

[illegible]

SIN CLASIFICAR

Edita:



© Centro Criptológico Nacional, 2017
NIPO:785-17-027-0

Fecha de Edición: abril de 2017

José A. Mañas ha participado en la realización y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

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 (CNI), 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 (CCN) en su artículo 9.2.f).

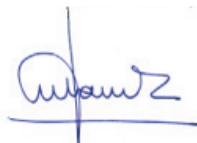
Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad 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.

El 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 (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, 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 (STIC) 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.

Abril de 2017



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

CAPÍTULO I – INTRODUCCIÓN.....	6
I.1. PRESENTACIÓN	6
I.2. INSTALACIÓN.....	6
I.2.1. ENTORNO JAVA	6
I.2.2. PILAR (WINDOWS)	6
I.2.3. PILAR (UNIX)	7
I.2.4. PILAR (MAC OS X).....	7
I.3. USO.....	7
I.3.1. PRIMERA PANTALLA.....	7
CAPÍTULO II - USO BÁSICO.....	9
II.1. CONFIGURACIÓN	9
II.2. ACTIVOS ESENCIALES	9
II.2.1. ACTIVOS ESENCIALES	9
II.2.2. IDENTIFICACIÓN Y CARACTERIZACIÓN.....	10
II.2.3. VALORACIÓN	11
II.3. ACTIVOS DE SOPORTE	12
II.4. AUTOMATIZACIÓN	13
II.5. PERFILES DE SEGURIDAD.....	14
II.5.1 RECOMENDACIÓN.....	14
II.5.2. APLICABILIDAD	15
II.5.3. VALORACIÓN	15
II.5.4. SEMÁFORO	17
II.5.4. DUDAS Y COMENTARIOS.....	17
II.6. INFORMES	17
CAPÍTULO III - USO MEDIO	19
III.1. DOMINIOS DE SEGURIDAD	19
III.2. FASES DEL PROYECTO	19
III.3. SALVAGUARDAS	20
CAPÍTULO IV - USO AVANZADO	24
IV.1. DEPENDENCIAS ENTRE ACTIVOS	24
IV.1.1. NODOS OR	25

IV.2. VALORACIÓN ACTIVO A ACTIVO	25
IV.3. AMENAZAS.....	25
IV.4. PERFILES DE SEGURIDAD – CUMPLIMIENTO	26
CAPÍTULO V – PERSONALIZACIÓN.....	27
V.1. FICHERO DE CONFIGURACIÓN.....	27
V.2. PERÍMETROS	27
V.3. PATRONES PARA INFORMES.....	28
CAPÍTULO VI - TEMAS AVANZADOS	29
VI.1. ZONAS	29
VI.2. VULNERABILIDADES.....	29
VI.3. IDIOMAS.....	30
VI.3.1. CREACIÓN DE DICCIONARIOS	30
VI.3.2. USO DE LOS DICCIONARIOS	31
VI.4. CONTROL DE ACCESO	31
VI.4.1. CONTRASEÑAS	32
VI.4.2. RESTRICCIONES DE ACCESO: DOMINIOS DE SEGURIDAD.....	32
VI.4.3. RESTRICCIONES DE ACCESO: FASES DEL PROYECTO.....	32
VI.4.4. RESTRICCIONES DE ACCESO: ZONAS	33
VI.5. BASES DE DATOS.....	33
VI.6. MODO BATCH	33
ANEXO A – NIVELES DE MADUREZ	34
ANEXO B - GLOSARIO	35
ANEXO C - REFERENCIAS.....	38

CAPÍTULO I – INTRODUCCIÓN

I.1. PRESENTACIÓN

Analizar los riesgos es identificar los riesgos potenciales y residuales en un sistema de información y comunicaciones (CIS). Se denomina riesgo a la incertidumbre sobre lo que puede pasar, teniendo en cuenta posibilidades positivas (nos van bien) o negativas (nos vienen mal). En este manual nos centraremos en los incidentes que pueden causar un perjuicio en la información y los servicios de la organización.

El análisis de riesgos proporciona información para decidir sobre la asignación de recursos, ya sean técnicos o de otro tipo, para proteger organización.

El análisis de riesgos requiere un enfoque metódico:

1. identificar el valor que hay que proteger,
2. Identificar los elementos del sistema que soportan ese valor; es decir, aquellos donde los ataques pueden causar daño,
3. establecer medidas de seguridad para protegernos contra los ataques y
4. estimar indicadores de la posición de riesgo para ayudar a los que tienen que tomar decisiones.

PILAR implementa la metodología Magerit:

[<http://administracionelectronica.gob.es/>].

I.2. INSTALACIÓN

I.2.1. ENTORNO JAVA

Se necesita un

- JRE – Entorno de ejecución Java

visite [<http://java.com>] y siga las instrucciones

paso 1: descargar

paso 2: instalación

paso 3: probar

I.2.2. PILAR (WINDOWS)

Puede instalar PILAR como administrador o como usuario normal. Los archivos se pueden instalar en cualquier lugar. Si tiene privilegios de administrador, los archivos pueden entrar en "Archivos de programa" para todo el mundo, y el registro puede tener un número de entradas para asociar PILAR a ficheros con extensión .mgr.

Cuando Java esté instalado ...

- ejecute `pilar_<version>_<lang>.exe`
- siga las instrucciones para instalar en el directorio que prefiera (varios idiomas pueden compartir el mismo directorio de instalación)
- Cuando la instalación termine, habrá un archivo

`pilar.exe`

donde haya decidido instalar el software.

I.2.3. PILAR (UNIX)

Cuando Java esté instalado...

- ejecute `pilar_linux_<version>_<lang>.jar`
- e instale la aplicación y la librería en donde considere apropiado (varios idiomas pueden compartir el mismo directorio de instalación)
- Cuando la instalación termine, habrá un archivo

`pilar.jar`

donde haya decidido instalar el software.

I.2.4. PILAR (MAC OS X)

Habitualmente, java ya se encuentra instalado en el sistema, pudiendo pasar directamente a la instalación de PILAR:

- ejecute `pilar_mac_<version>_<lang>.jar`
- e instale la aplicación y la librería en donde considere apropiado (varios idiomas pueden compartir el mismo directorio de instalación)
- al terminar la instalación, debe encontrar un fichero

`pilar.app`

I.3. USO

Ejecute `pilar`. Le pedirá un fichero configuración, que puede encontrar en dónde realizó la instalación:

ej. `STIC_es.car`

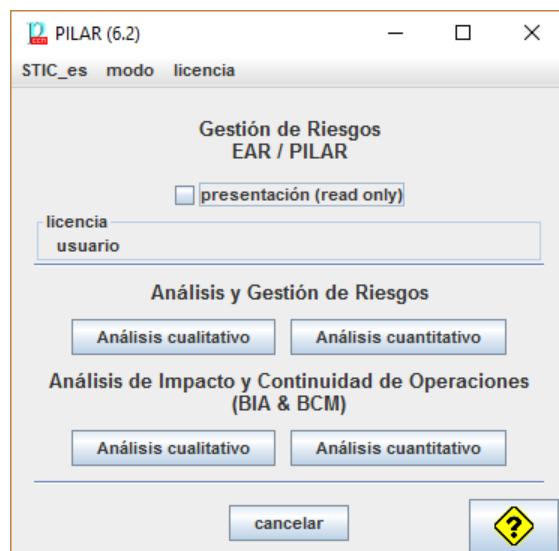
El fichero `.car` especifica un directorio para la biblioteca. Puede guardar varias librerías (varios idiomas o varias versiones) en el mismo directorio; pero sólo puede usar una en cada momento.

Si necesita más información, busque en “personalización”, en

<http://www.pilar-tools.com/en/tools/pilar/doc.html>

I.3.1. PRIMERA PANTALLA

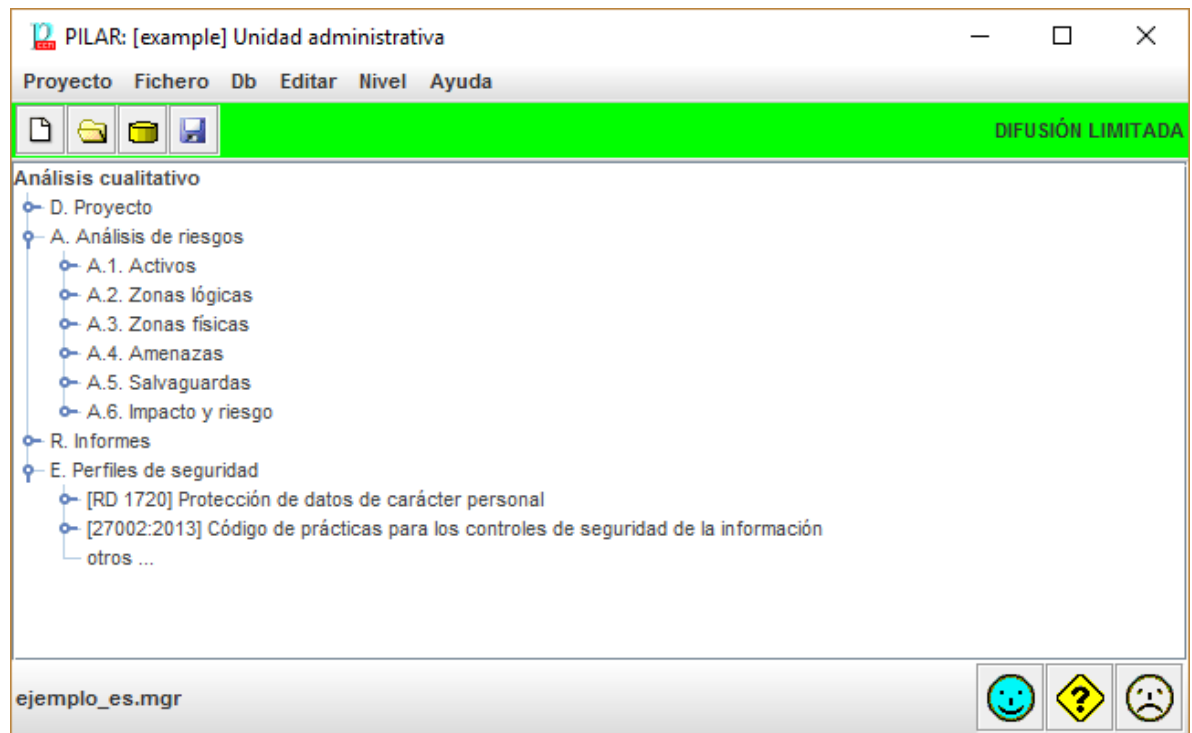
- [STIC_es] haga clic para cambiar el perfil (fichero CAR)
- [licencia] haga clic para cargar su licencia de uso (fichero LIC)
- seleccione el tipo de análisis:
 - riesgo: analiza confidencialidad, integridad, disponibilidad, ...



