdrawn)
  - [PL-6] Security-Related Activity Planning
  - [SA-1] System and Services Acquisition Policy and Procedures

- [SA-2] Allocation of Resources
- [SA-3] Life Cycle Support
- [SA-4] Acquisitions
- [SA-8] Security Engineering Principles

- NIST SP 800-18 - Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-65 - Integrating IT Security into the Capital Planning and Investment Control Process

- ISO/IEC 27002:2005:
  - 10.3.2 Aceptación del sistema
  - 12.1.1 Análisis y especificación de requisitos

4.1.4. [OP.PL.4] DIMENSIONAMIENTO / GESTIÓN DE CAPACIDADES

Disponibilidad: nivel MEDIO

74. Se considerará evidencia suficiente del cumplimiento de esta medida:
    - existe un estudio previo a cada adquisición realizada o planificada que ofrece unas conclusiones respecto de la capacidad de los medios presentes o la necesidad de medios adicionales
    - el estudio previo es un documento escrito
    - [nivel ALTO] el estudio previo está aprobado por Dirección
75. Referencias:
    - NIST SP 800-53 rev3:
      - [SA-2] Allocation of Resources

    - ISO/IEC 27002:2005:
      - 10.3.1 Gestión de capacidades
      - 12.1.1 Análisis y especificación de los requisitos de seguridad

4.1.5. [OP.PL.5] COMPONENTES CERTIFICADOS

Categoría ALTA

76. Todas las palabras se quedan cortas para insistir en la conveniencia de recurrir a componentes probados, evaluados y, a ser posible, certificados. Desarrollar los propios componentes exige un apreciable nivel de formación, un considerable esfuerzo y una capacidad de mantenimiento de la seguridad frente a vulnerabilidades, defectos y nuevas amenazas. Todo esto se simplifica notablemente recurriendo a componentes de terceras partes siempre y cuando dichos componentes estén asegurados para protegernos de acuerdo a nuestras necesidades y frente a nuestras amenazas. Esto quiere decir que antes de adquirir un producto, por muy acreditado que esté, hay que cerciorarse de que cubre nuestras necesidades específicas.
77. El empleo de componentes certificados requiere
    - un esfuerzo preliminar de validación: idoneidad para el caso
    - un esfuerzo de implantación: adquisición y formación
    - y un esfuerzo continuo de actualizaciones para no perder las garantías iniciales

78. Referencias:

- Guía CCN-STIC 813 – Componentes Certificados en el ENS

- Guía CCN-STIC 103 – Catálogo de Productos Certificados
- NIST SP 800-53 rev3:
  - [SA-13] Trustworthiness

- NIST SP 800-23 - Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
- NIST SP 800-36 – Guide to Selecting Information Technology Security Products

- ISO/IEC 27002:2005:
  - 12.1.1 Análisis y especificación de los requisitos de seguridad

- Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información
  http://www.oc.ccn.cni.es
- Orden PRE/2740/2007 de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

- ISO/IEC 15408-1:2005 – Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model
- ISO/IEC 15408-2:2005 – Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements
- ISO/IEC 15408-3:2005 – Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements
- ISO/IEC 18045:2005 - Information technology – Security techniques – Methodology for IT security evaluation
- ISO/IEC TR 19791:2006 - Information technology – Security techniques – Security assessment of operational systems

4.2. [OP.ACC] CONTROL DE ACCESO

79. El control de acceso cubre el conjunto de actividades preparativas y ejecutivas para que una determinada entidad pueda, o no, acceder a un recurso del sistema para realizar una determinada acción.

80. Con el cumplimiento de todas estas medidas se garantiza que nadie accederá a recursos sin autorización. Además debe quedar registrado el uso del sistema ([op.exp.8]) para poder detectar y reaccionar a cualquier fallo accidental o deliberado.

81. El control de acceso que se implanta en un sistema real es un punto de equilibrio entre la comodidad de uso y la protección de la información. En sistemas de categoría básica, se prima la comodidad, mientras que en sistemas de categoría alta se prima la protección.

82. Estas medidas suelen venir recogidas en la literatura de seguridad bajo los epígrafes

- I&A – Identificación y Autenticación
- Control de Acceso

4.2.1. [OP.ACC.1] IDENTIFICACIÓN

83. Condición de aplicabilidad: cuando la autenticidad o la trazabilidad sean relevantes: nivel BAJO o superior.

84. Se debe asignar un identificador singular para cada entidad (usuario o proceso) que accede al sistema.

85. De esta manera:

- se puede saber quién recibe qué derechos de acceso
- se puede saber quién ha hecho qué, para corregir o para perseguir

86. La identificación de usuarios suele ir asociada a una "cuenta de usuario". A menudo se habla de "derechos de una cuenta" para referirse a los derechos del titular de la cuenta. Se dice que los derechos de un usuario son los de su cuenta en el sistema.

87. Se deben gestionar las cuentas de usuario:

88. las cuentas deben ser inhabilitadas cuando

- el usuario deja la organización o
- cesa en la función para la cual se requería la cuenta de usuario o
- la persona que lo autorizó da orden en contra
- las cuentas deben ser retenidas durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a una cuenta (periodo de retención)
- no deben existir 2 cuentas con el mismo identificador, de forma que no se puedan confundir dos usuarios ni se puedan imputar actividades a usuarios diferentes

89. Principios recogidos de la guía NIST SP800-27 (Rev. A):

- Principle 6. Assume that external systems are insecure.
- Principle 32. Authenticate users and processes to ensure appropriate access control decisions both within and across domains.
- Principle 33. Use unique identities to ensure accountability.

90. Referencias:

- NIST SP 800-53 rev3:
  - [AC-2] Account Management
  - [IA-2] User Identification and Authentication
  - [IA-3] Device Identification and Authentication
  - [IA-4] Identifier Management
  - [IA-8] Identification and Authentication (Non-organizational users)

- ISO/IEC 27002:2005:
  - 11.2.1 Registro de usuarios
  - 11.4.3 Identificación de equipos en la red
  - 11.5.2 Identificación y autorización de usuarios

4.2.2. [OP.ACC.2] REQUISITOS DE ACCESO

91. Principios recogidos de la guía NIST SP800-27 (Rev. A):

- Principle 6. Assume that external systems are insecure.

- Principle 20. Isolate public access systems from mission critical resources (e.g., data, processes, etc.).
- Principle 22. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.
- Principle 26. Implement least privilege.
- Principle 32. Authenticate users and processes to ensure appropriate access control decisions both within and across domains.
- Principle 33. Use unique identities to ensure accountability.

92. Referencias:

- NIST SP 800-53 rev3:
  - [SA-6] Software Usage Restrictions
  - [AC-3] Access Enforcement
  - [AC-4] Information Flow Enforcement
  - [AC-14] Permitted Actions without Identification or Authentication

- ISO/IEC 27002:2005:
  - 11.1.1 Política de control de acceso
  - 11.2.2 Gestión de privilegios
  - 11.5.4 Uso de los recursos del sistema
  - 11.6.1 Restricción del acceso a la información

- Manageable Network Plan
  - Milestone 5: Control Your Network (User Access)

4.2.3. [OP.ACC.3] SEGREGACIÓN DE FUNCIONES Y TAREAS

Integridad, confidencialidad, autenticidad o trazabilidad: nivel MEDIO

93. La segregación de funciones tiene dos objetivos

- prevenir frente a errores
- impedir el abuso de privilegios por parte de los usuarios autorizados

94. Debe documentarse un esquema de funciones y tareas en el que se contemplan las que son incompatibles en una misma persona. La incompatibilidad debe garantizar que para llevar a cabo un proceso o actividad crítica siempre se requieren al menos 2 personas.

95. Debe establecerse un procedimiento de asignación de personas a funciones y tareas a personas que garantice que no se viola el esquema anterior, ni cuando se asignan responsabilidades inicialmente, ni cuando se actualizan.

96. Deberá prestarse una especial atención a los roles asociados a cuentas de administración del sistema (administración de equipos, de aplicaciones, de comunicaciones, de seguridad), fragmentando las funciones administrativas entre varias personas cuando la categoría del sistema lo requiera. En todo caso el número de personas con derechos de administración debe ser lo más reducido posible sin menoscabo de la usabilidad del sistema.

97. Referencias:

- NIST SP 800-53 rev3:
  - [AC-5] Separation of Duties

- ISO/IEC 27002:2005:
  - 10.1.3 Segregación de tareas

- 10.1.4 Separación de los recursos de desarrollo, prueba y operación
- 15.3.1 Controles de auditoría
- 15.3.2 Protección de las herramientas de auditoría

4.2.4. [OP.ACC.4] PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

98. En la estructuración de los derechos de acceso se deben en cuenta las necesidades de cada usuario según su función en la organización y las tareas que tiene encomendadas.

99. La necesidad de acceso debe venir por escrito de parte del responsable de la información o proceso al que va a concedérsele acceso.

100. El reconocimiento de la necesidad de acceso debe ser reasegurado periódicamente, extinguiéndose cuando no se demuestre positivamente que la necesidad perdura.

101. Deberá prestarse una especial atención a las cuentas de administración del sistema (administración de equipos, de aplicaciones, de comunicaciones, de seguridad), estableciendo procedimientos ágiles de cancelación y mecanismos de monitorización del uso que se hace de ellas.

102. Referencias:

- NIST SP 800-53 rev3:
  - [AC-2] Account Management
  - [AC-6] Least Privilege

- ISO/IEC 27002:2005:
  - 11.2.2 Gestión de privilegios
  - 11.2.4 Revisión de derechos de acceso
  - 8.3.3 Retirada de derechos de acceso

- Manageable Network Plan
  - Milestone 5: Control Your Network (User Access)

4.2.5. [OP.ACC.5] MECANISMO DE AUTENTICACIÓN

103. Es el mecanismo que permite validar la identidad de un usuario. Es crítico por cuanto la identificación del usuario es en general fácilmente accesible.

104. Típicamente lo mecanismos de autenticación recurren

- a algo que se conoce (un secreto, por ejemplo una contraseña)
- a algo que se tiene (un objeto, por ejemplo una tarjeta o una llave)
- a algo que es propio del usuario (características biométricas)

105. A veces estos mecanismos se emplean por pares para dificultar la falsificación y ganar tiempo frente a la pérdida de alguno de los mecanismos:

- una tarjeta + un PIN
- una tarjeta + una característica biométrica
- una característica biométrica + una contraseña

106. Cada mecanismo tiene sus puntos débiles que deben atajarse por medio de normativa y procedimientos que regulen su uso, periodo de validez y gestión de incidencias tales como la pérdida por parte del usuario legítimo.

		nivel en I C A T		
		BAJO	MEDIO	ALTO
algo que se sabe	contraseñas claves concertadas PIN	ok	con cautela	no
algo que se tiene	tokens tarjetas	ok	ok	criptográficos
algo que se es	biometría	ok	ok	con doble factor

Contraseñas (secretos compartidos en general)

107. Características

- se pueden olvidar
- a veces los usuarios las escriben abriendo una oportunidad al conocimiento por robo
- si el número de posibilidades es reducido y el mecanismo de validación permite probar rápidamente, un atacante puede descubrir el secreto a base de pruebas
- nótese que la revelación de un secreto puede producirse son el conocimiento de la parte afectada por lo que el ladrón dispone de una amplia ventana de tiempo para actuar maximizando sus oportunidades
- la principal ventaja es que son baratas de implantar y fáciles de reemplazar en caso de pérdida

108. Al ser las contraseñas el mecanismo más usado con diferencia, es habitual encontrar normativa y procedimientos para generar, custodiar y tratar las incidencias al respecto. La seguridad depende fuertemente del bien hacer del usuario por lo que se impone su concienciación y formación básica sobre cómo cuidar sus secretos y cómo actuar en caso de fallo.

109. Se debe concienciar a los usuarios de los riesgos del uso de contraseñas e instruirles en cómo generarlas y custodiarlas.

110. Se debe verificar al establecerlas o regularmente que las contraseñas son robustas.

111. Se debe implementar un procedimiento de resolución de incidencias relacionadas con contraseñas; en particular debe haber un procedimiento urgente de suspensión de cuanta tras un robo.

Claves concertadas

112. Las claves concertadas son una alternativa al empleo de certificados. Se supone que será más cómodo, barato y fácil para el ciudadano usuario.

113. Se entienden por claves concertadas códigos generados previa identificación y autenticación del ciudadano por otros medios. Jurídicamente, el ciudadano expresa su voluntad de utilizar este mecanismo en el proceso de solicitud. Las claves concertadas deberán garantizar que el usuario no puede ser suplantado, ni por otro usuario, ni por la propia Administración. Para ello deberán

- ser razonablemente robustas frente a ataques de adivinación, tanto por estar asociadas a datos ampliamente conocidos del ciudadano, como por falta de aleatoriedad suficiente en la generación

- ser razonablemente robustas frente a ataques de diccionario
- ser razonablemente robustas frente a ataques de fuerza bruta; es decir, deben disponer de suficiente entropía
- impedir que el ciudadano pueda ser suplantado por su contraparte en la Administración
- seguir un procedimiento de generación que garantice la autenticidad del ciudadano
- seguir un procedimiento de comunicación al interesado que garantice que llega a la persona correcta
- disponer de un procedimiento de comunicación de pérdida o robo que suspenda inmediatamente la operatividad de la clave
- disponer de procedimientos de custodia de los datos de firma y verificación de la firma durante el periodo de validez de la información firmada, incluyendo los instantes de tiempo en que se genera, se suspende y se extingue la validez de la clave concertada

114. A fin de garantizar la robustez, la Administración deberá recurrir a generadores aleatorios que proporcionen suficiente entropía (que hayan tantas claves posibles que sea imposible probarlas todas una por una).

115. Es responsabilidad del usuario custodiar dichas claves de forma segura.

116. El proceso de generación debe garantizar la identidad del sujeto y dejar evidencia documental de las pruebas de identidad empleadas.

117. El procedimiento de distribución debe garantizar que sólo se le facilita al titular legítimo. Por ejemplo,

- usando una red privada virtual cifrada y autenticada (mp.com.2 y mp.com.3).
- por doble canal; ej. Internet + teléfono móvil
- por escrito en sobre cerrado

118. Deben generarse de forma aleatoria para

- resistir ataques de adivinación
- resistir ataques de diccionario

119. Deben ser suficientemente complejas para resistir ataques de fuerza bruta.

	BAJO	MEDIO	ALTO
número limitado de intentos	≥ 4 caracteres alfanuméricos del conjunto A-Z a-z 0-9 ~24 bits	≥ 5 caracteres alfanuméricos del conjunto A-Z a-z 0-9 ~30 bits	≥ 6 caracteres alfanuméricos del conjunto A-Z a-z 0-9 ~36 bits
sin límite en el número de intentos	≥ 8 caracteres alfanuméricos del conjunto A-Z a-z 0-9 ~48 bits	≥ 10 caracteres alfanuméricos del conjunto A-Z a-z 0-9 ~60 bits	≥ 12 caracteres alfanuméricos del conjunto A-Z a-z 0-9 ~72 bits
	< 1 año de validez	< 180 días de validez	< 90 días de validez

Llaves o tarjetas

120. Características

- se pueden perder, accidental o deliberadamente
- se pueden robar
- se pueden hacer copias

- en general, son caras y difíciles de reemplazar en caso de pérdida o deterioro

121. Uso habitual:

- autenticación frente a terminales (logon)
- acceso remoto y establecimiento de canales seguros
- activación de dispositivos criptográficos
- uso de dos o más tarjetas de activación
- acceso a instalaciones

122. Parece natural que se potencie el uso del DNI electrónico como mecanismo de autenticación de la persona. Este dispositivo proporciona medios de autenticación criptográficos acreditados. Frente a su uso no autorizado se protege con un PIN de activación. Nótese que el DNI electrónico sólo está capacitado por política para identificar a la persona; el resto del sistema de control y registro de acceso debe implementarse aparte.

123. Otras tarjetas de la administración pueden proporcionar funciones de autenticación del usuario asociadas a las funciones propias de su cargo en el organismo.

124. Guía CCN-STIC 807 Criptografía (claves de autenticación y certificados electrónicos)

tipo	nivel BAJO	nivel MEDIO	nivel ALTO
clave pública			
RSA	≥ 1.024 bits	≥ 1.024 bits	≥ 2.048 bits
curvas elípticas	≥ 224 bits	≥ 224 bits	≥ 256 bits
función hash			
SHA-1 (DNIe)	160 bits (PCP)	160 bits (PCP)	160 bits (PCP)
SHA-2	≥ 256 bits	≥ 256 bits	≥ 256 bits
SHA-3	≥ 256 bits	≥ 256 bits	≥ 256 bits

PCP – permitido a corto plazo

Biometría

125. Características

- normalmente no son secretas, y su robustez depende de que no se pueda suplantar al usuario; esto depende mucho del mecanismo concreto, pero algunos permiten técnicas de reproducción, un tanto avanzadas
- en general los dispositivos son costosos
- es difícil de reemplazar en caso de pérdida del control por parte del usuario legítimo

126. Uso habitual:

- En la autenticación frente a terminales:
  - reconocimiento de huella dactilar
  - reconocimiento facial
  - como doble factor se puede una contraseña o un PIN

- En el acceso a locales o áreas:
  - reconocimiento de la mano
  - reconocimiento del iris o del fondo del ojo
  - como doble factor se puede utilizar una tarjeta o un PIN

127. Se deben elegir productos certificados [op.pl.5] siempre que sea posible.

128. Referencias:

- NIST SP 800-53 rev3:
  - [IA-2] Identification and Authenticaton (Organizational Users)
  - [IA-3] Device Identification and Authentication
  - [IA-5] Authenticator management
  - [IA-7] Cryptographic Module
  - [IA-8] Identification and Authentication (Non-organizational users)

- ISO/IEC 27002:2005:
  - 11.2.3 Gestión de contraseñas
  - 11.3.1 Uso de contraseñas
  - 11.5.2 Identificación y autorización de usuarios
  - 11.5.3 Gestión de contraseñas

- Password Policy, SANS Institute
  http://www.sans.org/resources/policies/Password_Policy.pdf
- Guía CCN-STIC 436 - Herramientas de Análisis de Contraseñas
- Guía CCN-STIC 490 Dispositivos biométricos de huella dactilar

4.2.6. [OP.ACC.6] ACCESO LOCAL (LOCAL LOGON)

Integridad, confidencialidad, autenticidad o trazabilidad: nivel BAJO

129. La mayor parte de las medidas requeridas se pueden conseguir simplemente configurando los puestos de usuario según se indica.

Integridad, confidencialidad, autenticidad o trazabilidad: nivel MEDIO

130. El requisito de que en ciertos puntos se requiera una identificación singular no es alcanzable por medio de configuración del puesto del usuario, sino que requiere instrumentar workflow de los procesos. Como regla general, estos puntos deben ser pocos y el sistema no debe memorizar la identidad del usuario, sino que debe verificarla cada vez.

131. Como ejemplo, piense en la firma electrónica que se exige en banca por Internet cada vez que queremos realizar una transferencia; esta 'firma' complementa la identificación y autenticación de la sesión de usuario. Esta verificación puntual acota la ventana de riesgo ate un posible robo de sesión.

Integridad, confidencialidad, autenticidad o trazabilidad: nivel ALTO

132. Referencias:

- NIST SP 800-53 rev3:
  - [AC-7] Unsuccessful Login Attempts
  - [AC-8] System Use Notification
  - [AC-9] Previous Login Notification
  - [IA-6] Authenticator Feedback
  - [SI-11] Error Handling

- ISO/IEC 27002:2005:
  - 11.5.1 Procedimientos de inicio de sesión (logon)

- 11.5.6 Limitación del tiempo de conexión

4.2.7. [OP.ACC.7] ACCESO REMOTO (REMOTE LOGIN)

133. El acceso remoto es fuente de numerosos problemas porque no puede suponer el mismo nivel de controles de seguridad física que en las instalaciones corporativas. Por ello conviene tener reglas específicas respecto de qué se puede hacer y qué se puede hacer desde un acceso remoto. E incluso dentro de lo que está autorizado, hay que esmerarse en el cuidado del proceso de identificación y autenticación para prevenir la suplantación de la identidad de un usuario autorizado.

Integridad, confidencialidad, autenticidad y trazabilidad: nivel BAJO

134. Se exige establecer un mecanismo robusto de identificación y autenticación según [op.acc.6]

135. Prácticamente se exige establecer una red privada virtual, VPN, según [mp.com.2] y [mp.com.3].

Integridad, confidencialidad, autenticidad y trazabilidad: nivel MEDIO

136. Se debe redactar una política que rija lo que se puede hacer remotamente: qué aplicaciones se pueden usar, qué datos son accesibles y en qué condiciones estos datos pueden almacenarse en el dispositivo externo de acceso.

137. La política también debe establecer límites al tiempo que puede estar abierta una sesión y e imponer un tiempo máximo para cerrar sesiones inactivas.

138. Además de redactar la política, hay que imponerla. Esto es casi imposible si el dispositivo es del usuario (BYOD) y en general si el usuario tiene derechos de administrador del equipo. Es por ello que se procurará que el equipo remoto sea propiedad del organismo, esté configurado por el organismo y el usuario no tenga derechos de administrador.

139. A fin de limitar lo que se puede hacer en remoto, se debe establecer un filtro, bien en el servidor, bien en el propio cliente.

140. Si las limitaciones se imponen en el servidor, haremos que el usuario acceda a un segmento de red separado del núcleo corporativo y entre el segmento de acceso remoto y el núcleo estableceremos un cortafuegos interno que sólo permita las aplicaciones y protocolos autorizados.

141. Si las limitaciones se imponen en el equipo cliente, instalaremos un cortafuegos personal, configurado por el organismo, que establezca las limitaciones correspondientes.

142. En ambos escenarios se debe considerar la oportunidad de instalar una función DLP que monitorice los datos que viajan por la red.

143. En todos los casos se deben activar los registros de actividad y analizar regularmente que se cumple la política autorizada. Considere la oportunidad de un sistema SIEM que levante alarmas y centralice su reporte.

144. Referencias:

- http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf
- http://www.sans.org/security-resources/policies/Remote_Access.pdf
- http://www.sans.org/reading_room/whitepapers/vpns/remote-access-vpn-security-concerns-policy-enforcement_881
- NIST SP 800-53 rev3:

- [AC-17] Remote Access
- [AC-20] Use of External Information Systems
- [MA-4] Remote Maintenance

- ISO/IEC 27002:2005:
  - 11.4.2 Autenticación de usuarios en acceso remoto
  - 11.4.4 Puertas de diagnóstico y configuración remota
  - 11.5.6 Limitación del tiempo de conexión
  - 11.7.2 Teletrabajo

4.3. [OP.EXP] EXPLOTACIÓN

4.3.1. [OP.EXP.1] INVENTARIO DE ACTIVOS

145. El inventario debe cubrir todo el dominio de seguridad del responsable de la seguridad del sistema de información, hasta alcanzar los puntos de interconexión y los servicios prestados por terceros. La granularidad debe ser suficiente para cubrir las necesidades de reporte de incidentes y para hacer un seguimiento, tanto formal (auditorías) como reactivo en el proceso de gestión de incidentes.

- Identificación del activo: fabricante, modelo, número de serie
- Configuración del activo: perfil, política, software instalado
- Software instalado: fabricante, producto, versión y parches aplicados
- Equipamiento de red: MAC, IP asignada (o rango)
- Ubicación del activo: ¿dónde está?
- Propiedad del activo: persona responsable del mismo

146. Referencias:

- NIST SP 800-53 rev3:
  - [PM-5] Information System Inventory
  - [CM-8] Information System Component Inventory

- ISO/IEC 27002:2005:
  - 7.1.1 Inventario de activos
  - 7.1.2 Propiedad de los activos

4.3.2. [OP.EXP.2] CONFIGURACIÓN DE SEGURIDAD

147. Todos los sistemas deben ser configurados de forma sistemática antes de entrar en producción. El organismo debe elaborar unos poco perfiles de configuración para las diferentes actividades a que pueden ser dedicados. Típicamente no llegará a la docena de perfiles, siendo típicos los siguientes:

- usuarios normales (uso administrativo)
- atención a clientes
- gestión de proveedores (incluidos bancos)
- desarrollo
- operadores y administradores (técnicos de sistemas)
- responsable de seguridad (consola de configuración)
- auditoría

148. La medida en instrumenta por medio de unas checklists que se deben aplicar sistemáticamente a cada equipo antes de entrar en producción.

149. Básicamente, en todos los perfiles se debe bloquear la opción de que el usuario pueda cambiar la configuración del sistema o pueda instalar nuevos programas o nuevos periféricos (drivers)

150. La configuración de seguridad debe incluir un perfil básico de auditoría de uso del equipo.

151. Se considerará evidencia suficiente del cumplimiento de esta medida:

- existe un procedimiento de eliminación de cuentas o contraseñas estándar
- existen perfiles avalados por una autoridad reconocida
- existen procedimientos de configuración que garanticen la aplicación de dichos perfiles
- existe un procedimiento de revisión periódica de los perfiles
- existe un procedimiento de revisión de perfiles atendiendo a la publicación de vulnerabilidades de los sistemas

152. Referencias:

- Serie CCN-STIC 500 Guías para Entornos Windows
- Serie CCN-STIC 600 Guías para otros Entornos

- FDCC - Federal Desktop Core Configuration
  http://nvd.nist.gov/fdcc/index.cfm

- USGCB - The United States Government Configuration Baseline
  http://usgcb.nist.gov/

- NIST SP 800-53 rev3:
  - [CM] Configuration management
  - [CM-2] Baseline Configuration
  - [CM-6] Configuration Settings
  - [CM-7] Least Functionality

- Manageable Network Plan
  - Milestone 7: Manage Your Network, Part II (Baseline Management)

4.3.3. [OP.EXP.3] GESTIÓN DE LA CONFIGURACIÓN

Categoría MEDIA

153. Se considerará evidencia suficiente del cumplimiento de esta medida la existencia de un procedimiento para modificar la configuración del sistema que exige

- la aprobación del responsable,
- la documentación del cambio,
- pruebas de la seguridad del sistema bajo la nueva configuración
  - se mantiene la regla de funcionalidad mínima (Artículo 19 y [op.exp.2])
  - se mantiene la regla de seguridad por defecto (Artículo 19 y [op.exp.2])
  - se mantiene el control de acceso (Artículo 16 y [op.acc.4])
  - se afrontan las vulnerabilidades identificadas (Artículo 20 y [op.exp.4])
  - se gestionan las incidencias (Artículo 24 y [op.exp.7])
- la retención de la configuración previa por un tiempo prestablecido

- se realizan copias de seguridad de la configuración de los diferentes componentes, cubriendo al menos la configuración actual y la inmediata anterior

154. Referencias:

- Ver [op.exp.2]

4.3.4. [OP.EXP.4] MANTENIMIENTO

155. Se considerará evidencia suficiente del cumplimiento de esta medida la existencia de procedimientos para llevar a cabo las especificaciones del fabricante en cuanto a mantenimiento.

156. Referencias:

- NIST SP 800-53 rev3:
  - [MA-2] Controlled Maintenance
  - [MA-3] Maintenance Tools
  - [MA-4] Non-local Maintenance
  - [MA-5] Maintenance Personnel
  - [MA-6] Timely Maintenance
  - [SI-2] Flaw Remediation
  - [SI-5] Security Alerts, Advisories, and Directives
- NIST SP 800-40 - Creating a Patch and Vulnerability Management Program
- ISO/IEC 27002:2005:
  - 9.2.4 Mantenimiento de equipos
  - 12.4.1 Control de programas en producción
  - 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
  - 12.6.1 Control de vulnerabilidades técnicas
- Manageable Network Plan
  - Milestone 6: Manage Your Network, Part I (Patch Management)

4.3.5. [OP.EXP.5] GESTIÓN DE CAMBIOS

Categoría MEDIA

157. Se considerará evidencia suficiente del cumplimiento de esta medida:

- existe un mecanismo para recibir regularmente los anuncios de los fabricantes
- existe un procedimiento para evaluar el impacto del cambio
- existe un procedimiento para implantar los cambios con urgencia proporcionada al riesgo que implica su no aplicación

158. Debe existir un procedimiento para cambiar componentes del sistema que requiere

- la aprobación del responsable,
- la documentación del cambio,
- pruebas de la seguridad del sistema tras el cambio
- la retención de una copia del componente previo por un tiempo prestablecido
- copias de seguridad de los componentes software, cubriendo al menos la versión actual y la inmediata anterior
- se actualiza el inventario de activos

- se actualizan los procedimientos operativos relacionados con el componente actualizado
- se actualiza el plan de continuidad de negocio [si existe tal plan; ver [op.cont]

159. Referencias:

- NIST SP 800-53 rev3:
  - [CA-7] Continuous Monitoring
  - [CM-3] Configuration Change Control
  - [CM-5] Access Restrictions for Change
  - [MA-2] Controlled Maintenance
  - [SI-2] Flaw Remediation

- ISO/IEC 27002:2005:
  - 10.1.2 Gestión de cambios
  - 10.2.3 Gestión del cambio en los servicios prestados por terceros
  - 12.4.1 Control de programas en producción
  - 12.5.1 Procedimientos de control de cambios
  - 12.5.3 Restricciones a los cambios en los paquetes de software

4.3.6. [OP.EXP.6] PROTECCIÓN FRENTE A CÓDIGO DAÑINO

160. Se considerará evidencia suficiente del cumplimiento de esta medida:

- los programas de protección arriba mencionados existes, estás activados y actualizados de forma automática
- la cobertura de los programas de protección alcanza a todos los equipos: servidores y puestos de trabajo, bien sea por instalación local o en modo cliente-servidor
- el correo entrante y saliente se analiza para detectar y eliminar contenidos activos indeseables
- los puestos de usuario se configuran para bloquear código dañino

161. Referencias:

- Guía CCN-STIC 827 Procedimientos de actuación ante código dañino

- NIST SP 800-53 rev3:
  - [SI-3] Malicious Code Protection
  - [SI-8] Spam Protection
  - [SC-18] Mobile Code

- NIST SP 800-28 - Guidelines on Active Content and Mobile Code
- NIST SP 800-83 - Guide to Malware Incident Prevention and Handling

- ISO/IEC 27002:2005:
  - 10.4.1 Controles contra el código malicioso

4.3.7. [OP.EXP.7] GESTIÓN DE INCIDENCIAS

Categoría MEDIA

162. Hay que establecer un proceso de gestión que instrumente las siguientes actividades

- reporte de incidencias, reales o sospechadas, detectadas por los usuarios

- reporte de incidencias reportadas por proveedores externos (terceras partes)
- se informa a los usuarios potencialmente afectados
- se informa a los proveedores potencialmente afectados
- se toman medidas urgentes para contener el problema, evitar que crezca dentro de la organización e impedir que se transmita a otras organizaciones
- se reparan daños

163. También hay que ejecutar una serie de actividades de carácter administrativo:

- recopilación de evidencias para analizar, aprender y reportar a las órganos de gestión
- se documenta el incidente, su análisis y los pasos seguidos para su resolución
- se actualizan los procedimientos operativos de seguridad afectados
- se actualizan los planes de continuidad afectados
- se incluye la notificación al CERT cuando el incidente se deba a defectos en el equipamiento que pudieran causar problemas similares en otras organizaciones

164. En categoría ALTA, afectos de monitorizar el desempeño del proceso de resolución de incidencias, se recopilarán datos sobre el tiempo de resolución y los recursos que han sido necesarios.

165. En el análisis del incidente conviene identificar la causa raíz o causa última por la que se ha sido origen del incidente. En categoría ALTA, esta caracterización se incorporará a las métricas de eficacia, identificándose debilidades recurrentes y elaborando un plan para su remedio.

166. Referencias:

- Guía CCN-STIC 817 – Gestión de Incidentes de Seguridad
- Guía CCN-STIC 403 Gestión de Incidentes de Seguridad
- Guía CCN-STIC 403 Gestión de Incidentes de Seguridad
- NIST SP 800-53 rev3:
  - [IR] Incident Response
  - [AT-5] Contacts with Security Groups and Associations
- NIST SP 800-61 – Computer Security Incident Handling Guide
- ISO/IEC 27002:2005:
  - 10.2.2 Supervisión y revisión de los servicios prestados por terceros
  - 13 Gestión de incidentes de seguridad de la información
- ISO/IEC TR 18044:2004 - Information technology – Security techniques – Information security incident management

4.3.8. [OP.EXP.8] REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS

Categoría ALTA

167. Se considerará evidencia suficiente del cumplimiento de esta medida:

- existen registros para todas las actividades realizadas en el sistema
- existe un proceso formal para determinar el nivel de detalle de los registros basado en el análisis de riesgos
- existen mecanismos que garanticen la corrección de la hora a la que se realiza el registro, en prevención de manipulaciones de los relojes
- se realiza una inspección regular de los registros para identificar anomalías en el uso de los sistemas (uso irregular o no previsto)
- se utilizan herramientas automáticas para analizar los registros en busca de actividades fuera de lo normal

168. Referencias:

- NIST SP 800-53 rev3:
  - [AC-7] Unsuccessful Login Attempts
  - [AC-13] Supervision and Review Access Control (withdrawn)
  - [AU] Audit and Accountability

- ISO/IEC 27002:2005:
  - 10.10 Supervisión
  - 10.10.1 Pistas de auditoría
  - 10.10.2 Supervisión del uso de los sistemas
  - 10.10.4 Registros de administración y operación
  - 10.10.5 Registro de fallos

4.3.9. [OP.EXP.9] REGISTRO DE LA GESTIÓN DE INCIDENCIAS

Categoría MEDIA

169. Se considerará evidencia suficiente del cumplimiento de esta medida:

- existen los registros arriba indicados
- existe un procedimiento formal para determinar las evidencias requeridas de cara a un proceso judicial
- existen mecanismos que garanticen la corrección de la hora a la que se realiza el registro, en prevención de manipulaciones de los relojes

170. Referencias:

- NIST SP 800-53 rev3:
  - [IR-5] Incident Monitoring
  - [IR-6] Incident Reporting

- ISO/IEC 27002:2005:
  - 10.10.5 Registro de fallos
  - 13.2 Gestión de incidentes y mejoras
  - 13.2.3 Recopilación de evidencias

4.3.10. [OP.EXP.10] PROTECCIÓN DE LOS REGISTROS

Categoría ALTA

171. Se considerará evidencia suficiente del cumplimiento de esta medida:

- existe una declaración formal de los periodos de retención habituales
- existe un plan para garantizar la capacidad de almacenamiento de registros atendiendo a su volumen y política de retención
- existe un procedimiento formal para la retención de evidencias tras un incidente
- existen mecanismos para prevenir el acceso a los registros de personas no autorizadas
- existen mecanismos para prevenir el acceso de personas no autorizadas a la configuración del sistema para el registro automático de actividades
- existe un procedimiento para la eliminación de los registros tras el periodo estipulado de retención, incluyendo las copias de seguridad
- los registros están contemplados en los procesos de copias de seguridad garantizando las seguridades mencionadas

172. Referencias:

- NIST SP 800-53 rev3:
  - [AU-9] Protection of Audit Information
- NIST SP 800-92 - Guide to Computer Security Log Management

- ISO/IEC 27002:2005:
  - 10.10.3 Protección de registros (logs)
  - 10.10.6 Sincronización del reloj

4.3.11. [OP.EXP.11] PROTECCIÓN DE LAS CLAVES CRIPTOGRÁFICAS

173. Condición de aplicabilidad: se utilizan claves criptográficas. Ver [op.acc.5] [mp.com.2] [mp.si.2] [mp.info.3] [mp.info.4] y [mp.info.9].