- bcm: analiza continuidad del negocio: interrupciones del servicio
- cualitativo: usa una escala de valores relativos
- cuantitativo: usa valores numéricos

Este manual presenta análisis cualitativo de riesgos, que es la funcionalidad más habitual.

CAPÍTULO II - USO BÁSICO



II.1. CONFIGURACIÓN

Estas son las opciones más utilizadas:

Editar >> opciones	seleccionar	
valoración	activos + dominios	se valoran los activos por dominios de seguridad
amenazas	automático	PILAR aplica un perfil estándar
fases del proyecto	conectadas	cada fase refina la anterior
probabilidad	nivel	opcional: cambia la presentación
efectos	porcentaje	opcional: cambia la presentación
madurez	madurez	opcional: cambia la presentación
fases	seleccionar PILAR	se presenta la fase PILAR
transferencia de valor entre dimensiones	seleccionar transferencia de valor entre dimensiones	PILAR calcula cómo una dimensión de seguridad depende de otras

II.2. ACTIVOS ESENCIALES

II.2.1. ACTIVOS ESENCIALES

Son activos esenciales la información y los servicios manejados por el sistema. Representan los requisitos de seguridad establecidos por sus dueños. Los activos esenciales existen antes de detallar la implementación del sistema de información:

- Su jefe le dice: “Esta es la información que debemos tratar, y estos los servicios que debemos proporcionar”.
- “Comprendo. Me hago cargo”, respondemos.

Los activos esenciales pueden ser de tipo ‘información’ o de tipo ‘servicio’. O una mezcla de ambos. Lo que es importante es queden identificados por un nombre que se entienda por la organización.

Los activos esenciales imponen requisitos de seguridad al sistema. En PILAR hablamos de niveles de seguridad. Los activos de información suelen estar caracterizados por sus requisitos de confidencialidad e integridad. Los activos de servicio suelen estar caracterizados por su disponibilidad. Y unos y otros pueden imponer requisitos de autenticidad y trazabilidad.

II.2.2. IDENTIFICACIÓN Y CARACTERIZACIÓN

Análisis de riesgos > Activos > Identificación

Capas > Nueva capa

[B] Activos esenciales

Activos > Nuevo activo

[INFO] Información del negocio

Seleccione las clases que considere oportunas

[example] análisis de riesgos > activos > identificación de activos > activo

código: D_files

nombre: Expedientes en curso

dato	valor
descripción	estado de los procesos de tramitación abiertos
contenido	almacena temporalmente datos financieros de los ciudadanos
propietario	jefe de servicio de tramitación

arriba abajo nueva eliminar estándar limpiar

Fuentes de información: info_owner

dominio: descripción

CLASES DE ACTIVOS

- [essential] Activos esenciales
 - [essential.info] información
 - [D.biz] datos de interés para el negocio
 - [D.com] datos de interés comercial
 - [D.adm] datos de interés para la administración pública
 - [D.vr] datos vitales (registros de la organización)
 - [D.per] datos de carácter personal
 - [D.per.A] nivel: alto
 - [D.per.M] nivel: medio
 - [D.per.B] nivel: bajo
 - [D.classified] información clasificada
 - [D.classified.TS] SECRETO
 - [D.classified.S] RESERVADO
 - [D.classified.C] CONFIDENCIAL
 - [D.classified.R] DIFUSIÓN LIMITADA
 - [D.classified.UC] SIN CLASIFICAR
 - [essential.service] servicio
 - [arch.bp] proceso de negocio

Añada los activos de información que necesite para capturar todos los elementos que son relevantes para los directores. Puede usar activos agregados que representen varios activos de información con igual valoración.

Luego, añada los servicios que manejan la información:

[example] análisis de riesgos > activos > identificación de activos > activo

código
S_in_person

nombre
Tramitación presencial

dato	valor
descripción	ventanilla de atención presencial al ciudadano
identificación	usuario + contraseña
responsable	jefe de servicio de tramitación

arriba abajo nueva eliminar estándar limpiar

descripción

CLASES DE ACTIVOS

- [essential] Activos esenciales
 - ☒ [essential.service] servicio
- [S] Servicios
 - [S.prov] proporcionado por nosotros
 - ☒ [S.prov.int] interno (usuarios y medios de la propia organización)
 - ☒ [S.prov.ftp] transferencia de ficheros

Puede ser útil combinar información y servicios en un único activo:

ACTIVOS

[B] Activos esenciales: información & servicios

[misión] unidad de negocio X

[example] análisis de riesgos > activos > identificación de activos > activo

código
misión

nombre
unidad de negocio X

dato	valor

arriba abajo nueva eliminar estándar limpiar

descripción

CLASES DE ACTIVOS

- [essential] Activos esenciales
 - [essential.info] información
 - ☒ [D.biz] datos de interés para el negocio
 - ☒ [D.classified] información clasificada
 - ☒ [D.classified.R] DIFUSIÓN LIMITADA
 - [essential.service] servicio
 - ☒ [essential.service.operations] operaciones

Ha terminado cuando tenga suficientes elementos de información y de servicio para hablar con sus directores de los requisitos de seguridad del sistema.

II.2.3. VALORACIÓN

Análisis de riesgos > Activos > Valoración de los dominios

Para los activos de información, valore el nivel requerido de seguridad:

- entre 0 (despreciable) y 10 (el máximo)
- con respecto de la confidencialidad, la integridad, ... la autenticidad y la trazabilidad
- si no especifica ningún nivel, PILAR entenderá que el activo no tiene requisitos significativos en esa dimensión (por ejemplo, no hay requisitos de confidencialidad en la información que es pública)

Para los activos de servicio:

- requisitos de disponibilidad

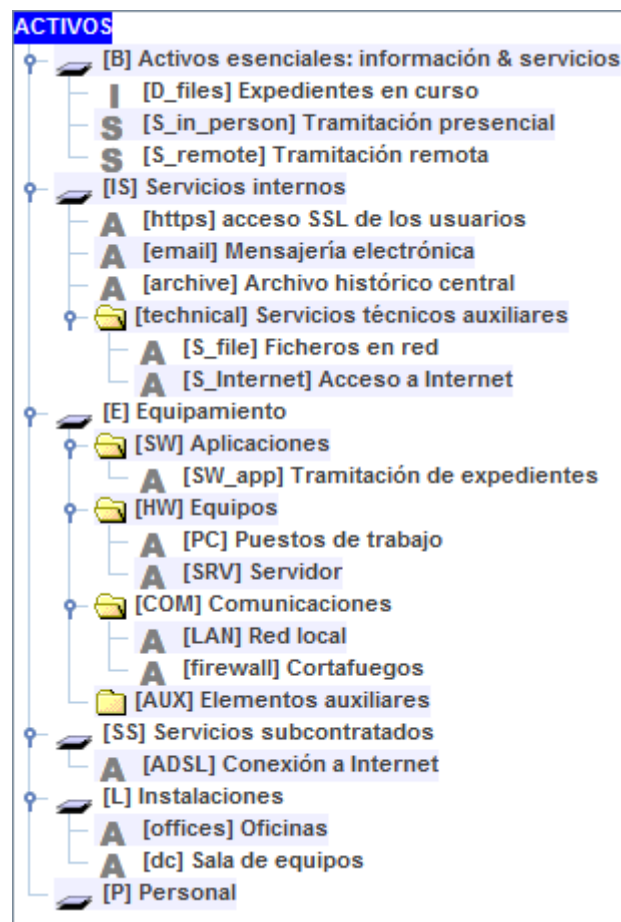
activo / dominio de seguridad	[D]	[I]	[C]	[A]	[T]	[V]
[example] Unidad administrativa						
[essential] Activos esenciales	[4]	[4]	[7]	[7]	[7]	
[D_files] Expedientes en curso		[4]	[7]	[4]	[4]	
[S_in_person] Tramitación presencial	[4]			[7]	[7]	
[S_remote] Tramitación remota	[1]			[7]	[7]	
Dominios de seguridad						
[base] red corporativa	[4]	[4]	[7]	[7]	[7]	

De momento, todos los activos están en el mismo dominio de seguridad, el dominio 'base', cuyos requisitos de seguridad son los máximos en cada dimensión de seguridad de los diferentes activos.

II.3. ACTIVOS DE SOPORTE

Análisis de riesgos > Activos > Identificación

Añada otros activos, materiales o intangibles, que constituyen el sistema de información. Puede organizarlos en capas y grupos por claridad, pero a PILAR solo le interesan los activos en sí.