Categoría BÁSICA

174. Las claves deben generarse en un equipo y después trasladarse al equipo en el que se van a usar. Los elementos de generación que no son necesarios para el uso se quedarán en el equipo de generación. Es muy recomendable emplear un soporte de información (por ejemplo, un disco USB o una tarjeta de memoria) para trasladar las claves.

175. Cuando una clave se retira de explotación, la política marcará durante cuánto tiempo se debe retener, bien por razones operativas, bien como prueba de auditoría. El motivo operacional más habitual se da en claves de descifrado cuando se requiere poder descifrar información cifrada con claves antiguas. Un motivo de auditoría frecuente se da en claves de verificación de firma electrónica cuando puede ser necesario validar firmas realizadas en el pasado.

176. Es muy recomendable que las claves que se retienen estén en equipos separados. Para su uso se trasladará la información al equipo donde estén.

Categoría MEDIA

177. Se deben proteger las claves criptográficas durante todo su ciclo de vida:

- generación
  - se debe garantizar que las claves generadas son imprevisibles
  - con programas evaluados o dispositivos criptográficos certificados
  - los medios de generación deben estar aislados de los medios de explotación
- transporte o distribución al punto de utilización
  - se debe asegurar la confidencialidad de la clave y la autenticidad del receptor
  - entrega en mano
  - uso de contenedores físicos seguros
  - uso de contenedores criptográficos
  - doble canal: clave y datos de activación por separado
- custodia en explotación
  - se debe garantizar la confidencialidad de la clave en los dispositivos o aplicaciones que la emplean
  - se debe procurar su cambio cuando el volumen de datos cifrados o el tiempo que lleva en uso superen los parámetros recomendados antes de que un atacante pueda descubrirla por análisis de los datos cifrados
  - en tarjeta inteligente protegida por contraseña
  - en dispositivo criptográfico certificado con control de acceso

- archivo: copias de seguridad de claves activas y retención de claves retiradas de explotación activa
  - en contenedores físicos seguros (por ejemplo, caja fuerte)
  - en contenedores criptográficos
  - en medios alternativos aislados de los medios de explotación
- destrucción
  - eliminación de original y copias
  - se debe garantizar su destrucción, aunque por política puede requerirse su retención durante un periodo a efectos de auditoría
  - en el caso de retención, debe garantizarse la confidencialidad de la clave controlando su acceso
  - ver [org.4] Proceso de autorización
  - ver [mp.si.5] Borrado y destrucción de soportes de información

178. Referencias:

- Guía CCN-STIC 807 Criptografía

tipo	nivel BAJO	nivel MEDIO	nivel ALTO
secreto compartido TDEA AES	≥ 112 bits 112 o 168 128, 192 o 256	≥ 128 bits no 128, 192 o 256	≥ 128 bits no 128, 192 o 256
clave pública RSA curvas elípticas	 ≥ 2.048 bits ≥ 224 bits	 ≥ 3.072 bits ≥ 256 bits	 ≥ 3.072 bits ≥ 256 bits

- NIST SP 800-53 rev3:
  - [SC-12] Cryptographic Key Establishment and Management
  - [SC-17] Public Key Infrastructure Certificates
- NIST SP 800-57 Recommendation for Key Management

- ISO/IEC 27002:2005:
  - 12.3 Controles criptográficos
  - 12.3.1 Política de uso
  - 12.3.2 Gestión de claves

4.4. [OP.EXT] SERVICIOS EXTERNOS

179. Medidas para proteger al sistema de posibles perjuicios derivados de la contratación de determinados servicios a proveedores externos.

180. La Organización puede delegar funciones, pero nunca la responsabilidad sobre la información y los servicios.

181. Un problema que debe quedar resuelto es el de alineamiento de los procesos de la organización contratante y los procesos del proveedor externo, estableciendo puntos de contacto y protocolos de comunicación. Esto incluye tanto los procesos organizativos como los procesos operacionales.

182. Referencias

- Guía CCN-STIC 823 – Seguridad en entornos *cloud*

4.4.1. [OP.EXT.1] CONTRATACIÓN Y ACUERDOS DE NIVEL DE SERVICIO

Categoría MEDIA

183. Debe realizarse un análisis de riesgos que identifique los riesgos asociados al proveedor externo.

184. Debe establecerse un contrato formal, aprobado por ambas partes y actualizado periódicamente estableciendo

- roles y funciones en ambas partes, en materia de seguridad, incluyendo los mecanismos de contacto (teléfono, email, etc.)
- obligaciones de cada parte
- responsabilidades de cada parte
- protocolo de aviso previo de actuaciones que puedan impactar a la otra parte
- mecanismos y procedimientos para la sincronización de las actividades de gestión de incidencias
- [categoría ALTA] un conjunto de indicadores para evaluar el servicio prestado (ver [op.mon.2])

185. También hay que tener preparado un procedimiento de desconexión o terminación de la provisión del servicio. En este escenario es especialmente importante la recuperación de la información dentro del RPO establecido y la destrucción de la información en los equipos del proveedor saliente.

186. Referencias:

- modelos de contrato de prestación de servicios (CSAE)

- NIST SP 800-53 rev3:
  - [PS-7] Third Party Personnel Security
  - [SA-9] External Information System Services
- NIST SP 800-35 – Guide to Information Technology Security Services

- ISO/IEC 27002:2005:
  - 6.2.1 Identificación de riesgos derivados del acceso de terceros
  - 6.2.3 Tratamiento de la seguridad en contratos con terceros
  - 10.2 Gestión de servicios prestados por terceros
  - 10.2.1 Prestación de los servicios

4.4.2. [OP.EXT.2] GESTIÓN DIARIA

Categoría MEDIA

187. A partir de una serie de indicadores, se establece un plan de reporte y seguimiento con puntos de alarma cuando se superen ciertos umbrales. Estas alarmas dispararán procedimientos de resolución y de escalado, tratándose como una incidencia que debe resolverse.

188. El proceso de resolución de la incidencia levantada por una alarma se regirá según [op.exp.9] y [op.exp.10].

189. Referencias:

- NIST SP 800-53 rev3:
  - [SA-9] External Information System Services
- NIST SP 800-35 – Guide to Information Technology Security Services

- ISO/IEC 27002:2005:
  - 10.2 Gestión de servicios prestados por terceros
  - 10.2.1 Prestación de los servicios
  - 10.2.2 Supervisión y revisión de los servicios
  - 10.2.3 Gestión de cambios en los servicios

4.4.3. [OP.EXT.9] MEDIOS ALTERNATIVOS

Disponibilidad: nivel ALTO

190. La provisión de servicios externos será parte de los planes de continuidad de la Organización ([op.cont]).
191. Se ha establecido un protocolo de comunicación con el proveedor para avisar de desastres y escalar el problema.
192. Se ha definido un procedimiento de reacción y recuperación (RTO) ante fallos prolongados de servicio por parte del proveedor.
193. Se ha definido un procedimiento para recuperar la información con la antigüedad (RTPO) determinada por la política de la Organización.
194. Los procesos de actuación en caso de desastre se prueban dentro del plan de pruebas periódicas ([op.cont.3]) de la Organización.
195. Hay una amplia variedad de opciones alternativas a un servicio prestado por un tercero:
    - El propio proveedor proporciona los medios alternativos, de forma que el cliente sólo tiene que conmutar el acceso.
    - La organización cliente recurre a otro proveedor con el que hay establecido un plan de activación ([op.ext.1] y [op.ext.2]). Parte del plan es cargar (o transferir) datos frescos según política (RPO).
    - Si el proveedor alternativo en realidad está funcionando siempre y simplemente se hace cargo de toda la carga de trabajo, hay que establecer un procedimiento para ampliar la contratación y mantener un nivel mínimo de calidad del servicio.
    - La organización puede recurrir a medios, debiendo preverse los procedimientos citados en los puntos anteriores.

4.5. [OP.CONT] CONTINUIDAD DEL SERVICIO

196. Estas actividades permiten instrumentar los principios de seguridad
    - Artículo 7 – Prevención, reacción y recuperación
197. Principios recogidos de la guía NIST SP800-27 (Rev. A):
    - Principle 17. Design and operate an IT system to limit damage and to be resilient in response
    - Principle 18. Provide assurance that the system is, and continues to be, resilient in the face of expected threats.
    - Principle 23. Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.
198. Medidas para frenar incidentes desastrosos y permitir que los servicios se sigan prestando en unas condiciones mínimas tras la ocurrencia de un desastre.

199. Se entiende por desastre cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

200. Las medidas de esta sección se entienden como complemento holístico de las medidas requeridas en otros puntos relativas a medios alternativos y copias de seguridad de la información.

201. Referencias:

- NIST SP 800-53 rev3:
  - [CP] Contingency Planning
- NIST SP 800-34 - Contingency Planning Guide for Information Technology Systems

- ISO/IEC 27002:2005:
  - 14 Gestión de la continuidad del negocio

- BSI 25999 - BS 25999 Business continuity
- BS 25999-1:2006 Business continuity management. Code of practice.
- BS 25999-2:2007 Business continuity management. Specification.

- ISO 22301:2012
  Societal security – Business continuity management systems – Requirements
- ISO/IEC 24762:2008
  Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services
- ISO/IEC 27031:2011
  Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity

4.5.1. [OP.CONT.1] ANÁLISIS DE IMPACTO

Disponibilidad: Nivel MEDIO

202. Un análisis de impacto es un estudio pormenorizado de cómo afectaría un desastre a la prestación de servicios, identificando los elementos del sistema de información que son necesarios para la prestación de cada servicio.

203. Un análisis de impacto es una actividad metódica que sigue los siguientes pasos:

- se identifican los servicios o procesos críticos
- se valora el coste de la interrupción de dichos servicios en función del tiempo que dure la interrupción; sin perjuicio de que en cada caso se elija la escala más adecuada, son escalas típicas de valoración las siguientes
  - días: 1, 2, 3, …, 10 días
  - horas: 1, 2, 4, 8, 24, 48 horas, 5 días
- se identifican los elementos necesarios para dar continuidad a cada servicio: instalaciones, personas, equipamiento, comunicaciones y software
- se establece un tiempo objetivo de recuperación, RTO, bien para cada servicio (muy laborioso), bien para todos los sistemas de información del organismo (lo ideal salvo que el coste derivado lo haga prohibitivo), bien por familias de servicios (críticos, normales, secundarios, …)

204. Para la información, hay que analizar cuánta información es aceptable que se pierda en caso de desastre. En base a ese cálculo se establece el RPO, un punto objetivo de recuperación, que marcará la frecuencia de copias de respaldo. Por ejemplo, si se hacen

copias cada 24 horas, en el peor de los casos perderemos las actualizaciones de las últimas 24 horas, diciéndose que el RPO = 24h. Si no se puede admitir esa pérdida, hay que establecer objetivos más ambiciosos, aumentando la frecuencia de realización de copias. En última instancia se puede llegar a un RPO prácticamente igual a 0 empleando técnicas de almacenamiento redundante.

205. El análisis de impacto debe incluir las implicaciones sobre los proveedores de servicios externos.

206. Se considerará evidencia suficiente del cumplimiento de esta medida:

- [MEDIO] existe un análisis de impacto realizado dando respuesta a las cuestiones planteadas más arriba.
- [ALTO] El análisis de impacto concluye en un informe formal, aprobado por la Dirección y sometido a un proceso de revisión periódica.

4.5.2. [OP.CONT.2] PLAN DE CONTINUIDAD

Disponibilidad: Nivel ALTO

207. Se debe identificar funciones, responsabilidades y actividades a realizar en caso de desastre que impida prestar el servicio en las condiciones habituales y con los medios habituales.

208. En particular:

- quiénes componen el comité de crisis que toma la decisión de aplicar los planes de continuidad tras analizar el desastre y avaluar las consecuencias
- quiénes se encargarán de la comunicación con las partes afectadas en caso de crisis
- quiénes se encargan de reconstruir el sistema de información (recuperación de desastre)

209. Debe existir una previsión de los medios alternativos que se van a conjugar para poder seguir prestando los servicios en caso de no poder hacerse con los medios habituales:

- instalaciones alternativas (ver [mp.if.9])
- comunicaciones alternativas (ver [mp.com.9])
- equipamiento alternativo (ver [mp.eq.9])
- personal alternativo (ver [mp.per.9])
- recuperación de la información con una antigüedad no superior a un tope determinado a la luz del análisis de impacto (ver [mp.info.9] y [mp.cont.1])

210. Todos los medios alternativos deben estar planificados y materializados en acuerdos o contratos con los proveedores correspondientes. El plan debe determinar la coordinación de todos los elementos para alcanzar la restauración de los servicios en los plazos estipulados.

211. Las personas afectadas por el plan deben recibir formación específica relativa a su papel en dicho plan.

212. El plan de continuidad debe ser parte integral y armónica con los planes de continuidad de la organización en otras materias ajenas a la seguridad.

213. Deben establecerse procedimientos para sincronizar el plan de continuidad con las actualizaciones del sistema en lo referente a arquitectura, elementos componentes y servicios y calidad de los servicios prestados. En otras palabras, los procedimientos operativos de seguridad referentes a cambios y actualizaciones deben incluir un punto para actualizar los planes de continuidad.

214. Referencias:

- NIST SP 800-53 rev3:
  - [CP-2] Contingency Plan
  - [CP-3] Contingency Training
  - [CP-5] Contingency Plan Update (withdrawn)

- ISO/IEC 27002:2005:
  - 14.1.3 Desarrollo e implantación de planes de continuidad incluyendo la seguridad de la información

4.5.3. [OP.CONT.3] PRUEBAS PERIÓDICAS

Disponibilidad: Nivel ALTO

215. Se debe pruebas periódicas para localizar (y corregir en su caso) los errores o deficiencias que puedan existir en el plan de acción en caso de desastre.

216. Tras cada ejercicio debe realizarse un informe de análisis de las pruebas realizadas, destacando las incidencias propias o en subcontratistas y derivando un plan de mejoras tanto en los medios como en los procedimientos y en la concienciación y formación de las personas implicadas.

217. Referencias:

- NIST SP 800-53 rev3:
  - [CP-4] Contingency Plan Testing and Exercises

- ISO/IEC 27002:2005:
  - 14.1.5 Prueba, mantenimiento y re-evaluación de los planes de continuidad

4.6. [OP.MON] MONITORIZACIÓN DEL SISTEMA

4.6.1. [OP.MON.1] DETECCIÓN DE INTRUSIÓN

Categoría ALTA

218. Estas actividades permiten instrumentar los principios de seguridad

- Artículo 7 – Prevención, reacción y recuperación
- Artículo 8 – Líneas de defensa

219. Principios recogidos de la guía NIST SP800-27 (Rev. A):

- Principle 22. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.

220. La monitorización del sistema permite detectar ataques e incidentes en general habilitando las medidas de reacción y recopilando información para analizar el incidente.

221. Las herramientas de monitorización pueden observar en tráfico en la red o los registros de actividad en los equipos. En este segundo caso, hay que organizar un sistema de recopilación de información desde los puntos en que se genera.