Cada activo debe calificarse con las clases que utiliza PILAR para proponer amenazas (oportunidades para los atacantes) y proponer contramedidas (de protección).

[example] análisis de riesgos > activos > identificación de activos > activo

código: SRV

nombre: Servidor

dato	valor
descripción	equipo medio con disco local
servicios	ficheros, comunicaciones, email, servidor web
propietario	administrador de sistemas
cantidad	1 + contrato de mantenimiento hw y sw

arriba abajo nueva eliminar estándar limpiar

Fuentes de información:

dominio: [base] red corporativa

descripción

CLASES DE ACTIVOS

- [D] Datos / Información
 - ☒ [D.conf] datos de configuración
 - ☒ [D.log] registro de actividad (log)
- [SW] Aplicaciones (software)
 - ☒ [SW.std] estándar (off the shelf)
 - ☒ [SW.std.www] servidor de presentación
 - ☒ [SW.std.app] servidor de aplicaciones
 - ☒ [SW.std.email_server] servidor de correo electrónico
 - ☒ [SW.std.file] servidor de ficheros
 - ☒ [SW.std.os] sistema operativo
 - ☒ [SW.std.os.windows] windows
 - ☒ [SW.sec] herramientas de seguridad
 - ☒ [SW.sec.av] anti virus
- ☒ [HW] Equipamiento informático (hardware)
 - ☒ [HW.mid] equipos medios
- ☒ [Media] Soportes de información
 - ☒ [Media.electronic] electrónicos
 - ☒ [Media.electronic.disk] discos

La granularidad de los activos puede variar desde activos muy detallados, hasta activos que representan un subsistema completo en sí mismos. Tendrá que encontrar un punto de equilibrio entre una descripción lo bastante detallada para conocer los riesgos a los que nos exponemos, y lo bastante compacta para no perdernos en los detalles. Típicamente, un número de activos entre decenas y unos pocos cientos.

II.4. AUTOMATIZACIÓN

PILAR se encarga automáticamente de trasladar los requisitos de seguridad (niveles) de los activos esenciales a los activos de soporte. Puede revisarlos y ajustarlos manualmente si fuera necesario:

Análisis de riesgos > Activos > valoración de los activos

PILAR aplica un perfil típico de ataque; es decir,

- identifica amenazas típicas
- propone valores típicos de probabilidad y consecuencias (estimadas como una fracción del valor transferido desde los activos esenciales).

En conjunto, PILAR elabora un mapa de riesgos: los riesgos inherentes al sistema (riesgo potencial) que puede consultar

- desde un punto de vista técnico:
Análisis de riesgos > Impacto y riesgo > Valores acumulados > ...
- desde el punto de vista del negocio:
Análisis de riesgos > Impacto y riesgo > Valores repercutidos > ...

II.5. PERFILES DE SEGURIDAD

Un perfil de seguridad es un conjunto de contramedidas, técnicas y procedimentales. PILAR puede cargar uno o más para ayudar a los usuarios

- a tratar los riesgos técnicos por medio de contra medidas
- a cumplir requisitos de acreditación

Perfiles de seguridad > 27002:2013 > Valoración

Esta pantalla presenta el cumplimiento de un cierto perfil de seguridad, compuesto por controles (✓) que pueden ser refinados o alineados con salvaguardas (⚠).

rec...	control	du...	fu...	ap...	co...	current	target	PILAR
	[27002:2013] Código de prácticas para los controles de seguridad de la información					_-L5	_-L5	L2-L5
2	✓ [5] Políticas de seguridad de la información					L0	L5	L2
7	✓ [6] Organización de la seguridad de la información			...		_-L5	_-L5	L2-L4
7	✓ [7] Seguridad relativa a los recursos humanos					_-L1	_-L5	n.a.
7	✓ [8] Gestión de activos					_-L5	_-L5	L2-L4
7	✓ [9] Control de acceso					_-L5	_-L5	L2-L4
4	✓ [9.1] Requisitos de negocio para el control de acceso					L0-L5	L3-L5	L2-L3
7	✓ [9.2] Gestión de acceso de usuario					_-L5	_-L5	L2-L4
5	✓ [9.2.1] Registro y baja de usuario					L0-L5	L3-L5	L2-L3
3	✓ [9.2.2] Provisión de acceso de usuario					L0-L5	L3-L5	L2-L3
7	✓ [9.2.3] Gestión de privilegios de acceso					_-L5	_-L5	L2-L4
7	⚠ [H.ST.1] Se separan las responsabilidades de administración y operación					L5	L5	L4
5	⚠ [IA.5] Cuentas especiales (administración)					_-L1	_-L3	L2-L3

II.5.1 RECOMENDACIÓN

Para cada medida de seguridad, la columna [recomendación] presenta una estimación de la importancia relativa de esa fila.

Es un valor en el rango [nulo .. 10], estimado por PILAR teniendo en cuenta los activos, las dimensiones de seguridad y el nivel de riesgo que trata la medida.

La celda está en gris si PILAR no ve utilidad para la medida: no sabría a qué riesgo aplicarla.

(o) – overkill – PILAR piensa que la medida es desproporcionada para los riesgos a que se enfrenta el sistema

(u) – under kill – PILAR piensa que la medida es insuficiente para los riesgos a que se enfrenta el sistema

II.5.2. APLICABILIDAD

En la columna [aplica] puede indicar si la fila es aplicable o no. Tenga en cuenta que algunos perfiles marcan algunos controles como obligatorios a efectos de conformidad. PILAR marca estos controles como **M**. Incluso para los controles que la norma marca como obligatorios, usted puede decidir que en su caso no es aplicable (bien porque el sistema no cumple algún requisito, bien porque dispone de controles compensatorios).

Por ejemplo, si carece de servidores (porque usa servicios virtuales en la nube), entonces no hay que proteger ningún equipo. PILAR pone la recomendación en gris.

O puede ocurrir que el control sería útil, pero el sistema dispone de mejores medidas de protección.

Algunas medidas pueden ser desproporcionadas (overkill), y puede argumentarse que no se justifican. Esto no hace que la medida no sea aplicable. Si decide no implantarla (madurez L0), el riesgo permanece y PILAR lo presenta. Normalmente, una medida que no se justifica va asociada a un riesgo bajo que se acepta tal cual. Cuando un control obligatorio se marca como 'n.a.', PILAR mantiene el color para recordar que es una situación singular.

Puede usar la columna [recomendación] como una guía, pero al final será su mejor criterio el que determine qué hacer. Tenga en cuenta que si el sistema va a ser objeto de una acreditación, el inspector requerirá una buena explicación para eliminar una fila. La explicación puede introducirse como un comentario en su columna correspondiente.

Cuando selecciona un control y lo marca como 'n.a.', todos los controles 'hijos' quedan marcados como 'n.a.'; pero la no aplicabilidad no se transmite a las salvaguardas bajo el control. Puede ser que haya unas salvaguardas que sí y otras que no bajo el mismo control. Queda de su mano marcarlas manualmente.

II.5.3. VALORACIÓN

control	current	target	PILAR
♀ ✓ [9.1] Requisitos de negocio para el control de acceso	L0-L5	L3-L5	L2-L3
♀ ✓ [9.1.1] Política de control de acceso	L0-L5	L3-L5	L2-L3
♂ [AC.1.1] Se dispone de normativa para el control de accesos	L0-L5	L3	L2
♂ [H.ST.3] Se definen roles con autorización exclusiva para realizar tareas	L1	L5	L2-L3
♀ ✓ [9.1.2] Acceso a las redes y a los servicios de red	L0-L3	L5	L2
♀ [COM.op.1.1] Se dispone de normativa de uso de los servicios de red	L0-L3	L5	L2
♂ [COM.op.1.1.1] Se identifican las redes y los servicios a los que se puede acceder	L3	L5	L2
♂ [COM.op.1.1.2] Se dispone de normativa relativa a las autorizaciones de acceso a las redes y servicios	L0	L5	L2
♂ [COM.op.1.1.3] Se dispone de normativa relativa a la protección de los accesos a las redes y servicios	L0	L5	L2

Las columnas presentan fases del proyecto. Sirven para evaluar la madurez de las medidas en varios momentos y poder observar la evolución de la seguridad del sistema. Típicamente, hay 2 fases: la situación actual y adónde nos proponemos llegar. Una última columna, PILAR sirve para que PILAR proponga un objetivo "razonable" o "prudente".

La valoración se realiza usando niveles de madurez (ver Anexo A). Para medidas sencillas, tenemos un valor simple de madurez entre L0 y L5. Para medidas compuestas, PILAR muestra el rango (min-max) de la madurez de los componentes. Existe la opción de presentar la madurez del conjunto como una aproximación teniendo en cuenta la madurez ‘media’ de los componentes.