222. Es necesario instalar un sistema de monitorización en la red corporativa. Si existen puntos de interconexión, deben instalarse sistemas de monitorización en dichos puntos,

en particular si nos conectamos a redes públicas como Internet y si se permite el acceso remoto con dispositivos donde no se puede garantizar la configuración de seguridad.

223. Se monitorizarán aquellos puntos donde el análisis de riesgos ha identificado un riesgo elevado.

224. El sistema de monitorización buscará todo aquello que suponga un uso no autorizado del sistema o un uso sospechoso; por ejemplo:

- descargas masivas de información,
- barrido de puertos,
- accesos fuera de horario habitual,
- accesos con derechos de administrador,
- frecuencias anormales de uso del sistema,
- envío de información a servidores externos,
- tráfico cifrado,
- descargas de servidores externos,
- etc.

225. Hay que detectar actividades de atacantes internos y externos, así como la existencia de troyanos o APTs (Advanced Persistent Threats) que pudieran haberse introducido en el sistema.

226. Se considerará evidencia suficiente del cumplimiento de esta medida la existencia de una herramienta de detección de intrusión que:

- está activa
- se mantiene al día: el software y las reglas
- se atienden las alarmas
- se analizan los registros
- se verifica regularmente que la herramienta reacciona a las condiciones de disparo de alarmas que se han programado

227. Referencias:

- Guía CCN-STIC 818 Herramientas de seguridad
- Guía CCN-STIC 432 Seguridad Perimetral - Detección de Intrusos
- Guía CCN-STIC 435 Herramientas de Monitorización de Tráfico

- NIST SP 800-53 rev3:
  - [SI-4] Information System Monitoring
- NIST SP 800-94 - Guide to Intrusion Detection and Prevention Systems (IDPS)

- ISO/IEC 27002:2005:
  - 15.1.5 Prevención frente al mal uso de los medios de tratamiento de la información

4.6.2. [OP.MON.2] SISTEMA DE MÉTRICAS

Categoría ALTA

228. Estas actividades permiten instrumentar los principios de seguridad

- Artículo 7 – Prevención, reacción y recuperación
- Artículo 9 – Reevaluación periódica

229. Se debe disponer de métricas de eficacia, que indiquen que el sistema de protección está protegiendo realmente la seguridad de la información y los servicios. Típicamente se analizan datos del proceso de gestión de incidentes de seguridad.

230. Se debe disponer de métricas predictivas que anuncian posibles incidentes antes de que estos se produzcan. Típicamente se recurre a indicadores de cumplimiento y medidas de los recursos dedicados a la seguridad del sistema.

231. Se debe disponer de métricas de eficiencia que miden si los recursos dedicados a la seguridad son de un volumen adecuado y prudente. Típicamente se medidas de recursos humanos y de dotación económica.

232. Debe formalizarse el proceso de generación de indicadores, debiendo estar aprobado un conjunto de indicadores, indicando para cada uno de ellos:

- el objetivo que se pretende medir
- el responsable del indicador
- el origen de la información
- el procedimiento de recogida y tratamiento de datos (mediciones)
- la frecuencia de recogida de datos
- el método de elaboración de indicadores a partir de las medidas
- la elaboración de indicadores agregados a partir de otros indicadores
- los criterios de valoración del indicador a efectos de reaccionar y tomar decisiones

233. El proceso de evaluación de los indicadores debe complementarse con un proceso de reporte a los diferentes niveles que deben tomar decisiones en la Organización:

- debe establecerse una lista formal de las personas u órganos que van a recibir los indicadores
- debe establecerse el conjunto de indicadores (probablemente agregados) que recibirá cada destinatario
- cada indicador vendrá acompañado de una explicación de su objetivo y los criterios de interpretación, empleando los términos adecuados a la actividad del receptor
- debe establecerse la frecuencia con que se suministrará cada indicador
- debe formalizarse el canal de reporte

234. Referencias:

- Guía CCN-STIC 815 – Métricas e indicadores
- Guía CCN-STIC 824 – Informe anual

- NIST SP 800-53 rev.3
  - [PM-6] Information Security Measures of Performance

- NIST SP 800-55 - Performance Measurement Guide for Information Security
- NIST SP 800-80 - Guide for Developing Performance Metrics for Information Security

- ISO/IEC 27004 - Information technology – Security techniques – Information security management – Measurement

5. [MP] MEDIDAS DE PROTECCIÓN

5.1. [MP.IF] PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS

5.1.1. [MP.IF.1] ÁREAS SEPARADAS Y CON CONTROL DE ACCESO

235. Se deben delimitar las áreas de trabajo y de equipos, disponiendo de un inventario actualizado que para área determine su función y las personas responsables de su seguridad y de autorizar el acceso.

236. Cuando el acceso se controle por medio de llaves o dispositivos equivalentes, se dispondrá de un inventario de llaves junto con un registro de quién las toma, quién las devuelve y en manos de quién hay copias en cada momento. En caso de sustracción o pérdida, se procederá al cambio con diligencia para cerrar la ventana de riesgo.

237. Se dispondrá de medios que eviten el acceso por puntos diferentes al que dispone del control de acceso. Se evitarán ventanas accesibles y puertas desprotegidas. En particular hay que vigilar puertas de evacuación de emergencia para que no permitan la entrada ni en condiciones normales ni cuando se utilizan como vía de evacuación.

238. Referencias:

- NIST SP 800-53 rev3:
  - [PE-2] Physical Access Authorizations
  - [PE-3] Physical Access Control
  - [PE-4] Access Control for Transmission Medium
  - [PE-5] Access Control for Display Medium

- ISO/IEC 27002:2005:
  - 9.1 Áreas seguras
  - 9.1.1 Perímetro de seguridad física
  - 9.1.2 Controles físicos de entrada
  - 9.1.3 Aseguramiento de oficinas, salas e instalaciones
  - 9.1.6 Áreas abiertas al público, zonas de entrega, carga y descarga
  - 9.2 Seguridad del equipamiento
  - 9.2.1 Ubicación y protección de los equipos
  - 11.6.2 Aislamiento de sistemas sensibles

5.1.2. [MP.IF.2] IDENTIFICACIÓN DE LAS PERSONAS

239. Para las áreas de acceso restringido, se debe mantener una relación de personas autorizadas y un sistema de control de acceso que verifique la identidad y la autorización y deje registro de todos los accesos.

240. Referencias:

- NIST SP 800-53 rev3:
  - [PE-6] Monitoring Physical Access
  - [PE-7] Visitor Control
  - [PE-8] Access Records

- ISO/IEC 27002:2005:
  - 9.1.2 Controles físicos de entrada

5.1.3. [MP.IF.3] ACONDICIONAMIENTO DE LOS LOCALES

241. Se debe disponer de unas instalaciones adecuadas para el eficaz desempeño del equipamiento que se instala en ellas.

242. Sin perjuicio de lo dispuesto en otras medidas más específicas, los locales deben

- garantizar que la temperatura se encuentra en el margen especificado por los fabricantes de los equipos
- garantizar que la humedad se encuentra dentro del margen especificado por los fabricantes de los equipos
- se debe proteger el local frente a las amenazas identificadas en el análisis de riesgos, tanto de índole natural, como derivadas del entorno o con origen humano, accidental o deliberado (complementando [mp.if.1], [mp.if4], [mp.if.5], [mp.if.6] y [mp.if.7])
- se debe evitar que el propio local sea una amenaza en sí mismo, o atractor de otras amenazas
- el cableado debe estar:
  - etiquetado: se puede identificar cada cable físico y su correspondencia a los planos de la instalación
  - protegido frente a accidentes (por ejemplo, que las personas tropiecen con los cables)
  - protegido frente a accesos no autorizados, protegiendo armarios de distribución y canaletas

243. Referencias:

- NIST SP 800-53 rev3:
  - [PE-14] Temperature and Humidity Control
  - [PE-18] Location of Information System Components

- ISO/IEC 27002:2005:
  - 9.1.3 Aseguramiento de oficinas, salas e instalaciones
  - 9.1.4 Protección frente a amenazas externas
  - 9.2.1 Ubicación y protección de los equipos
  - 9.2.2 Suministros
  - 9.2.3 Seguridad del cableado

5.1.4. [MP.IF.4] ENERGÍA ELÉCTRICA

244. Se deben prever medidas para atajar un posible corte de suministro eléctrico.

245. Prevención de problemas de origen interno

- dimensionado y protección del cableado de potencia
- dimensionado y protección de los cuadros y armarios de potencia

246. Reacción a problemas de origen externo

- suministro alternativo: ups, generadores, proveedor alternativo

247. Se debe disponer de un plan de emergencia, de reacción y de recuperación de desastres

Disponibilidad: Nivel MEDIO

248. Hay que disponer de una alimentación suficiente para apagar los equipos de forma ordenada. Normalmente, esto supone una alimentación local (UPS) que garantice el suministro eléctrico durante los minutos necesarios para activar y concluir el procedimiento de apagado de emergencia.

249. Referencias:

- NIST SP 800-53 rev3:
  - [PE-9] Power Equipment and Power Cabling
  - [PE-10] Emergency Shutoff
  - [PE-11] Emergency Power
  - [PE-12] Emergency Lighting

- ISO/IEC 27002:2005:
  - 9.2.2 Suministros

5.1.5. [MP.IF.5] PROTECCIÓN FRENTE A INCENDIOS

250. Se debe realizar un estudio del riesgo de incendios, tanto de origen natural como industrial:

- entorno natural proclive a incendios
- entorno industrial que pudiera incendiarse
- instalaciones propias con riesgo de incendio

251. Si el fuego no se puede evitar, hay que desplegar medidas de prevención, monitorización y limitación del impacto

- evitar el uso de materiales inflamables
- aislamiento (cortafuegos, puertas ignífugas)
- sistema de detección conectado a central de alarmas 24x7
- medios de reacción: medios de extinción
- plan de emergencia, de reacción y de recuperación de desastres

252. Referencias:

- NIST SP 800-53 rev3:
  - [PE-13] Fire Protection

- ISO/IEC 27002:2005:
  - 9.1.4 Protección frente a amenazas externas

- Planes de emergencia y evacuación contra incendios de locales y edificios. http://www.mtas.es/insht/FDN/FDN_011.htm

5.1.6. [MP.IF.6] PROTECCIÓN FRENTE A INUNDACIONES

Disponibilidad: Nivel MEDIO

253. Se debe realizar un estudio del riesgo de inundaciones, tanto de origen natural como industrial:

- cercanía a ríos o corrientes de agua
- canalizaciones de agua (tuberías) especialmente encima de los equipos

254. Si el riesgo no se puede evitar, hay que desplegar medidas de prevención, monitorización y limitación del impacto

- aislamiento de humedades
- canalización de desagüe con procedimientos regulares de limpieza
- sistema de detección conectado a central de alarmas 24x7

- plan de reacción y recuperación de desastres; en el caso de canalizaciones industriales, el plan de reacción puede incluir el cierre de llaves o válvulas que atajen el vertido

255. Referencias:

- NIST SP 800-53 rev3:
  - [PE-15] Water Damage Protection
- ISO/IEC 27002:2005:
  - 9.1.4 Protección frente a amenazas externas

5.1.7. [MP.IF.7] REGISTRO DE ENTRADA Y SALIDA DE EQUIPAMIENTO

256. Se debe llevar un registro pormenorizado de toda entrada y salida de equipamiento, haciendo constar en el mismo:

- fecha y hora
- identificación inequívoca del equipamiento
- persona que realiza la entrada o salida
- persona que autoriza la entrada o salida
- persona que realiza el registro

257. Referencias:

- NIST SP 800-53 rev3:
  - [PE-16] Delivery and Removal
- ISO/IEC 27002:2005:
  - 9.2.7 Retirada de materiales propiedad de la empresa

5.1.8. [MP.IF.9] INSTALACIONES ALTERNATIVAS

Disponibilidad: Nivel ALTO

258. Se debe disponer de planes para poder prestar los servicios en lugar alternativo en caso de indisponibilidad de las instalaciones actuales.

259. Las instalaciones alternativas deben garantizar las mismas medidas de protección que las habituales. En particular, en lo que respecta a control de acceso de personas y entrada y salida de equipos.

260. Las instalaciones alternativas pueden estar dispuestas para entrar en servicio inmediatamente (hot site) o requerir un tiempo de personalización (cold site). En todo caso el tiempo de entrada en servicio debe estar respaldado por un análisis de impacto (ver [op.cont.1]), ser parte del plan de continuidad probado (ver [op.cont.2]) y ser objeto de pruebas regulares para validar la viabilidad del plan (ver [op.cont.3]).

261. Referencias:

- NIST SP 800-53 rev3:
  - [CP-6] Alternate Storage Site
  - [CP-7] Alternate Processing Site
  - [PE-17] Alternate Work Site
- ISO/IEC 27002:2005:

- 14.1.4 Marco de planificación de la continuidad

5.2. [MP.PER] GESTIÓN DEL PERSONAL

262. Medidas para proteger al sistema de problemas que pudieran ser causados por las personas que disfrutan de acceso al mismo.

5.2.1. [MP.PER.1] CARACTERIZACIÓN DEL PUESTO DE TRABAJO

Categoría MEDIA

263. Se deben definir las responsabilidades relacionadas con capa puesto de trabajo en materia de seguridad. La definición debe venir respaldada por el análisis de riesgos en la medida en que afecta a cada puesto de trabajo.

264. Se deben definir los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular en términos de confidencialidad.

265. Se deben tener en cuenta dichos requisitos en la selección de la persona que va a ocuparlo, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias dentro del marco de la ley.

266. Se considerará evidencia suficiente del cumplimiento de esta medida:

- se cumple [op.acc.3]
- [MEDIA] existe un análisis de las responsabilidades de cada tipo de puesto de trabajo;
- [ALTO] el análisis anterior es singular para cada puesto de trabajo y está formalmente aprobado según política

267. Referencias:

- NIST SP 800-53 rev3:
  - [PS-2] Position categorization
  - [PS-3] Personnel Screening

- ISO/IEC 27002:2005:
  - 8.1.1 Funciones y responsabilidades
  - 8.1.2 Investigación de antecedentes

5.2.2. [MP.PER.2] DEBERES Y OBLIGACIONES

268. Se debe informar a cada persona relacionada con el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad, incluyendo las medidas disciplinarias a que haya lugar.

269. Es de especial relevancia el deber de confidencialidad respecto de los datos a los que tengan acceso, tanto durante el periodo durante el que estén adscritos al puesto de trabajo, como su prolongación posterior a la terminación de la función para la que tuvo acceso a la información confidencial.

270. Se debe cubrir tanto el periodo durante el cual se desempeña el puesto como las obligaciones en caso de terminación de la asignación, incluyendo el caso de traslado a otro puesto de trabajo.

271. En el caso de personal contratado a través de una tercera parte,

- se deben determinar deberes y obligaciones de la persona
- se deben determinar deberes y obligaciones de la parte contratante
- se debe determinar el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones, involucrando a la parte contratante

272. Se considerará evidencia suficiente del cumplimiento de esta medida:

- [BAJO] acuerdos verbales
- [MEDIO] acuerdos explícitos, por escrito, y firmados por cada una de las partes involucradas

273. Referencias:

- NIST SP 800-53 rev3:
  - [PS-4] Personnel Termination
  - [PS-5] Personnel Transfer
  - [PS-6] Access Agreements
  - [PS-7] Third-Party Personnel Security
  - [PS-8] Personnel Sanctions

- ISO/IEC 27002:2005:
  - 6.1.5 Acuerdos de confidencialidad
  - 8.1.3 Términos y condiciones laborales
  - 8.2.1 Responsabilidades de la Dirección
  - 8.2.3 Proceso disciplinario
  - 8.3 Fin de la contratación o cambio de puesto de trabajo
  - 8.3.1 Responsabilidad del cese o cambio
  - 8.3.2 Devolución de activos

5.2.3. [MP.PER.3] CONCIENCIACIÓN

274. Se debe concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.

275. En particular hay que refrescar regularmente:

- la normativa de seguridad relativa al buen uso de los sistemas
- la identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado
- el procedimiento de reporte de incidencias de seguridad, seas reales o falsas alarmas

276. Se considerará evidencia suficiente del cumplimiento de esta medida:

- todo el personal recibe inicial y regularmente información acerca de los puntos arriba descritos
- [MEDIO] existe un plan documentado y financiado para que esta actividad se lleve a cabo regularmente
- [ALTO] existe constancia de que cada persona ha seguido el plan establecido en cada periodo temporal

277. Referencias:

- NIST SP 800-53 rev3:
  - [AT-2] Security Awareness
- NIST SP 800-50 - Building an Information Technology Security Awareness and Training Program

- ISO/IEC 27002:2005:
  - 8.2.2 Concienciación, formación y capacitación en seguridad de la información

5.2.4. [MP.PER.4] FORMACIÓN

278. Se debe formar regularmente a las personas en aquellas técnicas que requieran para el desempeño de sus funciones.

279. Es de destacar, sin perjuicio de otros aspectos:

- configuración de sistemas
- gestión de incidencias
- procedimientos relativos a sus funciones

280. La formación debe actualizarse cada vez que cambian los componentes del sistema de información, introduciéndose nuevos equipos, nuevo software, nuevas instalaciones, etc.

281. Se considerará evidencia suficiente del cumplimiento de esta medida:

- todo el personal recibe inicial y regularmente formación acerca de los puntos arriba descritos
- [MEDIO] existe un plan documentado y financiado para que esta actividad se lleve a cabo regularmente, explicitando qué puestos deben recibir qué formación y con qué regularidad
- [ALTO] existe constancia de que cada persona ha seguido el plan establecido en cada periodo temporal

282. Referencias:

- NIST SP 800-53 rev3:
  - [AT-3] Security Training
  - [AT-4] Security Training Records
- NIST SP 800-16 - Information Technology Security Training Requirements: A Role- and Performance-Based Model
- NIST SP 800-50 - Building an Information Technology Security Awareness and Training Program

- ISO/IEC 27002:2005:
  - 8.2.2 Concienciación, formación y capacitación en seguridad de la información

5.2.5. [MP.PER.9] PERSONAL ALTERNATIVO

Disponibilidad: Nivel ALTO

283. Se debe prever la existencia de otras personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual. El personal alternativo deberá ofrecer las mismas garantías de seguridad que el personal habitual.

284. El plan de utilización de personal alternativo se vertebra dentro del plan de continuidad de la organización, incluyéndose en las pruebas periódicas. Ver [op.cont]

285. Referencias:

- NIST SP 800-53 rev3:
  - [CP] Contingency Planning

- ISO/IEC 27002:2005:
  - 14.1.4 Marco de planificación de la continuidad

5.3. [MP.EQ] PROTECCIÓN DE LOS EQUIPOS

5.3.1. [MP.EQ.1] PUESTO DE TRABAJO DESPEJADO

Categoría BÁSICA

286. Se debe exigir que los puestos de trabajo permanezcan despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento. Según se termine una tarea, el material se retirará a otra zona: cajones, estanterías personales o comunes, cuarto de almacenamiento, etc.
287. Existirá un procedimiento disciplinario asociado al incumplimiento de esta medida.

Categoría MEDIA

288. El material de trabajo se guardará en lugar cerrado. Pueden ser cajones o armarios con llave, o un cuarto separado cerrado con llave al menos fuera del horario de trabajo.
289. Se establecerá un procedimiento para revisar que se cumple la medida; es decir, una inspección regular tras el cierre, con notificación de los incumplimientos detectados y retirada del material olvidado a un lugar cerrado.
290. Referencias:
    - ISO/IEC 27002:2005:
      - 11.3.3 Puesto de trabajo limpio y pantalla en blanco

5.3.2. [MP.EQ.2] BLOQUEO DE PUESTO DE TRABAJO

Autenticidad: nivel MEDIO

291. Se debe bloquear el puesto de trabajo al cabo de un tiempo de inactividad que se marcará por política.
292. El tiempo mencionado será parte de la configuración del equipo y no podrá ser alterado por el usuario.

Autenticidad: nivel ALTO

293. El tiempo mencionado será parte de la configuración del equipo y no podrá ser alterado por el usuario.
294. El tiempo mencionado será parte de la configuración del equipo y no podrá ser alterado por el usuario.
295. Referencias:
    - NIST SP 800-53 rev3:
      - [AC-11] Session Lock
      - [AC-12] Session Termination (withdrawn)

    - ISO/IEC 27002:2005:
      - 11.3.2 Equipo desatendido

- 11.3.3 Puesto de trabajo limpio y pantalla en blanco
- 11.5.5 Desconexión automática de la sesión

5.3.3. [MP.EQ.3] PROTECCIÓN DE EQUIPOS PORTÁTILES

Categoría BÁSICA

296. Los equipos portátiles deben tener instalado y activado un sistema de protección perimetral (cortafuegos personal) configurado para bloquear accesos salvo los autorizados. Los accesos autorizados seguirán los procedimientos de autorización del organismo (ver [org.4]).
297. El mecanismo de control formará parte de la configuración del equipo y no podrá ser modificado por el usuario.
298. Los usuarios recibirán instrucciones sobre el uso admisible del equipo y sobre los aspectos que debe contemplar en su manejo diario y en caso de avería, pérdida o terminación.

Categoría ALTA

299. Se debe verificar regularmente que el equipo permanece bajo control del usuario al que está asignado.
300. Se debe establecer un mecanismo adecuado de autenticación: [op.acc.5].
301. Se debe proteger la información contenida por medios criptográficos: [mp.si.2].
302. Las claves criptográficas deben protegerse según [op.exp.11]]
303. Cuando el equipo es desmantelado, se debe aplicar lo previsto en [mp.si.5].
304. Referencias:
    - NIST SP 800-53 rev3:
        - [AC-19] Access Control for Portable and Mobile Devices
    - ISO/IEC 27002:2005:
        - 9.2.5 Seguridad de los equipos fuera de las instalaciones
        - 11.7.1 Equipos móviles

5.3.4. [MP.EQ.9] MEDIOS ALTERNATIVOS

Disponibilidad: Nivel MEDIO

305. Se debe prever medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales. Estos medios alternativos estarán sujetos a las mismas garantías de protección.
306. Se debe establecer un tiempo máximo para que los equipos alternativos entren en funcionamiento.
307. Los equipos alternativos pueden estar dispuestos para entrar en servicio inmediatamente (es decir, configurados) o requerir un tiempo de personalización (se puede disponer de ellos en el tiempo prestablecido; pero hay que configurarlos y cargar los datos). En todo caso el tiempo de entrada en servicio debe estar respaldado por un análisis de impacto (ver [op.cont.1]).
308. Se considerará evidencia suficiente del cumplimiento de esta medida:

- [MEDIO] existen acuerdos formales y procedimientos para utilizar otros medios, indicando el tiempo estimado de entrada en operación
- [ALTO] el plan de utilización de equipos alternativos se vertebra dentro del plan de continuidad aprobado (ver [op.cont.2]) y ser objeto de pruebas regulares para validar la viabilidad del plan (ver [op.cont.3]).

5.4. [MP.COM] PROTECCIÓN DE LAS COMUNICACIONES

5.4.1. [MP.COM.1] PERÍMETRO SEGURO

309. Se debe delimitar el perímetro lógico del sistema; es decir, los puntos de interconexión con el exterior.

310. Se debe disponer de cortafuegos que separen la red interna del exterior. Todo el tráfico deberá atravesar dichos cortafuegos que sólo dejaran transitar los flujos previamente autorizados.

Categoría ALTA

311. Cuando se requiera niveles de seguridad ALTA, el sistema de cortafuegos constará de dos o más equipos de diferente fabricante dispuestos en cascada.

312. Cuando la disponibilidad de las transmisiones a través del cortafuegos sea de nivel ALTO, se dispondrán sistemas redundantes.

313. Los ataques de denegación de servicio pueden ser afrontados en el perímetro, aunque pueden requerir la intervención de otros elementos. En el perímetro se pueden detectar patrones sospechosos de comportamiento: avalanchas de peticiones, peticiones trucadas y, en general, un uso malicioso de los protocolos de comunicaciones. Algunas de estas peticiones pueden ser denegadas directamente por el equipo perimetral, en otras ocasiones hay que levantar una alarma para actuar en donde corresponda (servidores web, servidores de bases de datos, …, o contactando con los centros de respuesta a incidentes).

314. Referencias:

- Guía CCN-STIC 811 – Interconexión
- Guía CCN-STIC 408 Seguridad Perimetral - Cortafuegos
- Guía CCN-STIC 419 Configuración segura con IPtables

- NIST SP 800-53 rev3:
  - [SC-5] Denial of Service Protection
  - [SC-7] Boundary Protection
- NIST SP 800-41 - Guidelines on Firewalls and Firewall Policy

- ISO/IEC 27002:2005:
  - 10.6.2 Seguridad de los servicios de red

5.4.2. [MP.COM.2] PROTECCIÓN DE LA CONFIDENCIALIDAD

315. Es frecuente que autenticidad, integridad y confidencialidad se traten de forma conjunta negociando los protocolos, los parámetros y las claves en la fase de establecimiento. Es por ello que esta medida suele implementarse a la par que [mp.com.3].

Confidencialidad: nivel MEDIO

316. Se debe emplear métodos criptográficos que garanticen el secreto de los datos transmitidos.

317. En conexiones establecidas se puede recurrir a redes privadas virtuales que, tras una autenticación fiable (ver [mp.com.3]), establecen una clave de cifrado para la sesión.

318. El cifrado de las comunicaciones es especialmente adecuado en redes inalámbricas (WiFi). Los equipos inalámbricos llevan incorporado mecanismos de cifrado de las comunicaciones, que deberán ser configurados de forma segura (ver [op.exp.2] y [op.exp.3]) empleando mecanismos actualizados.

319. Hay que atender al secreto de las claves de cifra según lo indicado en [op.exp.11]. En el caso de redes privadas virtuales, el secreto debe ser impredecible, mantenerse bajo custodia mientras dure la sesión, y ser destruido al terminar. En el caso de otros procedimientos de cifrado, hay que cuidar de las claves de cifra durante su ciclo de vida: generación, distribución, empleo, retirada del servicio y retención si la hubiera.

Confidencialidad: nivel ALTO.

320. Hay que seleccionar algoritmos evaluados o acreditados. A menudo basta con seleccionar los algoritmos y los parámetros adecuados dentro de las opciones posibles.

321. Hay que procurar que las tareas de cifrado en los extremos se realicen en equipos hardware especializados, evitando el cifrado por software.

322. Referencias:

- Guía CCN-STIC 807 Criptografía

tipo	nivel BAJO (opc)	nivel MEDIO	nivel ALTO
secreto compartido TDEA AES	≥ 112 bits 112 o 168 128, 192 o 256	≥ 112 bits 112 o 168 128, 192 o 256	≥ 128 bits no 128, 192 o 256
clave pública RSA curvas elípticas	 ≥ 2.048 bits ≥ 224 bits	 ≥ 2.048 bits ≥ 224 bits	 ≥ 2.048 bits ≥ 256 bits

- Guía CCN-STIC 816 – Seguridad en Redes Inalámbricas

- Guía CCN-STIC 406 Seguridad en Redes Inalámbricas
- Guía CCN-STIC 416 Seguridad en VPN's

- NIST SP 800-53 rev3:
  - [AC18] Wireless Access
  - [SC-8] Transmission Integrity
  - [SC-9] Transmission Confidentiality
- NIST SP 800-48 - Wireless Network Security for IEEE 802.11a/b/g and Bluetooth
- NIST SP 800-52 - Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
- NIST SP 800-77 - Guide to IPsec VPNs
- NIST SP 800-113 – Guide to SSL VPNs
- NIST SP 800-121 – Guide to Bluetooth Security
- NIST SP 800-127 – Guide to Securing WiMAX Wireless Communications
- NIST SP 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)

- ISO/IEC 27002:2005:
  - 10.6.1 Controles de red
  - 10.6.2 Seguridad de los servicios de red

- SSL – Secure Sockets Layer
  - [RFC 6101] The Secure Sockets Layer (SSL) Protocol Version 3.0
  - Guía CCN-STIC 826 Configuración de SSL/TLS

- TLS – Transport Layer Security
  - [RFC 5246] The Transport Layer Security (TLS) Protocol – Version 1.2
  - [RFC 6176] Prohibiting Secure Sockets Layer (SSL) Version 2.0
  - Guía CCN-STIC 826 Configuración de SSL/TLS

- SSH – Secure Shell
- SCP – Secure copy
- SFTP – SSH File Transfer Protocol

5.4.3. [MP.COM.3] PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD

323. Es frecuente que autenticidad, integridad y confidencialidad se traten de forma conjunta negociando los protocolos, los parámetros y las claves en la fase de establecimiento. Es por ello que esta medida suele implementarse a la par que [mp.com.2].

Integridad o Autenticidad: nivel BAJO

324. Se debe establecer de forma fehaciente la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información alguna.

325. Se deben usar protocolos que garanticen o al menos chequeen y detecten violaciones en la integridad de los datos intercambiados y en la secuencia de los paquetes.

326. La forma más habitual de establecer esta medida es establecer una red privada virtual que:

- garantice la autenticación de las partes al inicio de sesión, cuando la red se establece
- controle que la sesión no puede ser secuestrada por una tercera parte
- que no pueden realizarse ataques activos (alteración de la información en tránsito o inyección de información espuria) sin que sea, al menos, detectada

Integridad o Autenticidad: nivel MEDIO

327. Se deben elegir algoritmos y productos certificados [op.pl.5] siempre que sea posible.

328. La protección de las comunicaciones es especialmente relevante en redes inalámbricas (WiFi). Los equipos inalámbricos llevan incorporado mecanismos de cifrado de las comunicaciones, que deberán ser configurados de forma segura (ver [op.exp.2] y [op.exp.3]) empleando mecanismos actualizados.

329. Hay que seleccionar algoritmos evaluados o acreditados. A menudo basta con seleccionar los algoritmos y los parámetros adecuados dentro de las opciones posibles.

Integridad o Autenticidad: nivel ALTO

330. Hay que procurar el empleo de equipos hardware especializados, evitando las soluciones software.

331. Hay que procurar el empleo de productos evaluados o acreditados.

332. Referencias: ver [mp.com.2]

- Guía CCN-STIC 807 Criptografía
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

tipo	nivel BAJO	nivel MEDIO	nivel ALTO
secreto compartido	≥ 112 bits	≥ 112 bits	≥ 128 bits
TDEA	112 o 168	112 o 168	no
AES	128, 192 o 256	128, 192 o 256	128, 192 o 256
clave pública			
RSA	≥ 2.048 bits	≥ 2.048 bits	≥ 2.048 bits
curvas elípticas	≥ 224 bits	≥ 224 bits	≥ 256 bits
funciones hash			
SHA-1 (160)	PCP	PCP	PCP
RIPEMD-160	PCP	PCP	PCP
SHA-2	≥ 256 bits	≥ 256 bits	≥ 256 bits
SHA-3	≥ 256 bits	≥ 256 bits	≥ 256 bits

PCP – permitido a corto plazo

5.4.4. [MP.COM.4] SEGREGACIÓN DE REDES

Categoría ALTA

333. La segregación de redes acota el acceso a la información y acota la propagación de los incidentes de seguridad que quedan restringidos al entorno donde ocurren.

334. Se debe segmentar la red de forma que haya

- control (de entrada) de los usuarios que pueden trabajar en cada segmento, en particular si el acceso se realiza desde el exterior del segmento, tanto si es desde otro segmento de la red corporativa como si el acceso procede del exterior de la red, extremando las precauciones en este último escenario.
- control (de salida) de la información disponible en cada segmento
- control (de entrada) de las aplicaciones utilizables en cada segmento

335. El punto de interconexión debe estar particularmente asegurado, mantenido y monitorizado (ver [mp.com.1]). Estos puntos de interconexión interna son una defensa crítica frente a intrusos que han logrado superar las barreas exteriores y se alojan en el interior. Nótese que a menudo el objetivo de estas intrusiones es extraer información y enviarla al exterior, lo que se traduce en que hay que vigilar los protocolos de comunicaciones que se establecen y los datos que se transmiten.

336. No debería permitirse ningún protocolo directo entre los segmentos internos y el exterior, intermediando todos los intercambios de información.

337. Las redes se pueden segmentar por dispositivos físicos o lógicos.

338. Esta medida puede establecerse dinámicamente como reacción frente a intrusiones (supuestas o detectadas) y que van a requerir un cierto periodo de tiempo (días) en poder ser erradicadas. Los primeros servicios a aislar serían los servidores de datos y los servidores de autenticación para monitorizar y controlar su uso. Otros candidatos a ser aislados son los servicios de administración del propio sistema para evitar que se capturen credenciales con privilegios de administración o se pueda suplantar la identidad de los administradores.

339. Referencias:

- NIST SP 800-53 rev3:
  - [SC-32] Information System Partitioning
- ISO/IEC 27002:2005:
  - 11.4.5 Segregación de redes

5.4.5. [MP.COM.9] MEDIOS ALTERNATIVOS

Disponibilidad: Nivel ALTO

340. Se debe prever medios alternativos de comunicación para el caso de que fallen los medios habituales. Estos medios alternativos deben proporcionar las mismas garantías de seguridad que los medios habituales. y deberá establecerse un tiempo máximo de entrada en funcionamiento

341. En todo caso el tiempo de entrada en servicio debe estar respaldado por un análisis de impacto (ver [op.cont.1]), ser parte del plan de continuidad probado (ver [op.cont.2]) y ser objeto de pruebas regulares para validar la viabilidad del plan (ver [op.cont.3])-

342. Referencias:

- NIST SP 800-53 rev3:
  - [CP-8] Telecommunications Services
- ISO/IEC 27002:2005:
  - 14.1.4 Marco de planificación de la continuidad

5.5. [MP.SI] PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN

343. Los soportes de información incluyen

- discos de los servidores y equipos de usuario final, con especial consideración a equipos portátiles y discos removibles
- PDAs
- disquetes, cintas, CD, DVD, ...
- discos USB
- tarjetas de memoria y tarjetas inteligentes
- componentes de impresoras
- material impreso
- otros medios de almacenamiento de información con capacidad de que la información pueda ser recuperada de formar automática o manual

344. Referencias:

- Guía CCN-STIC 404 Control de Soportes Informáticos

5.5.1. [MP.SI.1] ETIQUETADO

345. Se debe etiquetar de forma que, sin revelar su contenido, se indique el nivel de clasificación más alto de la información contenida.