Se espera del usuario que valore la madurez de cada salvaguarda en cada fase. Algunos trucos pueden ayudar a agilizar la tarea:

- **IMPORTAR:** si dispone de la valoración realizada en otro análisis de riesgos, puede importarla.
- **SUGERENCIA:** empiece con una valoración global, a bulto, de todas las medidas y luego vaya refinando expandiendo el árbol
- La madurez de una medida en una fase se traslada a las fases siguientes, salvo que se introduzca un valor explícito
- Si introduce un valor en una fila, éste se propaga a los componentes hijos
- Los valores de madurez de los hijos se propagan al padre como rango

Cuando una medida se marca como XOR, se puede elegir cuál de los componentes optativos se va a utilizar en este sistema:

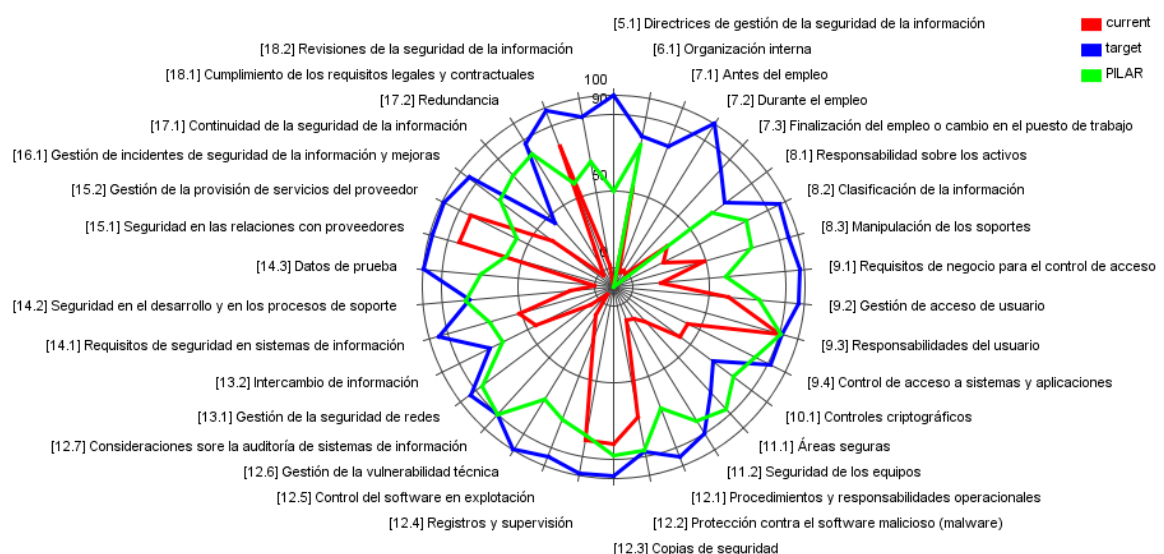
clic derecho > seleccionar

Presentación

Puede indicarle a PILAR que presente niveles de madurez (simples, rangos, o una aproximación a la madurez media=, o que presente la madurez interpretada como un porcentaje de efectividad, o que compare la madurez presente con la recomendación de PILAR.

Presentación gráfica

Seleccione en la columna [1] las filas que desea llegar al gráfico:



II.5.4. SEMÁFORO

El semáforo [columna 3] resume en un color si la madurez de la medida es suficiente o no.

A fin de calcular el color del semáforo, PILAR usa 2 referencias

VERDE: la madurez objetivo

- clic con el botón derecho en la cabecera de la fase que desea usar como objetivo
- la cabecera de la columna seleccionada se pinta en VERDE

ROJA: la madurez evaluada

- haga clic en la cabecera de la fase que desea evaluar
- la cabecera de la fase seleccionada se pinta en ROJO

Usando la información anterior, PILAR decide un color:

AZUL	la madurez actual (ROJA) está por encima del objetivo (VERDE)
VERDE	la madurez actual (ROJA) está a la altura del objetivo (VERDE)
AMARILLO	la madurez actual (ROJA) está por debajo del objetivo (VERDE)
RED	la madurez actual (ROJA) está muy por debajo del objetivo (VERDE)
GRIS	la salvaguarda no es aplicable

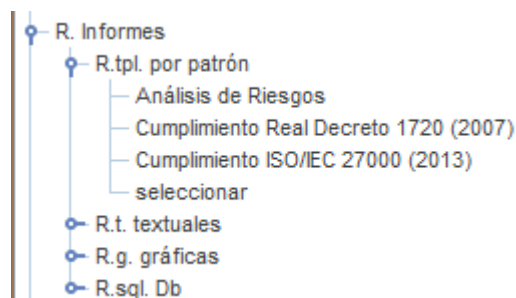
II.5.4. DUDAS Y COMENTARIOS

En la columna [dudas] puede marcar una medida como que quedan temas pendientes.

La columna [comentario] puede albergar un comentario referente a la medida.

II.6. INFORMES

PILAR se distribuye con una serie de informes predefinidos. Algunos informes están codificados dentro de la herramienta (textuales y gráficos), mientras que otros vienen regidos por patrones. Los patrones son plantillas RTF que pueden editarse con muchos procesadores de textos.



Las gráficas pueden ser útiles para presentaciones, como gráficos a adjuntar al texto.

Algunos informes textuales son valiosos en sí mismos, a veces como informe final del análisis, a veces como material de trabajo para que los propietarios de los activos puedan aportar o validar información de sus propiedades.

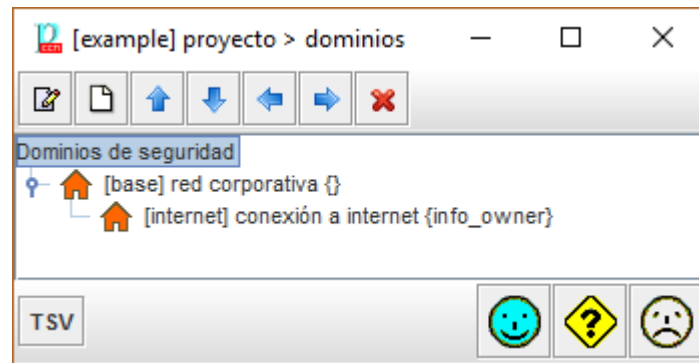
CAPÍTULO III - USO MEDIO

III.1. DOMINIOS DE SEGURIDAD

Los activos pueden ser distribuidos en dominios de seguridad. un dominio de seguridad define un perfil de ataque y un perfil de protección propios, permitiendo agrupar los activos desde el punto de vista de su exposición y su protección.

Proyecto > Dominios de seguridad

Para identificar dominios de seguridad



Los dominios de seguridad pueden anidarse unos dentro de otros formando una jerarquía de dominios. Un dominio es 'hijo' de otro. La jerarquía se utiliza para valorar salvaguardas y perfiles de seguridad. El dominio anidado hereda los niveles de madurez del dominio que lo contiene. De esta forma, basta valorar completamente el dominio base y luego ir refinando los cambios en los demás dominios.

A fin de valorar los activos, el usuario debe valorar los activos esenciales. PILAR traslada estos valores a todos los activos del dominio en el que está el activo esencial y a todos los dominios asociados a él.

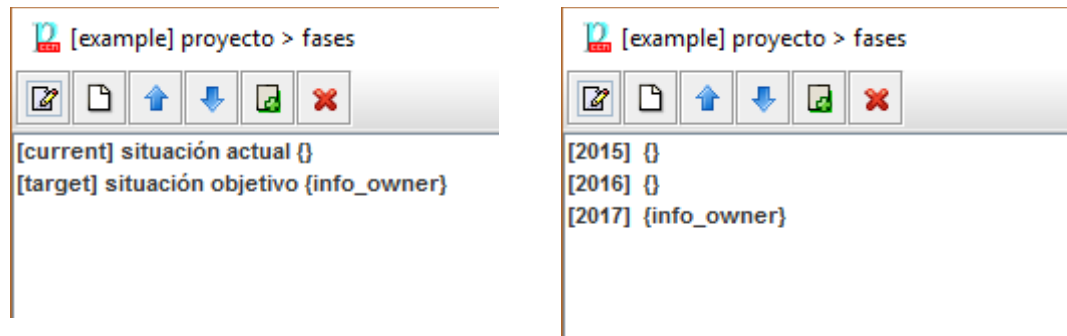
activo / dominio de seguridad	[D]	[I]	[C]	[A]	[T]	[M]
[example] Unidad administrativa						
[essential] Activos esenciales	[4]	[4]	[7]	[7]	[7]	
[D_files] Expedientes en curso		[4]	[7]	[4]	[4]	
[S_in_person] Tramitación presencial	[4]			[7]	[7]	
[S_remote] Tramitación remota	[1]			[7]	[7]	
Dominios de seguridad						
[base] red corporativa	[4]	[4]	[7]	[7]	[7]	
[internet] conexión a internet	[1]			[7]	[7]	

III.2.FASES DEL PROYECTO

Las fases del proyecto permiten trabajar con fotos de la seguridad del sistema en diferentes momentos.

Proyecto > Fases del proyecto

Para identificar y ordenar las fases.



Las fases se usan cuando se valoran salvaguardas y perfiles de evaluación. La valoración en una fase se traslada automáticamente a las siguientes fases hasta que se modifique explícitamente.

[example] análisis de riesgos > salvaguardas > Eficacia de las salvaguardas

Editar Expandir Exportar Importar Estadísticas

[base] red corporativa Fuentes de información

as...	tdp	salvaguarda	du...	fue...	co...	rec...	cur...	target	PILAR
SALVAGUARDAS									
G	EL	[IA] Identificación y autenticación				8	L0-L3	L0-L2	L2-L5
G	std	[IA.1] Se dispone de normativa de identificación y autenticación				3	L1		L3
G	proc	[IA.2] Se dispone de procedimientos para las tareas de identificación y autenticación				3	L1		L3
G	EL	[IA.3] Identificación de los usuarios				5	L0-L2	L1-L2	L3
G	EL	[IA.3.1] Cada usuario recibe un identificador exclusivo (no compartido)				5	L0	L1	L3
G	EL	[IA.3.2] La identificación del usuario no indica ni su función ni su nivel de privilegios				3	L2		L3
T	EL	[IA.3.3] Las cuentas de invitados están sometidas a un control estricto				3	L1		L3
G	EL	[IA.4] Gestión de la identificación y autenticación de usuario				5	L2	L2	L2-L3
G	EL	[IA.5] Cuentas especiales (administración)				5	L1	L1	L2-L3
T	EL	[IA.6] Canal seguro de autenticación				6	L2		L4

- 1 + fuentes operación sugiere buscar >>

III.3. SALVAGUARDAS

PILAR ofrece un amplio catálogo de medidas de seguridad bajo el nombre de salvaguardas. Las salvaguardas se organizan en forma de árbol, donde las salvaguardas cercanas a la raíz se van refinando en medidas más detalladas según bajamos por el árbol.

Las salvaguardas se seleccionan por dominios de seguridad. Cada dominio puede tener diferentes salvaguardas: de pende de los riesgos sobre sus activos.

PILAR calcula un nivel de recomendación (entre 0 y 10) para cada salvaguarda en cada dominio, teniendo en cuenta:

- las clases de los activos en el dominio
- El nivel de seguridad requerido, directa o indirectamente, para cada dimensión para cada activo en el dominio
- la capacidad de cada salvaguarda para proteger cada dimensión
- la potencia intrínseca de la salvaguarda

En primer lugar, el usuario puede determinar el subconjunto de salvaguardas que son de aplicación en cada dominio. Hay que marcar como n.a. las que no son de aplicación

[example] análisis de riesgos > salvaguardas > identificación

Editar Expandir Exportar Ver Estadísticas

[base] red corporativa

as...	tdp	salvaguarda	du...	fue...	co...	rec...	on ...	apli...
G	CR	[IR] Gestión de incidentes				6		
T	PR	[tools] Herramientas de seguridad				8		...
T	EL	[tools.AV] Herramienta contra código dañino				8		
T	DC	[tools.IDS] IDS/IPS: Herramienta de detección / prevención de intrusión				6		
T	EL	[tools.conf] Herramienta de chequeo de configuración				6		
T	MN	[tools.traffic] Herramienta de monitorización de tráfico				5		
T	MN	[tools.DLP] DLP: Herramienta de monitorización de contenidos				5		
T	MN	[tools.HP] Honey net / honey pot						n.a.
T	DC	[tools.SFV] Verificación de las funciones de seguridad				6		
G	CR	[V] Gestión de vulnerabilidades				6		
T	MN	[A] Registro y auditoría				7		
G	RC	[BC] Continuidad del negocio				5		
G	AD	[G] Organización				4		
G	AD	[E] Relaciones Externas				5		
G	AD	[NEW] Adquisición / desarrollo				5		






- 1 + fuentes eliminar recomendación sólo si ...

La columna [aspecto] presenta G para aspectos de gestión, T para aspectos técnicos, F para temas de seguridad física y P para lo referente al personal.

La columna [tdp] presenta el tipo de protección que proporciona la salvaguarda

- | | |
|---------------------------------|---------------------------------------|
| — PR – prevención | — AD – administrativa |
| — DR – disuasión | — AW – concienciación |
| — EL – eliminación | — DC – detección |
| — IM – minimización del impacto | — MN – monitorización |
| — CR – corrección | — std – norma |
| — RC – recuperación | — proc – procedimiento |
| | — cert – certificación o acreditación |

No todas las salvaguardas son igual de importantes:
















	máximo peso	crítica
	peso alto	muy importante
	peso normal	importante
	peso bajo	interesante
	aseguramiento: componentes certificados	

A continuación, puede introducir la evaluación de la madurez de cada salvaguarda en cada fase en cada dominio de seguridad. Tenga en cuenta que los valores se heredan en dominios anidados, salvo que se modifiquen manualmente. Y los valores en una fase se mantienen en las fases siguientes, salvo que se modifiquen manualmente.

[example] análisis de riesgos > salvaguardas > Eficacia de las salvaguardas

Editar Expandir Exportar Importar Estadísticas

[base] red corporativa Fuentes de información

as...	tdp	salvaguarda	dudas	fuen...	com...	reco...	cur...	target	PILAR
		SALVAGUARDAS							
G	EL	 [A] Identificación y autenticación				8	L0-L3	L0-L2	L2-L5
T	EL	 [AC] Control de acceso lógico				7	_L5	_L5	L2-L4
G	PR	 [D] Protección de la Información				6	_L5	_L5	L2-L4
G	EL	 [K] Protección de claves criptográficas				8	_L3	_L5	L2-L5
G	PR	 [S] Protección de los Servicios				6	L0-L5	L3-L5	L2-L4
G	PR	 [SW] Protección de las Aplicaciones Informáticas (SW)				7	_L5	_L5	L2-L4
G	PR	 [HW] Protección de los Equipos Informáticos (HW)				7	_L5	_L5	L2-L4
G	PR	 [COM] Protección de las Comunicaciones				8	_L5	_L5	L2-L5
G	PR	 [IP] Sistema de protección de frontera lógica					_L2	_L5	n.a.
G	PR	 [MP] Protección de los Soportes de Información				7	_L2	_L5	L2-L4
G	PR	 [AUX] Elementos Auxiliares		phy...		6	_L5	_L5	L2-L4
F	PR	 [L] Protección de las Instalaciones		phy...		6	_L5	_L5	L2-L4
F	EL	 [PPS] Protección del perímetro físico				5	_L2	_L5	L2-L3
P	PR	 [PS] Gestión del Personal					_L1	_L5	n.a.
G	PR	 [PDS] Servicios potencialmente peligrosos					L1-L2	L4-L5	n.a.

- 1 + fuentes operación sugiere buscar >>

El usuario puede pedir a PILAR que sugiera salvaguardas para un cierto dominio en una cierta fase, teniendo en cuenta las necesidades de seguridad y la fortaleza propia de la salvaguarda.

[example] análisis de riesgos > salvaguardas > Eficacia de las salvaguardas

Editar Expandir Exportar Importar Estadísticas

[base] red corporativa Fuentes de información

as...	tdp	salvaguarda	dudas	fuen...	com...	reco...	cur...	target	PILAR
G	CR	de incidentes				4	L0-L2	L2-L3	L2-L3
G	IM	[IR.3] Contención del incidente				6	-L2	-L5	L3-L4
G	AD	[IR.3.1] El personal designado cubre las 24h los 7 días de la semana				3	L1	L3	L3
G	IM	[IR.3.2] El fallo del sistema deja a este en un estado controlado				3	L1	L3	L3
G	IM	[IR.3.3] Se suspenden cautelarmente los trabajos en el sistema afectado				6	L2	L5	L4
G	IM	[IR.3.4] Se aísla cautelarmente el sistema afectado				6			L4

[IA.7.3.2] El certificado se inhabilita cuando se ve comprometido o hay sospecha de ello

[IR.3.4] Se aísla cautelarmente el sistema afectado

[L.3.5.3.4] Existe un plan de emergencia para hacer frente a la violencia

[L.6.8] Eliminación residuos

[tools.AV.b] Se bloquea el acceso a sitios web peligrosos (blacklisting)

1 fuentes operación sugiere buscar >>

CAPÍTULO IV - USO AVANZADO

IV.1. DEPENDENCIAS ENTRE ACTIVOS

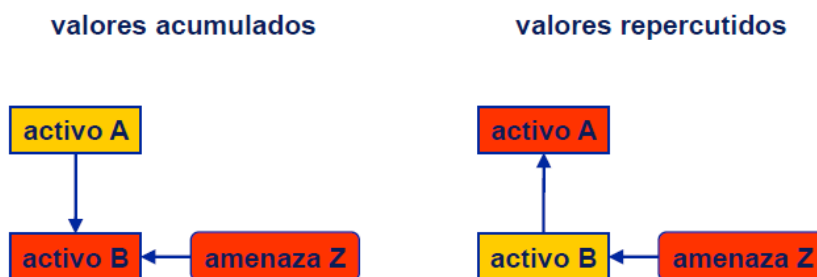
La aproximación de trasladar uniformemente los requisitos de seguridad a todos los activos en el mismo dominio es muy rápida, pero a veces puede resultar excesivamente simplista. Por ejemplo, cuando cada información y cada servicio usan sólo algunos servidores, no todos.

Las dependencias proporcionan una transferencia controlada de valor.

Hay que activar el uso de dependencias:

Editar > Opciones > Valoración > activos + dependencias

Ahora podemos indicar a PILAR que un activo A depende de un activo B:

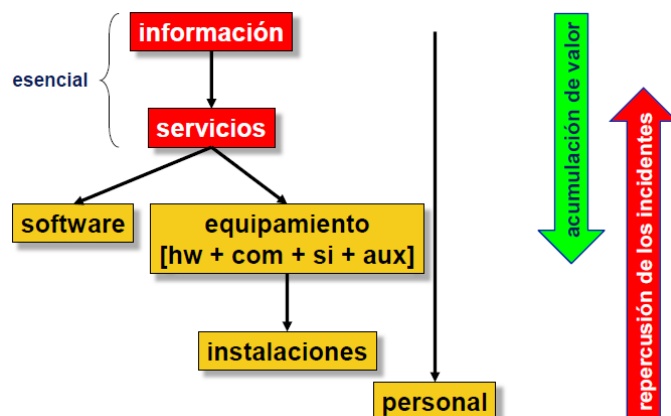


- los requisitos de seguridad (niveles de valoración) del activo A se transfieren al activo B
- los ataques en el activo B tienen un efecto directo sobre el valor acumulado en B
- los ataques en el activo B tienen un efecto indirecto (repercutido) en el activo A

Establecer un sistema correcto de dependencias lleva tiempo, y es difícil de mantener; pero proporciona un análisis ajustado de los riesgos.