346. Una opción es que el propio soporte, en su exterior, lleve escrito el nivel de información que contiene o puede contener.

347. Una alternativa es que el soporte sea identificable por medio de algún código o referencia y que el usuario pueda acceder a un repositorio de información donde se indica el nivel de información que el soporte contiene o puede contener.

348. La etiqueta del soporte determina las normativa y los procedimientos que deben aplicarse al mismo, concretamente en lo referente a:

- control de acceso
- cifrado del contenido
- entrada y salida de las instalaciones
- medios de transporte

349. Se considerará evidencia suficiente del cumplimiento de esta medida:

- existe un procedimiento para etiquetar todos los soportes, tanto lo que permanecen dentro de los locales de la organización como los que salen a otros destinos
- los usuarios son capaces de entender el significado de las etiquetas, y conocen y aplican los procedimientos asociados a cada nivel de información

350. Referencias:

- NIST SP 800-53 rev3:
  - [MP-3] Media Marking

- ISO/IEC 27002:2005:
  - 10.7.1 Gestión de soportes
  - 10.7.3 Procedimientos de tratamiento de la información

5.5.2. [MP.SI.2] CRIPTOGRAFÍA

351. En lo referente a claves criptográficas, se debe aplicar [op.exp.11].

Integridad o confidencialidad: nivel MEDIO

352. Una opción es asegurarse que los datos se protegen antes de copiarse al soporte; es decir, se cifran o se firman exteriormente.

353. Otra opción es proteger todo el soporte instalando en el mismo un disco virtual que se encarga de acoger todo lo que se copie en el mismo, así como controlar el acceso al mismo.

354. Otra opción es emplear soportes con cifrado incorporado por hardware que se encarga de acoger todo lo que se copie en el soporte así como controlar el acceso al mismo.

Integridad o confidencialidad: nivel ALTO

355. Se deben emplear algoritmos y parámetros acreditados.

356. Se deben elegir productos certificados [op.pl.5] siempre que sea posible.

357. Referencias:

- Guía CCN-STIC 807 – Criptografía

tipo	nivel BAJO (opc)	nivel MEDIO	nivel ALTO
secreto compartido TDEA AES	≥ 112 bits 112 o 168 128, 192 o 256	≥ 128 bits no 128, 192 o 256	≥ 128 bits no 128, 192 o 256
clave pública RSA curvas elípticas	 ≥ 2.048 bits ≥ 224 bits	 ≥ 2.048 bits ≥ 224 bits	 ≥ 2.048 bits ≥ 256 bits
función hash SHA-2 SHA-3	 ≥ 256 bits ≥ 256 bits	 ≥ 256 bits ≥ 256 bits	 ≥ 256 bits ≥ 256 bits

- Guía CCN-STIC 437 Herramientas de Cifrado Software

- NIST SP 800-53 rev3:
  - [MP-2] Media Access
- NIST SP 800-111 - Guide to Storage Encryption Technologies for End User Devices

- ISO/IEC 27002:2005:
  - 12.3 Controles criptográficos
  - 12.3.1 Política de uso

- Productos. Hay muchos donde elegir; sólo se citan algunos de uso frecuente:
  - BitLocker – Microsoft
  - Crypt2000 – Secuware
  - GPG – http://www.gnupg.org/
  - PGP – Symantec
  - TrueCrypt – http://www.truecrypt.org/

5.5.3. [MP.SI.3] CUSTODIA

358. Se debe aplicar la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización:
   - garantizando el control de acceso con medidas físicas ([mp.if.1] y [mp.if.7) o lógicas ([mp.si.2]) o ambas
   - garantizando que se respetan las exigencia de mantenimiento del fabricante, es especial en lo referente a temperatura, humedad y otros agresores medioambientales
359. Se considerará evidencia suficiente del cumplimiento de esta medida:
   - [categoría BÁSICA] existe un inventario exhaustivo de todos los soportes de información en uso, indicando su etiqueta, su ubicación física y quién es el responsable del mismo
   - [categoría MEDIA] se conserva la historia de cada dispositivo, desde su primer uso hasta la terminación de su vida útil
   - [categoría ALTA] se verifica regularmente que el soporte cumple las reglas acordes a su etiquetado
360. Referencias:
   - NIST SP 800-53 rev3:

  - [MP-2] Media Access
  - [MP-4] Media Storage
- NIST SP 800-111 – Guide to Storage Encryption Technologies for End User Devices

- ISO/IEC 27002:2005:
  - 9.2.5 Seguridad de los equipos fuera de las instalaciones

5.5.4. [MP.SI.4] TRANSPORTE

361. Se debe garantizar que los dispositivos permanecen bajo control y se satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro.

362. Se debe

- disponer de un registro de salida que identifica al transportista que recibe el soporte para su transporte
- disponer de un registro de entrada que identifica al transportista que lo entrega
- disponer de un procedimiento rutinario que coteja las salidas con las llegadas y levanta las alarmas pertinentes cuando se detecta algún incidente
- utilizar los medios de protección criptográfica ([mp.si.2]) correspondientes al nivel de clasificación de la información contenida de mayor nivel
- gestionar las claves según [op.exp.11]

363. Se considerará evidencia suficiente del cumplimiento de esta medida:

- [categoría BÁSICA] existe normativa al respecto y se ha instruido a los usuarios
- [categoría MEDIA] existen procedimientos al respecto
- [categoría ALTA] se verifica regularmente que los procedimientos establecidos se siguen, aplicando medidas correctivas en su defecto

364. Referencias:

- NIST SP 800-53 rev3:
  - [MP-2] Media Access
  - [MP-5] Media Transport

- ISO/IEC 27002:2005:
  - 10.8.3 Soportes físicos en tránsito

5.5.5. [MP.SI.5] BORRADO Y DESTRUCCIÓN

Confidencialidad: nivel MEDIO

365. Se debe aplicar un mecanismo de borrado seguro a los soportes que vayan a ser reutilizados para otra información o liberados a otra Organización. El mecanismo de borrado será proporcionado a la clasificación de la información que ha estado presente en el soporte.

366. Se deben destruir los soportes, de forma segura,

- cuando la naturaleza del soporte no permita un borrado seguro
- cuando el procedimiento asociado al nivel de clasificación de la información contenida así lo requiera

367. El mecanismo de destrucción será proporcionado a la clasificación de la información contenida.

368. Los mecanismos de borrado y destrucción deben ser respetuosos con la normativa de protección medioambiental y con los certificados de calidad medioambiental de la Organización.

369. Se deben elegir productos certificados [op.pl.5] siempre que sea posible.

370. Recomendaciones (tomadas de NIST SP 800-88)

medio	procedimiento	
papel microfilm	destruir	• trituradora en tiras o cuadraditos: 2mm
móviles PDAs	borrar manualmente	• agenda • mensajes • llamadas • resetear a la configuración de fábrica
routers	borrar manualmente	• tablas de encaminamiento • registros de actividad • cuantas de administración • resetear a la configuración de fábrica
impresoras fax	borrar manualmente	• resetear a la configuración de fábrica
discos reescribibles	reescribir	• reescribir 3 veces: con ceros, con unos, con datos aleatorios
discos de solo lectura	destruir	• trituradora: 5mm
discos virtuales cifrados	además de lo anterior	• destruir las claves

371. Se considerará evidencia suficiente del cumplimiento de esta medida:

- [categoría BÁSICA] existe normativa al respecto y se ha instruido a los usuarios
- [categoría MEDIA] existen procedimientos al respecto
- [categoría ALTA] se verifica regularmente que los procedimientos establecidos se siguen, aplicando medidas correctivas en su defecto

372. Referencias:

- Guía CCN-STIC 818 – Herramientas de seguridad

- NIST SP 800-53 rev3:
  - [MP-6] Media Sanitization and Disposal
- NIST SP 800-88 - Guidelines for Media Sanitization

- DoD 5220 Block Erase

- ISO/IEC 27002:2005:
  - 9.2.6 Retirada o reutilización de equipos (pasan a otras manos)
  - 10.7.2 Retirada de soportes

5.6. [MP.SW] PROTECCIÓN DE LAS APLICACIONES INFORMÁTICAS

5.6.1. [MP.SW.1] DESARROLLO

373. Son dignos de mención los siguientes principios recogidos de la guía NIST SP800-27 (Rev. A):

- Principle 2. Treat security as an integral part of the overall system design.
- Principle 4. Ensure that developers are trained in how to develop secure software.
- Principle 12. Where possible, base security on open standards for portability and interoperability.
- Principle 13. Use common language in developing security requirements.
- Principle 14. Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.
- Principle 15. Strive for operational ease of use.
- Principle 22. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.
- Principle 24. Strive for simplicity.
- Principle 29. Identify and prevent common errors and vulnerabilities.

Categoría MEDIA

374. Referencias:

- SANS
  http://www.sans.org/curricula/secure-software-development

- Métrica v3 - Metodología de Planificación, Desarrollo y Mantenimiento de sistemas de información, Ministerio de Administraciones Públicas, Consejo Superior de Administración Electrónica
- Guía CCN-STIC 205 Actividades Seguridad Ciclo Vida CIS

- NIST SP 800-53 rev3:
  - [SA-3] Life Cycle Support
  - [SA-8] Security Engineering Principles
  - [SA-9] External Information System Services
  - [SA-10] Developer Configuration Management
  - [SA-11] Developer Security Testing
  - [SI-10] Information Accuracy, Completeness, Validity, and Authenticity
- NIST SP 800-64 - Security Considerations in the System Development Life Cycle

- ISO/IEC 27002:2005:
  - 12.2 Garantías de procesamiento de información
  - 12.4.2 Protección de los datos de prueba
  - 12.4.3 Control de acceso al código fuente

- 12.5.5 Desarrollo externalizado (outsourcing)

5.6.2. [MP.SW.2] ACEPTACIÓN Y PUESTA EN SERVICIO

Categoría BÁSICA

375. Pruebas estándar de aceptación para que un nuevo software se integre en un proceso.

Categoría MEDIA

376. El análisis de vulnerabilidades constará de 3 fases: (1) revisión exhaustiva de los componentes del software, centrándose en su superficie de interacción con los usuarios con servicios de soporte y con otros programas. (2) Análisis de posibles vulnerabilidades en los elementos identificados en el primer paso y estimación del impacto potencial que supondría un incidente. (3) Pruebas de penetración para cerciorarse de si la vulnerabilidad es utilizable, priorizando aquellos puntos de mayor impacto potencial.
377. Deben hacerse pruebas simulando usuarios externos y usuarios internos, en función de a quienes sea accesible el software.

Categoría ALTA

378. El análisis de coherencia se hace a nivel de procesos, concretamente de los que componen el proceso administrativo que le compete a la Organización. Para cada proceso propio, hay que ejecutar pruebas comprobando que los datos de entrada producen los datos de salida correctos, y que datos incorrectos de entrada son detectados y atajados antes de destruir la integridad del sistema.
379. La auditoría completa de código fuente puede ser de un coste prohibitivo. Por ello nos centraremos en los puntos críticos identificados en el paso (2) del análisis de vulnerabilidades que se describe arriba.
380. Referencias:

- NIST SP 800-53 rev3:
  - [RA-5] Vulnerability Scanning

- ISO/IEC 27002:2005:
  - 10.3.2 Aceptación de nuevos sistemas

5.7. [MP.INFO] PROTECCIÓN DE LA INFORMACIÓN

5.7.1. [MP.INFO.1] DATOS DE CARÁCTER PERSONAL

381. Se considerará evidencia suficiente del cumplimiento de esta medida:

- cumplimiento de las medidas de protección determinadas para cada nivel en el Real Decreto 1720.

382. Referencias:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (B.O.E. Nº 298, de 14 de diciembre de 1999)
- Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- NIST SP 800-53 rev3:
  - [PL-5] Privacy Impact Assessment

- ISO/IEC 27002:2005:
  - 15.1.4 Protección de datos e información de carácter personal

5.7.2. [MP.INFO.2] CLASIFICACIÓN DE LA INFORMACIÓN

Confidencialidad: nivel BAJO

383. Se debe establecer un esquema para asignar un nivel de clasificación a la información, en función de sus necesidades de confidencialidad.

384. El sistema de clasificación:

- debe ser acorde con otros sistemas de clasificación propios del entorno en el que desarrolla su actividad la organización
- debe ser acorde con lo indicado en el Anexo I del ENS sobre clasificación de la información y categorización de los sistemas de información
- debe establecer las responsabilidades para adscribir inicialmente una cierta información a una cierta clase y para posibles re-clasificaciones posteriores
- deben definirse una serie de procedimientos que describan en detalle cómo se debe etiquetar y tratar la información en consideración a su nivel: control de acceso, almacenamiento, copias, transmisión, etc.

Confidencialidad: nivel MEDIO

385. Se deben desarrollar procedimientos de uso de la información para cada nivel, cubriendo al menos los siguientes aspectos

- ¿cómo se controla el acceso? normativa y procedimientos de autorización y mecanismos de control
- normativa relativa a la realización de copias en diferentes medios: proceso de autorización y mecanismos de control
- ¿cómo se marcan los documentos?
- soportes de información: condiciones de adquisición, inventario, marcado, uso, borrado y destrucción
- impresión: ¿en dónde se puede imprimir? ¿quién puede imprimir? gestión del papel impreso
- transporte físico: condiciones sobre el medio de transporte, del mensajero, autorizaciones de salida y controles de recepción
- transporte por redes de comunicaciones: condiciones de seguridad sobre el canal de comunicaciones (especialmente, autenticación y cifrado) y autorizaciones necesarias para poder trasmitir

386. Cabe esperar que los organismos organicen la información en tres niveles: BAJO, MEDIO y ALTO, alineados a los niveles del Anexo I. Siguiendo este esquema, se pueden desarrollar tablas como la siguiente:

	BAJO	MEDIO	ALTO	referencias
responsable de la clasificación	originador			
autorizado para	organismo			

re-clasificar				
autorizador de acceso	• accesible a todo el personal propio	• accesible a los que lo necesitan conocer por sus funciones	• autorización del organismo a la persona	[org.4]
copias impresas	• marcadas • cada persona se encarga de su destrucción cuando ya no hace falta	• marcadas • destrucción usando destructora	• marcadas • se lleva un inventario de las copias realizadas • destrucción procedimentada con actualización del inventario	[mp.si]
soportes electrónicos de información	• etiquetados • se borra el contenido o se inhabilita	• etiquetados • se cifra el contenido • se usa software de borrado seguro o se destruye	• etiquetados • se cifra el contenido • se usa software de borrado seguro o se destruye en trituradora homologada	[mp.si]
uso en equipos portátiles y PDAs	• con control de acceso	• con control de acceso	• debe estar cifrada en reposo	[mp.info.3] [mp.eq.3]
transmisión telemática	• canales autenticados	• canales autenticados y cifrados	• canales autenticados cifrados	[mp.com.2] [mp.com.3]

387. Referencias:

- Guía CCN-STIC 001 Seguridad de las TIC que manejan información nacional clasificada en la Administración
- NIST SP 800-53 rev3:
  - [RA-2] Security Categorization
  - [AC-15] Automated Marking (withdrawn)
  - [AC-16] Security Attributes
  - [MP-3] Media Labeling

- ISO/IEC 27002:2005:
  - 7.2 Clasificación de la información
  - 7.2.1 Directrices de clasificación
  - 7.2.2 Etiquetado y tratamiento de la información

5.7.3. [MP.INFO.3] CIFRADO

Confidencialidad: nivel ALTO

388. Se debe cifrar la información, tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella. Esto incluye

- cifrado de ficheros
- cifrado de directorios
- discos virtuales cifrados
- cifrado de datos en bases de datos

389. Ver

- [mp.com.2] Protección de la confidencialidad en comunicaciones
- [mp.si.2] Criptografía en los soportes de información

390. Referencias:

- Guía CCN-STIC 807 Criptografía

tipo	nivel BAJO (opc)	nivel MEDIO (opc)	nivel ALTO
secreto compartido TDEA AES	≥ 112 bits 112 o 168 128, 192 o 256	≥ 128 bits no 128, 192 o 256	≥ 128 bits no 128, 192 o 256
clave pública RSA curvas elípticas	 ≥ 2.048 bits ≥ 224 bits	 ≥ 2.048 bits ≥ 224 bits	 ≥ 2.048 bits ≥ 256 bits

- Guía CCN-STIC 955 – Recomendaciones empleo GnuPG

- NIST SP 800-53 rev3:
  - [SC-28] Protection of Information at Rest

- ISO/IEC 27002:2005:
  - 12.3.1Política de uso de los controles criptográficos
  - 12.5.4 Fugas de información

- GNUPG – The GNU Privacy Guard
- PGP – Pretty Good Privacy
- TrueCrypt

391. Se considerará evidencia suficiente del cumplimiento de esta medida:

- existen instrucciones para cifrar la información en función de su clasificación y el medio en que se almacena
- se constata que la información está, efectivamente cifrada
- se cumple [op.exp.11]

5.7.4. [MP.INFO.4] FIRMA ELECTRÓNICA

392. Todas las actividades relacionadas con la firma electrónica y el sellado de tiempo deben regirse por un marco técnico y procedimental aprobado formalmente. Se suele denominar Política de Firma.