Como reglas generales:

- la información esencial depende de los servicios esenciales
- los servicios esenciales dependen del equipamiento (hw, sw, comunicaciones y soportes de información)
- los equipos materiales dependen de las instalaciones
- todos los activos dependen de los usuarios que puede dañarlos con sus actividades



IV.1.1. NODOS OR

Algunos activos pueden ser caracterizados como nodos OR. Esto implica un comportamiento especial durante la transferencia de valor:

- La disponibilidad no se transmite a los hijos de los nodos OR, excepto a aquellos nodos descendientes a los que se pueda llegar a través de todas las ramas (hijos) del nodo OR



Es decir, los nodos OR representan formas alternativas de provisionar un servicio. Todas las ramas deben mantener los requisitos de seguridad de la información (confidencialidad, integridad, etc.) pero la disponibilidad o se traslada ya que cada rama tiene una alternativa que la respalda. Solamente los nodos compartidos (puntos únicos de fallo) reciben los requisitos de disponibilidad del nodo OR.

IV.2. VALORACIÓN ACTIVO A ACTIVO

Puede incluso evitar la valoración por dominios y no establecer ninguna dependencia. Ahora cada activo debe ser valorado individualmente. Es muy laborioso y difícil de mantener cuando el sistema cambia. Y PILAR no puede calcular riesgos repercutidos.

IV.3. AMENAZAS

Por defecto, PILAR aplica un perfil estándar de amenazas sobre sus activos. Este perfil identifica amenazas sobre cada activo, así como los valores de probabilidad y consecuencias. El perfil está en un fichero externo, bien en formato Excel o en formato xml. Busque TSV en el fichero de configuración CAR.

El usuario puede editar el fichero TSV. Incluso puede tener varios ficheros TSV que apliquen en diferentes dominios de seguridad. El uso de ficheros externos es ideal para

- documentar los cambios
- analizar el mismo sistema de información en diferentes escenarios de ataque

También puede modificar las amenazas manualmente dentro de PILAR

Editar > Opciones > Amenazas > manual

Se desactiva el uso del perfil TSV y se controlan manualmente los valores.

Editar > Opciones > Amenazas > mix

Modo semi-manual. Primero se marcan qué amenazas se quieren sacar del modo automático, y luego podemos modificar manualmente su probabilidad y consecuencias. El TSV se sigue aplicando a las demás amenazas.

IV.4. PERFILES DE SEGURIDAD – CUMPLIMIENTO

PILAR asocia salvaguardas a controles. Y cuando cambia la madurez de los controles, la propaga a las salvaguardas asociadas. Y al revés: los cambios en la madurez de las salvaguardas se trasladan a los controles.

Este mecanismo de propagación automática puede inhibirse

Editar > Opciones > Perfil de seguridad: propagar > no

control	d...	f...	...	c...	current	target
♀ ✓ [7.1] Antes del empleo					L2 (L1-L2)	L2 (L1-L5)
♀ ✓ [7.1.1] Investigación de antecedentes					L2	L2 (L2-L5)
♂ [PS.5.3] Selección de personal					L2	L2-L5
♀ ✓ [7.1.2] Términos y condiciones del empleo					L2 (L1)	L2 (L1-L5)
♂ [PS.4] Puestos de trabajo					L1	L5
♂ [PS.5.4] Términos y condiciones de la relación laboral					L1	L1

Se aplica la regla de presentar un valor de madurez para salvaguardas sin hijos y un rango para las que tienen hijos. Y se aplica la misma regla para indicar la madurez de los controles con y sin hijos. La novedad es que los valores de los controles van separados de los valores de las salvaguardas asociadas. Cuando coinciden, se muestra simplemente un valor (individual o rango); pero si difieren, se muestran ambos

madurez_del_control (madurez_de_las_salvaguardas)

Por ejemplo, “L2 (L1-L5)” significa que las salvaguardas asociadas están en el rango L1-L5; pero el control, en su conjunto, está valorado como L2. Diremos que la madurez formal del control es L2, a efectos de cumplimiento; mientras que el valor real es L1-L5, a efectos de mitigación del riesgo.

Manualmente, puede propagar el valor de los controles a las salvaguardas (push down) o propagar el valor de las salvaguardas a los controles (pull up).

¿Por qué se ofrece esta posibilidad de separar valoraciones? Porque la asociación de controles a salvaguardas no es oficial, es una proposición de PILAR que difícilmente se le puede imponer a los inspectores de seguridad en los procesos de acreditación:

- puede que PILAR no tenga una salvaguarda que recoja exactamente los detalles de un determinado control
- la misma salvaguarda en PILAR puede referenciarse desde varios controles
- la evolución de las salvaguardas de PILAR y de los perfiles de seguridad no se puede sincronizar

CAPÍTULO V – PERSONALIZACIÓN

PILAR puede personalizarse en muchos aspectos modificando ficheros en el directorio que funciona como biblioteca.

Aquí vamos a presentar un resumen. Puede encontrar los detalles en la web

“Personalización” en <http://www.pilar-tools.com/doc/v62/>

V.1. FICHERO DE CONFIGURACIÓN

PILAR se distribuye con una serie de ficheros de configuración estándar. Los ficheros CAR. Por ejemplo

STIC_es.car

Este fichero es de texto: puede visualizarlo y editarlo y tener su propia versión del mismo.

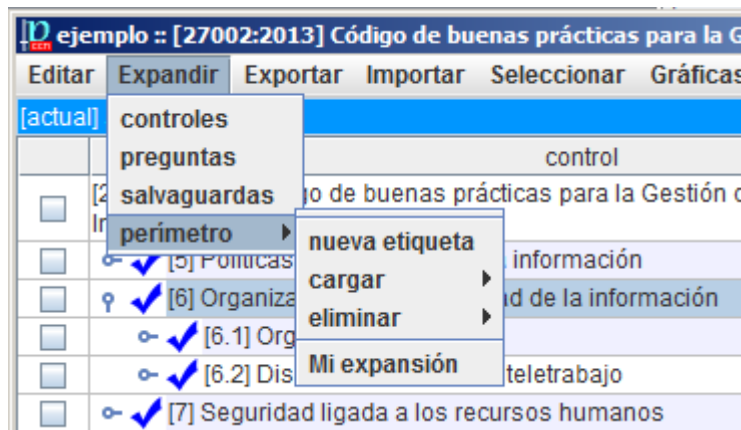
Algunos ajustes que se pueden hacer:

- añadir un icono de su organización
- añadir una pantalla de inicio (splash)
- cambiar el carácter de separación de los ficheros CSV
- ajustar las capas estándar y los datos administrativos estándar
- ajustar los niveles de confidencialidad
- añadir nuevos activos y nuevas amenazas
- añadir / modificar los criterios de valoración de activos
- usar otro(s) perfil(es) de ataque (TSV)
- ...

V.2. PERÍMETROS

PILAR recurre a estructuras arbóreas sistemáticamente para agrupar datos. Dependiendo de las circunstancias, a veces necesitamos desplegar más para ver detalles, o desplegar menos para ver el conjunto. Los perímetros son una forma de decirle a PILAR que un cierto grado de expansión nos interesa, y darle un nombre propio.

Algunos perímetros son parte de la librería estándar. El usuario puede añadir los suyos propios.



Los pasos a seguir son los siguientes:

1. Cree una nueva etiqueta con un nombre de su elección
Expandir > perímetro > nueva etiqueta
2. En el árbol, expanda o contraiga nodos hasta obtener el grado de detalle que le sea útil
3. Cargue el perímetro en su etiqueta
Expandir > perímetro > cargar > su etiqueta
4. Para cambiar el perímetro, repita los pasos 2-3

Par usar una etiqueta

Expandir > perímetro > su etiqueta

Para eliminar una etiqueta

Expandir > perímetro > eliminar > su etiqueta

V.3. PATRONES PARA INFORMES

El usuario puede preparar sus propios informes por medio de patrones, que son plantillas escritas en el formato RTF.

Ver “Patrones” en <http://www.pilar-tools.com/doc/v62/>

Puede establecer los patrones por defecto para sus análisis:

Ver “Personalización” en <http://www.pilar-tools.com/doc/v62/>

Para organizar su conjunto propio de patrones:

- edite el patrón (RTF) que necesita usando la documentación de patrones
- busque en el fichero CAR donde se indica qué patrones se van a usar (normalmente, en el fichero “reports.xml”)
- adapte reports.xml

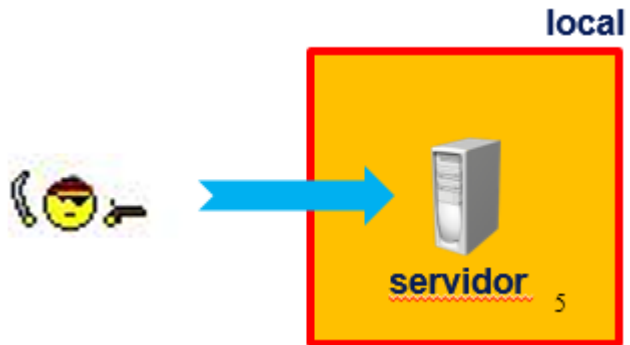
CAPÍTULO VI - TEMAS AVANZADOS

VI.1. ZONAS

Zonas son conjuntos de activos protegidos por un perímetro. Las zonas se usan en PILAR para reflejar arquitecturas de defensa en profundidad, donde los activos más valiosos están separados de los posibles atacantes.

Por ejemplo, el atacante puede estar en el exterior mientras el servidor está en un local:

- tenemos 2 zonas
 - dentro del área
 - fuera del área
- y una frontera, el local



El atacante necesita entrar, superando el perímetro de protección física (la protección que aportan paredes, puertas, ventanas, etc.) y luego podría atacar el servidor.

PILAR proporciona

- zonas lógicas, separando la red interna del exterior por medio de dispositivos y servicios de frontera (ej. cortafuegos y DMZs)
- zonas físicas, separando áreas internas de áreas externas por medios de sistemas de protección física del perímetro (ej. puertas, ventanas, ...)
- zonas tempest, separando las emisiones de cables y equipos de los posibles escuchas externos (ej. jaulas de Faraday)

Ver “Zonas” en <http://www.pilar-tools.com/doc/v62/>

VI.2. VULNERABILIDADES

PILAR analiza CVE's (Common Vulnerabilities and Exposures). Ver <https://cve.mitre.org/>

Una vulnerabilidad de la seguridad de la información es un error en los elementos del sistema que puede ser usada directamente por un hacker para acceder al sistema o a la red.

CVE considera un error como vulnerabilidad si permite al atacante violar la política de seguridad del sistema. No se consideran políticas de seguridad del tipo “puertas abiertas” en las que los usuarios son todos fiables por definición, o no se considera que el sistema corra ningún riesgo.

En el mundo CVE, una vulnerabilidad es un estado del sistema de información que

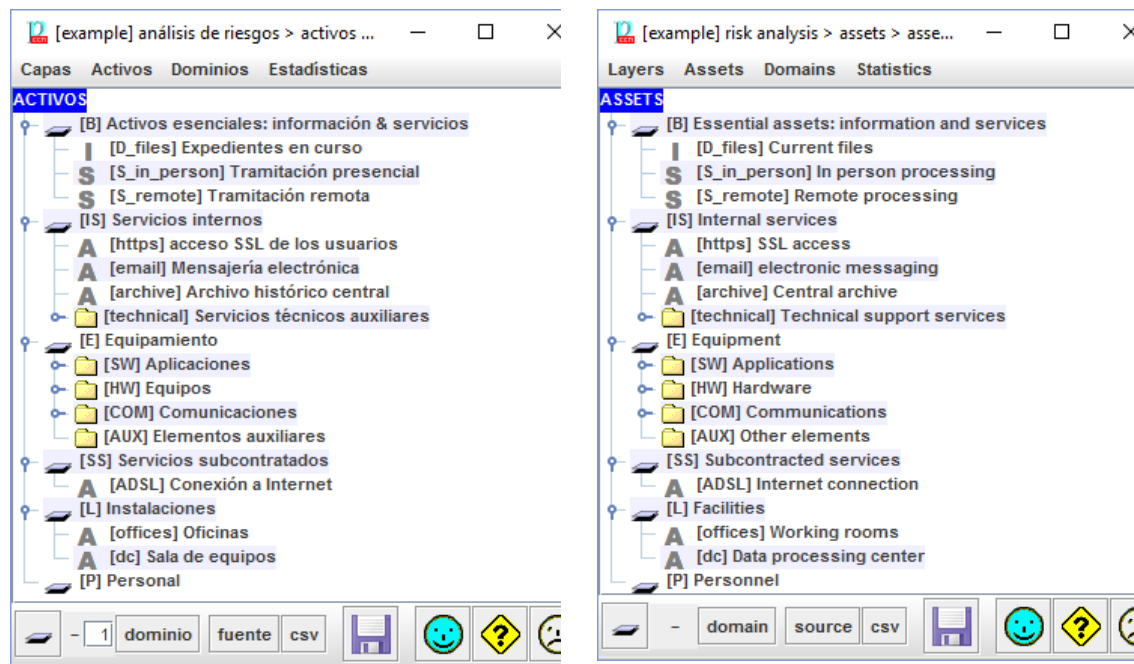
- permite a un atacante ejecutar acciones como si fuera otro usuario, o
- permite a un atacante acceder a datos violando las restricciones especificadas de control de acceso, o

- permite a un atacante suplantar la personalidad de otra entidad, i
- permite a un atacante llevar a cabo un ataque de denegación de servicio.

Ver “vulnerabilidades” en <http://www.pilar-tools.com/doc/v62/>

VI.3. IDIOMAS

Se puede partir de un proyecto escrito en un idioma I1 y verlo en otro idioma I2. PILAR utiliza los códigos de los elementos como claves y les asocia diferentes nombres en diferentes idiomas.



VI.3.1. CREACIÓN DE DICCIONARIOS

En la ventana principal

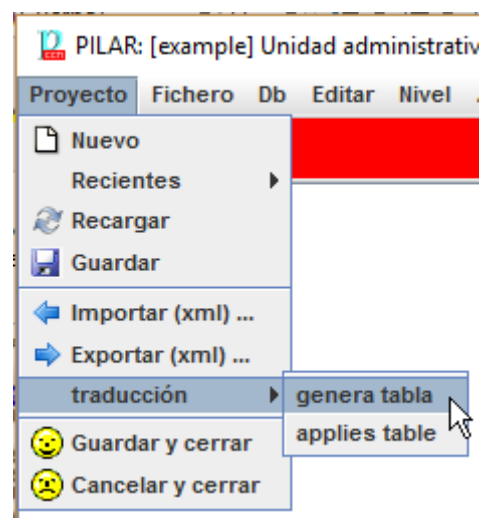
Proyecto > Traducción > generación

Seleccione un fichero

ejemplo_ml.xlsx

El resultado es un fichero Excel que el usuario puede editar.

En el fichero Excel, encontrará una tabla con tantas columnas como lenguajes. La primera fila se emplea para saber qué contiene cada columna. El usuario puede añadir nuevos idiomas añadiendo columnas.



A	B	C	D	E	F
PILAR	code	value	en	es	it
asset	firewall	name	Firewall	Cortafuegos	Firewall
asset	https	name	SSL access	acceso SSL de los usuarios	Accesso SSL degli utenti
asset	offices	name	Working rooms	Oficinas	Uffici
asset	technical	name	Technical support services	Servicios técnicos auxiliares	Servizi di assistenza tecnica
domain	base	name	corporate network	red corporativa	rete aziendale
domain	internet	name	access to Internet	conexión a internet	Internet
layer	B	name	Essential assets: information and services	Activos esenciales: información & servicios	Le attività principali: informazioni e servizi
layer	E	name	Equipment	Equipamiento	Apparecchiature
layer	IS	name	Internal services	Servicios internos	Servizi interni
layer	L	name	Facilities	Instalaciones	Siti
layer	P	name	Personnel	Personal	Personale
layer	SS	name	Subcontracted services	Servicios subcontratados	Appalti di servizi
layer	essential	name	Essential assets	Activos esenciales: información & servicios	Asset essenziali
phase	current	name	starting point	situación actual	situazione attuale
phase	target	name	long-term objective	situación objetivo	obiettivo a lungo termine
project	example	name	Public Administration Office	Unidad administrativa	Unità Amministrativa
source	info_owner	name	Information owner: Mary Steward	Responsable de la información: Mariano García	Information owner: Mary Steward
source	phys_sec	name	physical security	physical security	sicurezza fisica

VI.3.2. USO DE LOS DICCIONARIOS

Abra el proyecto con otro idioma (use el fichero CAR para elegir idioma).

Aplique el fichero de traducción.

Progetto > Traduzione > applica tabolo

PILAR cambia los nombres de los elementos, usando los que aparecen en la columna del lenguaje en el que estamos trabajando ahora.

VI.4. CONTROL DE ACCESO

PILAR proporciona medios para proteger el proyecto de modificaciones no autorizadas. Para ello recurre a las fuentes de información, a las que asocia una contraseña.

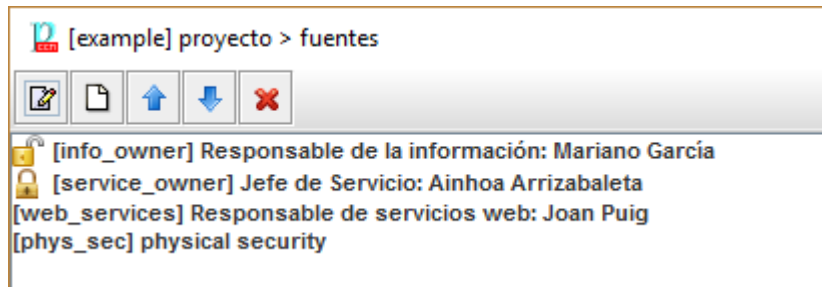
Conceptos básicos:

- una fuente de información puede tener una contraseña asociada;
- los usuarios pueden abrir una sesión en la fuente si conocen la contraseña
- los elementos pueden asociarse a una o más fuentes de información; se necesitará tener una sesión abierta en al menos una de las fuentes asociadas para tener derechos de escritura sobre el elemento; de lo contrario el elemento aparece como “solo lectura”

Los siguientes elementos tienen control de acceso

- dominios de seguridad
- zonas (lógicas, físicas y tempest)
- fases del proyecto

VI.4.1. CONTRASEÑAS



Las fuentes “info_owner” y “service_owner” tienen una contraseña. Tenemos una sesión abierta en “info_owner” y no en “service_owner”.

Proyecto > Fuentes de información > [clic derecho] > contraseña

Para establecer o eliminar una contraseña.

Proyecto > Fuentes de información > [clic derecho] > abrir

Para abrir una sesión. Se solicita la contraseña.

Proyecto > Fuentes de información > [clic derecho] > cerrar

Para cerrar una sesión.