Política de firma electrónica

393. Política de firma electrónica. En el caso de la AGE, debe cumplir los requisitos establecidos en el artículo 24 del Real Decreto 1671/2009.

394. En todos los casos debe cubrir los siguientes puntos técnicos y procedimentales:

- delimitación del ámbito de aplicación; es decir, qué información irá firmada y en qué procesos o procedimientos se firmará y se verificará cada firma
- los roles y funciones del personal involucrado en la generación y verificación de firmas
- los roles y funciones del personal involucrado en la administración de los medios de firma
- los roles y funciones del personal involucrado en la generación, custodia y distribución de claves y certificados
- directrices y normas técnicas aplicables a la utilización de certificados y firmas electrónicas
- los requisitos exigibles a las firmas electrónicas presentadas
- los medios de validación y verificación de firmas: protocolos y prestadores del servicio

395. En la Administración General del Estado se dispone de un marco de referencia. Ver http://administracionelectronica.gob.es/es/ctt/politicafirma

396. La política de firma debe cumplir los requisitos del Esquema Nacional de Interoperabilidad.

397. En cualquier escenario se debe buscar una interoperabilidad de las firmas electrónicas por lo que se recomienda fuertemente que los organismos referencien la política de firma de electrónica de un órgano superior y sólo en muy contadas ocasiones se establezca una política independiente.

Uso de claves concertadas para firmar

398. La firma con un secreto compartido requiere algunas cautelas.

399. Lo más que podemos hacer es

- presentarle la información al ciudadano en una página web
- pedirle que introduzca la clave de firma (sin memoria: hay que introducirla expresamente)
- conservar como evidencia el HMAC(documento + clave_concertada)

400. Este mecanismo garantiza la integridad del documento e identifica al ciudadano; pero no garantiza el no-repudio ya que cualquiera que puede verificar la firma, puede también generarla. Es decir, no cumple los requisitos de una firma electrónica avanzada, que requiere que “haya sido creada por medios que el firmante puede mantener bajo su exclusivo control” (Ley 59/2003).

401. Se considerará firma electrónica, sin más.

Código seguro de verificación

402. Se trata de una forma alternativa de asegurar la autenticidad e integridad de la información proporcionada por la Administración.

403. En lugar de proteger la información por medio de una firma inviolable, lo que se proporciona es una forma cómoda de verificar que la información es auténtica y no se ha modificado (es íntegra).

404. El sistema de código seguro de verificación deberá garantizar, en todo caso:

- El carácter único del código generado para cada documento.
- Su vinculación con el documento generado y con el firmante.
- Asimismo, se debe garantizar la posibilidad de verificar el documento por el tiempo que se establezca en la resolución que autorice la aplicación de este procedimiento.

405. La Administración queda obligada a

- garantizar la disponibilidad del mecanismo de verificación
- garantizar la integridad del documento referenciado
- garantizar la confidencialidad del documento correspondiente; por ejemplo controlando el acceso para que sólo accedan las personas autorizadas

406. Una forma fácil de proporcionar CSVs es usar un número consecutivo en un archivo documental identificado (lo que sería una clave primaria en una base de datos documental). Al ciudadano hay que proporcionarle la identificación del archivo y el número de expediente.

407. Una forma fácil de cumplir los requisitos de autenticidad e integridad es que el documento referenciado por medio del CSV, sea en sí mismo un documento firmado electrónicamente. De esta forma, el ciudadano (o cualquier tercera parte autorizada) puede en cualquier momento recabar el documento y conservarlo en su poder.

Integridad o autenticidad: nivel BAJO

Integridad o autenticidad: nivel MEDIO

Integridad o autenticidad: nivel ALTO

408. Referencias:

- Guía CCN-STIC 807 Criptografía

tipo	nivel BAJO	nivel MEDIO	nivel ALTO
clave pública			
RSA	≥ 1.024 bits	≥ 1.024 bits (PCP)	≥ 2.048 bits
DSA	≥ 1.024 bits	≥ 1.024 bits (PCP)	≥ 2.048 bits
curvas elípticas	≥ 224 bits	≥ 224 bits	≥ 256 bits
funciones hash			
MD5	no	no	no
SHA-1 (160)	corto plazo	corto plazo	corto plazo
RIPEMD-160	corto plazo	corto plazo	corto plazo
SHA-2	≥ 256 bits	≥ 256 bits	≥ 256 bits
SHA-3	≥ 256 bits	≥ 256 bits	≥ 256 bits

PCP – permitido a corto plazo

- Guía CCN-STIC 405 Algoritmos y Parámetros de Firma Electrónica
-
- Real Decreto 1671 de 2009

- NIST SP 800-53 rev3:

- [AU-10] Non-Repudiation
- [SC-28] Protection of Information at Rest

- NIST SP 800-89 - Recommendation for Obtaining Assurances for Digital Signature Applications

- ISO/IEC 27002:2005:
  - 6.2.2 Tratamiento de la seguridad en la relación con los clientes
  - 10.9.1 Comercio electrónico
  - 10.9.2 Transacciones en línea
  - 10.9.3 Información puesta a disposición pública
  - 12.3.1 Política de uso de controles criptográficos

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Real Decreto 1065/2007, de 27 de julio, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos.

409. Se considerará evidencia suficiente del cumplimiento de esta medida:

- se firman electrónicamente los documentos que requieren capacidad probatoria según la ley de procedimiento administrativo
- existen procedimientos para firmar y validar firmas
- se utilizan los formatos establecidos por la normativa para asegurar la validez de la firma: verificación de la validez del certificado y aportación de pruebas adicionales de validez (tales como consultas OCSP, CRL, etc.)
- se cumple [op.exp.11]

5.7.5. [MP.INFO.5] SELLOS DE TIEMPO

410. Todas las actividades relacionadas con la firma electrónica y el sellado de tiempo deben regirse por un marco técnico y procedimental aprobado formalmente. Se suele denominar Política de Firma

Política de firma electrónica y fechado electrónico

411. Ver [mp.info.4]

Trazabilidad: nivel ALTO

412. Se fechan electrónicamente los documentos cuya fecha y hora de entrada debe acreditarse fehacientemente.

413. Se fechan electrónicamente los documentos cuya fecha y hora de salida debe acreditarse fehacientemente.

414. Se fechan electrónicamente las firmas cuya validez deba extenderse por largos periodos o así lo exija la normativa aplicable; alternativamente se pueden utilizar formatos de firma avanzada que incluyan fechado.

415. Existe normativa y procedimientos para fechar y verificar fechas.

416. Referencias:

- Guía CCN-STIC 807 Criptografía

	nivel ALTO	
tipo	firma electrónica	listas enlazadas
clave pública		
RSA	≥ 3.072 bits	n.a.
curvas elípticas	≥ 284 bits	n.a.
funciones hash		
MD5	no	no
SHA-1 (160)	no	no
RIPEMD-160	no	no
SHA-2	≥ 256 bits	≥ 256 bits
SHA-3	≥ 256 bits	≥ 256 bits

- ISO/IEC 18014-1:2008
  Information technology – Security techniques – Time-stamping services –
  Part 1: Framework
- ISO/IEC 18014-2:2009
  Information technology – Security techniques – Time-stamping services –
  Part 2: Mechanisms producing independent tokens
- ISO/IEC 18014-3:2009
  Information technology – Security techniques – Time-stamping services –
  Part 3: Mechanisms producing linked tokens
- ISO/IEC TR 29149:2012
  Information technology – Security techniques –
  Best practices for the provision and use of time-stamping services

- RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

- NIST SP 800-53 rev3:
  - [AU-10] Non-Repudiation

- ISO/IEC 27002:2005:
  - 10.9.1Comercio electrónico
  - 10.9.2 Transacciones en línea

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

5.7.6. [MP.INFO.6] LIMPIEZA DE DOCUMENTOS

417. Se debe retirar de los documentos toda la información adicional contenida en campos ocultos, meta-datos, comentarios, revisiones anteriores, etc. salvo cuando dicha información sea pertinente para el receptor del documento.

418. Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorios de información.

419. El incumplimiento de esta medida puede perjudicar

- al mantenimiento de la confidencialidad de información que no debería haberse revelado al receptor del documento
- al mantenimiento de la confidencialidad de las fuentes u orígenes de la información, que no debe conocer el receptor del documento
- a la buena imagen de la organización que difunde el documento por cuanto demuestra un descuido en su buen hacer

420. Se considerará evidencia suficiente del cumplimiento de esta medida:

- existe un procedimiento para limpiar todos los documentos que van a ser transferidos a otro dominio de seguridad
- existe un procedimiento para limpiar todos los documentos que van a ser publicados electrónicamente
- se utilizan herramientas evaluadas para limpiar los datos ocultos innecesarios de los documentos

421. Referencias

- Guía CCN-STIC 825 Borrado de metadatos

- ISO/IEC 27002:2005:
  - 10.9.3 Información públicamente disponible

5.7.7. [MP.INFO.9] COPIAS DE SEGURIDAD (BACKUP)

Disponibilidad: Nivel MEDIO

422. Se deben realizar copias de respaldo que permitan recuperar datos perdidos accidental o intencionadamente con una antigüedad de determinar por la Organización.

423. Las copias de respaldo disfrutarán de las mismas seguridades que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, debe considerarse la conveniencia o necesidad de que las copias de seguridad estén cifradas para garantizar la confidencialidad (en cuyo caso se estará a lo dispuesto en [op.exp.11]).

424. Debe existir un proceso de autorización para la recuperación de información de las copias de respaldo

425. Los controles de acceso a las copias de respaldo garantizarán las mismas seguridades que los controles de acceso a la información original

426. Las copias de respaldo se conservarán en lugar(es) suficientemente independiente(s) de la ubicación normal de la información en explotación como para que los incidentes previstos en el análisis de riesgos no se den simultáneamente en ambos lugares

427. El trasporte de copias de respaldo desde el lugar donde se producen hasta su lugar de almacenamiento garantiza las mismas seguridades que los controles de acceso a la información original

428. Las copias de respaldo deben abarcar:

- información de trabajo de la organización
- aplicaciones en explotación, incluyendo los sistemas operativos
- datos de configuración: servicios, aplicaciones, equipos, etc.
- claves utilizadas para preservar el secreto de la información

429. En todo caso el tiempo de entrada en servicio debe estar respaldado por un análisis de impacto (ver [op.cont.1]).

430. La frecuencia con que se deben realizar copias se determinará por medio del parámetro RPO (Recovery Point Objective – Punto objetivo de recuperación).

431. Los procedimientos de recuperación de la información deberán asegurar que se satisface el parámetro RTO (Recovery Time Objective – Tiempo de recuperación objetivo).

432. Se considerará evidencia suficiente del cumplimiento de esta medida:

- [MEDIO] existen procedimientos para recuperar la información, indicando el tiempo estimado de recuperación.
- [MEDIO] se verifica regularmente que la información respaldada está correctamente dispuesta para ser recuperada en caso de necesidad.
- [ALTO] el plan de copias se vertebra dentro del plan de continuidad aprobado (ver [op.cont.2]) y ser objeto de pruebas regulares para validar la viabilidad del plan (ver [op.cont.3]).

433. Referencias:

- NIST SP 800-53 rev3:
  - [CP-6] Alternate Storage Site
  - [CP-9] Information System Backup
  - [CP-10] Information System Recovery and Reconstitution

- ISO/IEC 27002:2005:
  - 10.5.1 Copias de seguridad

434. Se considerará evidencia suficiente del cumplimiento de esta medida:

- existe un plan para realizar regularmente copia de seguridad de la información relevante (ver arriba los elementos que deben considerarse)

5.8. [MP.S] PROTECCIÓN DE LOS SERVICIOS

5.8.1. [MP.S.1] PROTECCIÓN DEL CORREO ELECTRÓNICO (E-MAIL)

435. Referencias:

- Guía CCN-STIC 814 – Seguridad en el Servicio de Correo

- NIST SP 800-53 rev3:
  - [SI-8] Spam Protection
- NIST SP 800-45 – Guidelines on Electronic Mail Security

- ISO/IEC 27002:2005:
  - 10.8.4 Mensajería electrónica
  - 12.5.4 Fugas de información

5.8.2. [MP.S.2] PROTECCIÓN DE SERVICIOS Y APLICACIONES WEB

436. Pueden presentarse ataques a nivel de red, a nivel del sistema operativo del servidor y a nivel de la aplicación que atiende a peticiones web. De los dos primeros modos de ataque nos defenderemos protegiendo el equipo de frontera.

437. Básicamente hay 2 formas de proteger el servidor frontal: protegiendo el equipo y el software que proporciona la interfaz para acceso al servicio web, o disponiendo una protección previa en forma de cortafuegos de aplicación (appliance) entre el servidor y los usuarios.

438. Los ataques a nivel de aplicación pueden detectarse en el servidor frontal o en algún servidor de soporte en la retaguardia; es decir, puede haber ataques que aparecen como correctos (sintácticamente correctos) pero que causan problemas por el tipo de petición o por la secuencia de peticiones (semántica incorrecta). Para los ataques que entran en el nivel interno será necesario desarrollar reglas específicas para detectar y reaccionar; reglas de tipo

- límite en el número de sesiones, total o por usuario anónimo o identificado
- cierre de sesiones al cabo de un tiempo
- límite en el volumen de datos (individual y agregado)

439. Referencias:

- Guía CCN-STIC 812 – Seguridad en Servicios Web
- NIST SP 800-44 - Guidelines on Securing Public Web Servers
- NIST SP 800-53 rev3:
  - [AC-22] Publicly Accessible Content
  - [SC-7] Boundary Protection
  - [SC-14] Public Access Protections
  - [SI-10] Information Input Validation
- ISO/IEC 27002:2005:
  - 10.9.3 Información públicamente disponible
  - 11.4.7 Control de encaminamiento (routing) de red

5.8.3. [MP.S.8] PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO

Disponibilidad: nivel MEDIO

440. Los ataques de denegación de servicio pueden prevenirse dimensionando con holgura los elementos susceptibles de ser atacados desde el exterior, aunque poco se puede hacer frente a un ataque con suficientes recursos por parte del atacante.

441. Múltiples ataques de denegación de servicio son facilitados por un software deficiente por parte del servidor, bien porque no se han actualizado los remedios, bien porque la configuración no es idónea. Ambos aspectos deberán ser analizados y reparados (ver medidas de protección [mp.exp] en lo relativo a configuración, mantenimiento y cambios).

Disponibilidad: nivel ALTO

442. Aun estando preparados, podemos ser víctimas de un nuevo tipo de ataque imprevisto, en cuyo caso hay que detectarlo rápidamente y gestionar la incidencia.

443. Los ataques de denegación de servicio pueden ser afrontados en el perímetro ([mp.com.1]), aunque pueden requerir la intervención de otros elementos. En el perímetro se pueden detectar patrones sospechosos de comportamiento: avalanchas de peticiones, peticiones trucadas y, en general, un uso malicioso de los protocolos de comunicaciones. Algunas de estas peticiones pueden ser denegadas directamente por el equipo perimetral,

en otras ocasiones hay que levantar una alarma para actuar en donde corresponda (servidores web, servidores de bases de datos, …, y contactando con los centros de respuesta a incidentes, CERT).

444. Es responsabilidad del organismo detectar y bloquear el uso deliberado o accidental del propio sistema de información para atacar a terceros. Nótese que el organismo puede ser simplemente víctima de una plantación de elementos agresivos que son lanzados contra otros. En estos casos el bloqueo puede ser una medida reactiva suficiente, seguido de una erradicación de la infección. La reacción a este tipo de incidencias debe ser reportada a los sistemas atacados y al centro de respuesta de emergencia (CERT) para coordinar la respuesta.

445. Referencias:

- Guía CCN-STIC 820 - Denegación de Servicio

- NIST SP 800-53 rev3:
  - [SC-5] Denial of Service Protection

5.8.4. [MP.S.9] MEDIOS ALTERNATIVOS

Disponibilidad: nivel ALTO

446. Ante interrupciones del servicio habitual, una respuesta posible es recurrir a servicios alternativos mientras se recupera la disponibilidad de los medios habituales. Por ejemplo,

447. Referencias:

- Ver [op.cont]

6. CORRESPONDENCIA CON OTRAS NORMAS DE SEGURIDAD

448. Se considera la relación con otras normas de seguridad de amplia difusión. Concretamente:

[RD 1720]
Real Decreto 1720/2007, de 21 de diciembre, por el que se prueba el Reglamento de desarrollo de la Ley Orgánica 155/1999, de 13 de diciembre, de protección de datos de carácter personal.