VI.4.2. RESTRICCIONES DE ACCESO: DOMINIOS DE SEGURIDAD

Cuando un dominio de seguridad tiene fuentes de información asociadas, necesita abrir una sesión en al menos una de dichas fuentes para

- modificar las fuentes
- modificar el código, el nombre o la descripción
- modificar activos (en ese dominio)
 - crear, cambiar de dominio o eliminar
 - modificar fuentes
 - modificar el código, el nombre, la descripción o atributos administrativos
 - modificar las clases
- modificar las salvaguardas para el dominio
 - modificar las fuentes
 - modificar aplicabilidad, comentarios o valoración
- modificar controles para el dominio
 - modificar las fuentes
 - modificar aplicabilidad, comentarios o valoración

VI.4.3. RESTRICCIONES DE ACCESO: FASES DEL PROYECTO

Cuando una fase del proyecto tiene fuentes de información asociadas, necesita abrir una sesión en al menos una de dichas fuentes para

- modificar las fuentes
- modificar el código, el nombre o la descripción

- modificar las salvaguardas para la fase
 - modificar las fuentes
 - modificar aplicabilidad, comentarios o valoración
- modificar controles para la fase
 - modificar las fuentes
 - modificar aplicabilidad, comentarios o valoración

VI.4.4. RESTRICCIONES DE ACCESO: ZONAS

Cuando una zona tiene fuentes de información asociadas, necesita abrir una sesión en al menos una de dichas fuentes para

- modificar las fuentes
- modificar el código, el nombre o la descripción

VI.5. BASES DE DATOS

Se puede usar una base de datos externa. En principio, es válida cualquier base de datos SQL con una interfaz JDBC.

En la base de datos se pueden almacenar proyectos y resultados del análisis de datos. Es útil para compartir proyectos entre varios usuarios y para explotar los datos generado informes por medio de herramientas que trabajen sobre datos SQL.

Ver “tablas SQL” en <http://www.pilar-tools.com/doc/v62/>

VI.6. MODO BATCH

PILAR puede ejecutarse en modo “batch”; es decir, sin interfaz gráfica de usuario. Este modo es útil para:

- cálculos programados (por ejemplo, a media noche)
- análisis de riesgo reactivo (por ejemplo, como consecuencia del descubrimiento de una vulnerabilidad)

Ver “modo batch” en <http://www.pilar-tools.com/doc/v62/>

ANEXO A – NIVELES DE MADUREZ

PILAR utiliza niveles de madurez para evaluar salvaguardas y controles según el modelo de madurez (CMM) usado para calificar la madurez de procesos.

L0 - Inexistente

En el nivel L0 de madurez no hay nada.

L1 - Inicial / ad hoc

En el nivel L1 de madurez, las salvaguardas existen, pero no se gestionan. El éxito depende de buena suerte. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta.

El éxito del nivel L1 depende de tener personal de la alta calidad.

L2 - Reproducible pero intuitivo

En el nivel L2 de madurez, la eficacia de las salvaguardas depende de la buena suerte y de la buena voluntad de las personas. Los éxitos son repetibles, pero no hay plan para los incidentes más allá de la reacción heroica.

Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.

L3 - Proceso definido

Se despliegan y se gestionan las salvaguardas. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular de las protecciones. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado).

El éxito es algo más que buena suerte: se merece.

L4 – Gestionado y medible

Usando medidas de campo, la dirección puede controlar empíricamente la eficacia y la efectividad de las salvaguardas. En particular, la dirección puede fijar metas cuantitativas de la calidad. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza es cuantitativa, mientras que en el nivel L3, la confianza era solamente cualitativa.

L5 - Optimizado

El nivel L5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora de los procesos. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.

ANEXO B - GLOSARIO

activo

Algo que tiene un valor, tangible o intangible, que vale la pena proteger, incluyendo personas, información, infraestructuras, aspectos financieros o de reputación. [ISACA, Cybersecurity Fundamentals Glossary, 2014]

activos esenciales

Activos del sistema de información que tienen unos requisitos de seguridad propios, a diferencia de otros elementos cuyos requisitos de seguridad derivan de la información y los servicios que soportan.

En un sistema suele haber información esencial y servicios esenciales que debemos proteger. La información y los servicios esenciales marcan, en última instancia, las necesidades del sistema de información en materia de seguridad.

activos de soporte

Activos que no son esenciales. Estos activos no son una necesidad de la organización, sino un instrumento para implementar la funcionalidad que se necesita. Los activos de soporte son tan valiosos como los activos esenciales que soportan.

amenazas

Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización. [ISO/IEC 27000:2014]

aplicabilidad

Declaración formal en relación a una salvaguardia o un control acerca de su idoneidad para proteger el sistema de información. Una salvaguardia no se aplica cuando no tendría ningún efecto sobre los riesgos del sistema. Un control no se aplica cuando no tendría ningún efecto sobre el cumplimiento de una norma.

declaración de aplicabilidad (SoA)

Declaración oficial que establece qué salvaguardias (o controles) son apropiados para un sistema de información.

autenticidad

Aseguramiento de la identidad u origen.

confidencialidad

Garantía de que se cumplen las restricciones autorizadas en materia de acceso y divulgación, así como los medios para la protección de la privacidad y la propiedad de la información. [ISACA, Cybersecurity Fundamentals Glossary, 2014]

cumplimiento

Adhesión a los requisitos obligatorios definidos por leyes o reglamentos, así como los requisitos voluntarios que resultan de las obligaciones contractuales y las políticas internas. [ISACA, Cybersecurity Fundamentals Glossary, 2014]

disponibilidad

Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

dominios de seguridad

Los activos se ubican dentro de algún dominio de seguridad. Cada activo pertenece a un dominio y sólo a un dominio.

Un dominio de seguridad es una colección de activos uniformemente protegidos, típicamente bajo una única autoridad.

Los dominios de seguridad se utilizan para diferenciar entre unas partes y otras en el sistema de información. Por ejemplo:

- instalaciones centrales, sucursales, comerciales trabajando con portátiles
- servidor central (host), frontal unix, y PCs administrativos
- seguridad física, seguridad lógica
- ...

fases

El tratamiento del riesgo se puede afrontar por etapas o fases.

Estas fases son fotografías de la evolución del sistema de protección; mientras que se ponen en ejecución las nuevas salvaguardas, o se mejora su madurez.

impacto

El impacto es un indicador de qué puede suceder cuando ocurren las amenazas.

integridad

Garantía de que datos importantes no se han modificado ni se han eliminado sin autorización o sin que se pueda detectar.

medidas de protección – medidas de seguridad – salvaguardas

Mecanismos para tratar el riesgo, incluyendo políticas, guías, prácticas y estructuras organizativas que pueden ser administrativas, técnicas, de gestión e incluso de tipo legal. [ISACA, Cybersecurity Fundamentals Glossary, 2014]

perfiles de seguridad

Agrupación de salvaguardas en una serie de epígrafes que se convierten en requisitos a satisfacer. [PILAR]

propietario del riesgo – dueño del riesgo

Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo. [ISO Guide 73:2009]

riesgo

Efecto de la incertidumbre sobre la consecución de los objetivos. [ISO Guide 73:2009]

NOTA 1 Un efecto es una desviación, positiva y/o negativa, respecto a lo previsto.

NOTA 2 Los objetivos pueden tener diferentes aspectos (tales como financieros, de salud y seguridad, o ambientales) y se pueden aplicar a diferentes niveles (tales como, nivel estratégico, nivel de un proyecto, de un producto, de un proceso o de una organización completa).

NOTA 3 Con frecuencia, el riesgo se caracteriza por referencia a sucesos potenciales y a sus consecuencias, o a una combinación de ambos.

NOTA 4 Con frecuencia, el riesgo se expresa en términos de combinación de las consecuencias de un suceso (incluyendo los cambios en las circunstancias) y de su probabilidad.

NOTA 5 La incertidumbre es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un suceso, de sus consecuencias o de su probabilidad.

riesgo inherente – riesgo potencial

Nivel de riesgo sin tener en cuenta las acciones tomadas para tratarlo (ej. implementar controles). [ISACA, Cybersecurity Fundamentals Glossary, 2014]

riesgo residual

Riesgo remanente que existe después de que se hayan tomado las medidas de seguridad. [ISACA, Cybersecurity Fundamentals Glossary, 2014]

salvaguardas

Las salvaguardas son medios para luchar contra las amenazas. Pueden tratar aspectos organizativos, técnicos, físicos o relativos a la gestión de personal.

Una salvaguarda o contramedida es cualquier cosa que ayuda a impedir, contener o reaccionar frente a las amenazas sobre nuestros activos.

trazabilidad

Capacidad para asociar una actividad o suceso a un responsable. [ISACA, Cybersecurity Fundamentals Glossary, 2014]

valoración

Los activos son valorados para establecer sus requisitos de seguridad; es decir, el valor que debe protegerse frente a las consecuencias directas o indirectas de una amenaza ejecutada sobre dicho activo.

ANEXO C - REFERENCIAS

- Magerit: versión 3,
“Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”.
<http://administracionelectronica.gob.es/>
- UNE-ISO 31000:2010
Gestión del riesgo – Principios y directrices.
- UNE-ISO/IEC Guía 73:2010
Gestión del riesgo – Vocabulario.
- UNE-EN 31010:2011
Gestión del riesgo – Técnicas de apreciación del riesgo.
- UNE 71504:2008
Metodología de análisis y gestión de riesgos de los sistemas de información,
AENOR.
- ISO/IEC 27005:2011
Information technology -- Security techniques -- Information security risk
management.
- NIST SP 800-39:2011
Managing Information Security Risk: Organization, Mission, and Information
System View
<http://csrc.nist.gov/publications/PubsSPs.html>
- NIST SP 800-37 Rev. 1, 2010
Guide for Applying the Risk Management Framework to Federal Information
Systems: A Security Life Cycle Approach
<http://csrc.nist.gov/publications/PubsSPs.html>
- NIST SP 800-30:2002
Risk Management Guide for Information Technology Systems.
<http://csrc.nist.gov/publications/PubsSPs.html>
- ISACA:2010
The Risk IT Framework
<http://www.isaca.org/>
- ISACA:2009
The Risk IT Practitioner Guide
<http://www.isaca.org/>
- AS/NZS 4360:2004
Risk management