[27002]
ISO/IEC 27002, Code of Practice for Information Security Management, 2005.

[800-53]
NIST SP 800-53, Recommended Security Controls for Federal Information Systems, revision 3, August 2009, revised May 1, 2010.

[SANS 20]
20 Critical Security Controls
http://www.sans.org/critical-security-controls/

449. Nótese que la correspondencia no es una relación matemática de equivalencia. Más bien debe entenderse como una tabla que muestra en qué sitios se trata el mismo tema en dos normas diferentes. O, siendo más precisos, se intenta mostrar para cada medida del ENS, en dónde se trata el mismo tema en otras normas. La tabla sólo tiene valor a efectos informativos; pero puede ayudar al cumplimiento simultáneo de varias normas.

6.1. [ORG] MARCO ORGANIZATIVO

ENS	RD 1720	27002	800-53	SANS 20
[org.1] Política de seguridad	89.1 95	5.1 6.1.1 6.1.3 15.1.1	PM-2 PM-11	
[org.2] Normativa de seguridad		7.1.3 11.4.1 11.7.2 12.3.1 15.1.2	*-1 PL-4 SA-8	
[org.3] Procedimientos de seguridad		10.1.1	*-1	
[org.4] Proceso de autorización	100.2	6.1.4 11.4.6 12.4.1	PM-10 CA-3 CA-6	CC11

6.2. [OP.PL] PLANIFICACIÓN

ENS	RD 1720	27002	800-53	SANS 20
[op.pl.1] Análisis de riesgos		4 12.1.1	RA-3 PM-9	
[op.pl.2] Arquitectura de seguridad		6.2.2 10.7.4 11.1.1 12.1.1 12.2	CA-3 PM-3 PM-7 PM-8 SA-5 SA-9 CM-8 SI-10 SI-11	CC6 CC19
[op.pl.3] Adquisición de nuevos componentes		10.3.2 12.1.1	PL-1 PL-2 PL-3 PL-6 SA-1 SA-2 SA-3 SA-4 SA-8	
[op.pl.4] Dimensionamiento / Gestión de capacidades		10.3.1 12.1.1	SA-2	
[op.pl.5] Componentes certificados		12.1.1	SA-13	

6.3. [OP.ACC] CONTROL DE ACCESO

ENS	RD 1720	27002	800-53	SANS-20
[op.acc.1] Identificación	93.1 93.2	11.2.1 11.4.3 11.5.2	AC-2 IA-2 IA-3 IA-4 IA-8	
[op.acc.2] Requisitos de acceso	91.3 91.5 93.2	11.1.1 11.2.2 11.5.4 11.6.1	SA-6 AC-3 AC-4 AC-14	
[op.acc.3] Segregación de funciones y tareas	91.4	10.1.3 10.1.4 15.3.1 15.3.2	AC-5	CC6

ENS	RD 1720	27002	800-53	SANS-20
[op.acc.4] Proceso de gestión de derechos de acceso	91.2 91.5	11.2.2 11.2.4 8.3.3	AC-2 AC-6	CC12
[op.acc.5] Mecanismo de autenticación	93.1 93.2 93.3 93.4	11.2.3 11.3.1 11.5.2 11.5.3	IA-2 IA-3 IA-5 IA-7 IA-8	
[op.acc.6] Acceso local (local logon)	98	11.5.1 11.5.6	AC-7 AC-8 AC-9 IA-6 SI-11	
[op.acc.7] Acceso remoto (remote login)	98	11.4.2 11.4.4 11.5.6 11.7.2	AC-17 AC-20 MA-4	

6.4. [OP.EXP] EXPLOTACIÓN

ENS	RD 1720	27002	800-53	SANS-20
[op.exp.1] Inventario de activos		7.1.1 7.1.2	PM-5 CM-8	CC1 CC2
[op.exp.2] Configuración de seguridad			CM-2 CM-6 CM-7	CC3 CC10
[op.exp.3] Gestión de la configuración		12.4.1	CM-2 CM-3 CM-4 CM-6 SA-7	CC3 CC10
[op.exp.4] Mantenimiento		9.2.4 12.4.1 12.5.2 12.6.1	MA-2 MA-3 MA-4 MA-5 MA-6 SI-2 SI-5	CC4 CC20
[op.exp.5] Gestión de cambios		10.1.2 10.2.3 12.4.1 12.5.1 12.5.3	CA-7 CM-3 CM-5 MA-2 SI-7	CC4

ENS	RD 1720	27002	800-53	SANS-20
[op.exp.6] Protección frente a código dañino		10.4	SI-3 SI-8 SC-18	CC5
[op.exp.7] Gestión de incidencias	90	10.2.2 13	IR-2 IR-3 IR-4 IR-7 IR-8 AT-5	CC18
[op.exp.8] Registro de la actividad de los usuarios	103.1 103.2 103.6	10.10 10.10.1 10.10.2 10.10.4 10.10.5	AC-7 AC-13 AU-2 AU-3 AU-6 AU-7	CC14 CC16
[op.exp.9] Registro de la gestión de incidencias	90 100.1	10.10.5 13.2 13.2.3	IR-5 IR-6	
[op.exp.10] Protección de los registros	103.3 103.4 103.5	10.10.3 10.10.6	AU-9	
[op.exp.11] Protección de claves criptográficas		12.3.1 12.3.2	SC-12 SC-17	

6.5. [OP.EXT] SERVICIOS EXTERNOS

ENS	RD 1720	27002	800-53	SANS 20
[op.ext.1] Contratación y acuerdos de nivel de servicio		6.2.1 6.2.3 10.2 10.2.1	PS-7 SA-9	
[op.ext.2] Gestión diaria		10.2 10.2.1 10.2.2 10.2.3	SA-9	
[op.ext.3] Medios alternativos		14.1.4		

6.6. [OP.CONT] CONTINUIDAD DEL SERVICIO

ENS	RD 1720	27002	800-53	SANS 20

ENS	RD 1720	27002	800-53	SANS 20
[op.cont.1] Análisis de impacto		14 14.1.2	CP	
[op.cont.2] Plan de continuidad		14 14.1.3	CP-2 CP-3 CP-5	
[op.cont.3] Pruebas periódicas		14.1.5	CP-4	

6.7. [OP.MON] MONITORIZACIÓN DEL SISTEMA

ENS	RD 1720	27002	800-53	SANS 20
[op.mon.1] Detección de intrusión		15.1.5	SI-4	
[op.mon.2] Sistema de métricas			PM-6	

6.8. [MP.IF] PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS

ENS	RD 1720	27002	800-53	SANS 20
[mp.if.1] Áreas separadas y con control de acceso	99	9.1.1 9.1.2 9.1.3 9.1.6 9.2.1 11.6.2	PE-2 PE-3 PE-4 PE-5	
[mp.if.2] Identificación de las personas	99	9.1.2	PE-6 PE-7 PE-8	
[mp.if.3] Acondicionamiento de los locales		9.1.3 9.1.4 9.2.1 9.2.2 9.2.3	PE-14 PE-18	
[mp.if.4] Energía eléctrica		9.2.2	PE-9 PE-10 PE-11 PE-12	
[mp.if.5] Protección frente a incendios		9.1.4	PE-13	

ENS	RD 1720	27002	800-53	SANS 20
[mp.if.6] Protección frente a inundaciones		9.1.4	PE-15	
[mp.if.7] Registro de entrada y salida de equipamiento	92.2 97.1 97.2	9.2.7	PE-16	
[mp.if.9] Instalaciones alternativas	102	14.1.4	CP-6 CP-7 PE-17	

6.9. [MP.PER] GESTIÓN DEL PERSONAL

ENS	RD 1720	27002	800-53	SANS 20
[mp.per.1] Caracterización del puesto de trabajo		8.1.1 8.1.2	PS-2 PS-3	
[mp.per.2] Deberes y obligaciones	89.2	6.1.5 8.1.3 8.2.1 8.2.3 8.3.1 8.3.2	PS-4 PS-5 PS-6 PS-7 PS-8	
[mp.per.3] Concienciación	89.2	8.2.2	AT-2	CC9
[mp.per.4] Formación	89.2	8.2.2	AT-3 AT-4	CC9
[mp.per.9] Personal alternativo		14.1.4		

6.10. [MP.EQ] PROTECCIÓN DE LOS EQUIPOS

ENS	RD 1720	27002	800-53	SANS 20
[mp.eq.1] Puesto de trabajo despejado		11.3.3		
[mp.eq.2] Bloqueo del puesto de trabajo		11.3.2 11.3.3 11.5.5	AC-11 AC-12	
[mp.eq.3] Protección de equipos portátiles		9.2.5 11.7.1	AC-19	

ENS	RD 1720	27002	800-53	SANS 20
[mp.eq.9] Medios alternativos		14.1.4		

6.11. [MP.COM] PROTECCIÓN DE LAS COMUNICACIONES

ENS	RD 1720	27002	800-53	SANS 20
[mp.com.1] Perímetro seguro		10.6.2	SC-5 SC-7	CC6 CC13 CC15 CC17
[mp.com.2] Protección de la confidencialidad	104	10.6.1 10.6.2	AC-18 SC-8 SC-9	CC7
[mp.com.3] Protección de la autenticidad y de la integridad	104	10.6.2 11.4.3	AC-18 SC-23	CC7
[mp.com.4] Segregación de redes		11.4.5	SC-32	CC15
[mp.com.9] Medios alternativos		14.1.4	CP-8	

6.12. [MP.SI] PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN

ENS	RD 1720	27002	800-53	SANS 20
[mp.si.1] Etiquetado	92.1 92.5 101.1	10.7.1 10.7.3	MP-3	
[mp.si.2] Criptografía	92.3 101.2	12.3.1	MP-2	
[mp.si.3] Custodia	101.3	9.2.5	MP-2 MP-4	
[mp.si.4] Transporte	92.3 97 101.2	10.8.3	MP-2 MP-5	
[mp.si.5] Borrado y destrucción	92.4	9.2.6 10.7.2	MP-6	

6.13. [MP.SW] PROTECCIÓN DE LAS APLICACIONES INFORMÁTICAS

ENS	RD 1720	27002	800-53	SANS 20

ENS	RD 1720	27002	800-53	SANS 20
[mp.sw.1] Desarrollo	94.4	12.2 12.4.2 12.4.3 12.5.5	SA-3 SA-8 SA-9 SA-10 SA-11 SI-10	CC6
[mp.sw.2] Aceptación y puesta en servicio	94.4	10.3.2	RA-5	CC6

6.14. [MP.INFO] PROTECCIÓN DE LA INFORMACIÓN

ENS	RD 1720	27002	800-53	SANS 20
[mp.info.1] Datos de carácter personal		15.1.4	PL-5	
[mp.info.2] Calificación de la información		7.2	RA-2 AC-15 AC-16 MP-3	
[mp.info.3] Cifrado		12.3.1 12.5.4	SC-28	
[mp.info.4] Firma electrónica		6.2.2 10.9.1 10.9.2 10.9.3 12.3.1	AU-10 SC-28	
[mp.info.5] Sellos de tiempo		10.9.1 10.9.2	AU-10	
[mp.info.6] Limpieza de documentos		10.9.3		
[mp.info.9] Copias de seguridad (backup)	94.1 94.2 94.3 100.1 100.2 102	10.5.1	CP-6 CP-9 CP-10	CC8

6.15. [MP.S] PROTECCIÓN DE LOS SERVICIOS

ENS	RD 1720	27002	800-53	SANS 20
[mp.s.1] Protección del correo electrónico (e-mail)		10.8.4 12.5.4	SI-8	

ENS	RD 1720	27002	800-53	SANS 20
[mp.s.2] Protección de servicios y aplicaciones web		10.9.3 11.4.7	AC-22 SC-7 SC-14 SI-10	CC6
[mp.s.8] Protección frente a la denegación de servicio			SC-5	
[mp.s.9] Medios alternativos		4.1.4		

ANEXO A. GLOSARIO Y ABREVIATURAS

Ver guía CCN-STIC 800 Glosario de Términos y Abreviaturas del ENS.

ANEXO B. REFERENCIAS

- CCN-CERT
  https://www.ccn-cert.cni.es/

  Guías relacionadas con el ENS:

  - 800 – Glosario de Términos y Abreviaturas
  - 801 – Responsables y Funciones
  - 802 – Auditoría
  - 803 – Valoración de los Sistemas
  - 804 – Guía de Implantación
  - 805 – Política de Seguridad
  - 806 – Plan de Adecuación
  - 807 – Criptografía
  - 808 – Verificación de Cumplimiento de las Medidas (auditoría técnica)
  - 809 – Declaración de Conformidad
  - 810 – Ciclo de Creación de CERT's
  - 811 – Interconexión
  - 812 – Seguridad en Servicios Web
  - 813 – Componentes Certificados
  - 814 – Seguridad en el Servicio de Correo
  - 815 – Indicadores y Métricas
  - 816 – Seguridad en Redes Inalámbricas
  - 817 – Gestión de Incidentes de Seguridad
  - 818 – Herramientas de Seguridad
  - 819 –
  - 820 - Denegación de Servicio
  - 821 – Normas de Seguridad
  - 822 – Procedimientos Operativos de Seguridad

- 823 – Seguridad en entornos Cloud
- 824 – Informe del Estado de Seguridad
- 825 – Borrado de metadatos
- 826 - Configuración SSL / TLS
- 827 - Procedimientos de actuación ante código dañino

- DSD - Australian Defence Signals Directorate (DSD)
  Top 35 Mitigation Strategies
  http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- ENS
  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.
  https://www.ccn-cert.cni.es/publico/ens/ens/index.html
- ISO/IEC 27000:2012
  Information technology – Security techniques – Information security management systems – Overview and vocabulary
- ISO/IEC 27001:2005
  Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27002:2005
  Information technology – Security techniques – Code of practice for information security management
- ISO/IEC 27003:2010
  Information technology – Security techniques – Information security management system implementation guidance
- ISO/IEC 27005:2011
  Information technology – Security techniques – Information security risk management
- Ley 11:2007
  LEY 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Manageable Network Plan
  NSA, version 2.2, April 2012
- NIST SP 800-37 Rev.1 Feb. 2010
  Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

- NIST SP 800-39 Mar. 2011
  Managing Information Security Risk: Organization, Mission, and Information System View

- NIST SP 800-53 Rev. 3 (Aug. 2009); Rev. 4 (draft Feb. 2012)
  Recommended Security Controls for Federal Information Systems,
  http://web.nvd.nist.gov/view/800-53/home
  http://csrc.nist.gov/

- RD 1065/2007
  Real Decreto 1065/2007, de 27 de julio, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos.

- RD 1720:2007
  Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

- RD 1671:2009
  Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

- SANS
  20 Critical Security Controls
  http://www.sans.org/critical-security-controls/

ANEXO C. SECURITY ENGINEERING PRINCIPLES

Principios recogidos de la guía NIST SP800-27 (Rev. A):

- Principle 1. Establish a sound security policy as the "foundation" for design.
- Principle 2. Treat security as an integral part of the overall system design.
- Principle 3. Clearly delineate the physical and logical security boundaries governed by associated security policies.
- Principle 4. Ensure that developers are trained in how to develop secure software.
- Principle 5. Reduce risk to an acceptable level.
- Principle 6. Assume that external systems are insecure.
- Principle 7. Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness
- Principle 8. Implement tailored system security measures to meet organizational security goals
- Principle 9. Protect information while being processed, in transit, and in storage.
- Principle 10. Consider custom products to achieve adequate security.
- Principle 11. Protect against all likely classes of "attacks."
- Principle 12. Where possible, base security on open standards for portability and interoperability.
- Principle 13. Use common language in developing security requirements.
- Principle 14. Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.
- Principle 15. Strive for operational ease of use.
- Principle 16. Implement layered security (Ensure no single point of vulnerability).
- Principle 17. Design and operate an IT system to limit damage and to be resilient in response
- Principle 18. Provide assurance that the system is, and continues to be, resilient in the face of expected threats.
- Principle 19. Limit or contain vulnerabilities
- Principle 20. Isolate public access systems from mission critical resources (e.g., data, processes, etc.).
- Principle 21. Use boundary mechanisms to separate computing systems and network infrastructures.
- Principle 22. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.
- Principle 23. Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.
- Principle 24. Strive for simplicity.
- Principle 25. Minimize the system elements to be trusted.
- Principle 26. Implement least privilege.
- Principle 27. Do not implement unnecessary security mechanisms.
- Principle 28. Ensure proper security in the shutdown or disposal of a system.
- Principle 29. Identify and prevent common errors and vulnerabilities.
- Principle 30. Implement security through a combination of measures distributed physically and logically.
- Principle 31. Formulate security measures to address multiple overlapping information domains.
- Principle 32. Authenticate users and processes to ensure appropriate access control decisions both within and across domains.
- Principle 33. Use unique identities to ensure accountability.