

# Guía de Seguridad de las TIC

## CCN-STIC 473

### μPILAR – Manual de Usuario (v7.1)



MAYO 2018

Edita:



© Centro Criptológico Nacional, 2018

NIPO: 785-18-029-6

Fecha de Edición: mayo de 2018

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 la comunicación (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).

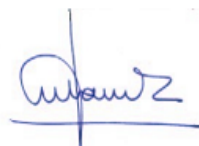
Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad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

Mayo de 2018



Félix Sanz Roldán  
Secretario de Estado  
Director del Centro Criptológico Nacional

## ÍNDICE

<b>1. CAPÍTULO I - INTRODUCCIÓN.....</b>	<b>1</b>
1.1. PRESENTACIÓN .....	1
1.2. INSTALACIÓN .....	1
1.2.1. ENTORNO JAVA.....	1
1.2.2. PILAR (WINDOWS) .....	1
1.2.3. PILAR (UNIX).....	2
1.2.4. PILAR (MAC OS X).....	2
1.3. USO .....	2
1.3.1. PRIMERA PANTALLA .....	3
1.3.2. PANTALLA DE DATOS DEL PROYECTO.....	3
<b>2. CAPÍTULO II - USO BÁSICO .....</b>	<b>4</b>
2.1. ACTIVIDADES PRELIMINARES: EL CONTEXTO .....	4
2.1.1. ACTIVOS ESENCIALES .....	4
2.2. ACTIVOS ESENCIALES: IDENTIFICACIÓN Y CARACTERIZACIÓN .....	4
2.2.1. CARACTERÍSTICAS .....	5
2.2.2. VALORACIÓN.....	6
2.3. ACTIVOS DE SOPORTE.....	6
2.4. AGRAVANTES Y ATENUANTES .....	7
2.5. MEDIDAS DE SEGURIDAD .....	8
2.5.1. RECOMENDACIÓN .....	8
2.5.2. APLICABILIDAD.....	9
2.5.3. VALORACIÓN POR FASES .....	10
2.5.4. SEMÁFORO.....	12
2.5.5. DUDAS Y COMENTARIOS .....	12
2.6. RIESGO .....	13
2.7. INFORMES.....	13
2.8. MEJORAS.....	14
<b>3. CAPÍTULO III – PERSONALIZACIÓN .....</b>	<b>15</b>
3.1. FICHERO DE CONFIGURACIÓN.....	15
3.2. PERÍMETROS .....	15
3.3. PATRONES PARA INFORMES.....	16
3.4. PERFILES DE ATAQUE.....	16
<b>ANEXO A – NIVELES DE MADUREZ .....</b>	<b>17</b>
<b>ANEXO B - GLOSARIO .....</b>	<b>18</b>

## 1. CAPÍTULO I - INTRODUCCIÓN

### 1.1. PRESENTACIÓN

1. 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. En este manual nos centraremos en los incidentes que pueden causar un perjuicio en la información y los servicios de la organización.
2. El análisis de riesgos proporciona información para decidir sobre la asignación de recursos, ya sean técnicos o de otro tipo, para proteger organización.
3. 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.
4. PILAR implementa la metodología Magerit: [<http://administracionelectronica.gob.es/>].
5. μPILAR es una versión de PILAR que se enfoca a sistemas pequeños con un planteamiento homogéneo de la seguridad. El análisis es rápido, aunque poco preciso. La información recogida en μPILAR puede ser analizada posteriormente en PILAR para un análisis más preciso.

### 1.2. INSTALACIÓN

#### 1.2.1. ENTORNO JAVA

6. Se necesita un
  - JRE – Entorno de ejecución Java
7. visite [<http://java.com>] y siga las instrucciones
  - paso 1: descargar
  - paso 2: instalar
  - paso 3: probar

#### 1.2.2. PILAR (WINDOWS)

8. 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.
9. Cuando Java esté instalado ...
  - ejecute `pilarmicro_<version>_<perfil>_<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

`pilarmicro.exe`

donde haya decidido instalar el software.

### 1.2.3. PILAR (UNIX)

10. Cuando Java esté instalado...

- ejecute `pilarmicro_linux_<version>_<perfil>_<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

`pilarmicro.jar`

donde haya decidido instalar el software.

### 1.2.4. PILAR (MAC OS X)

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

- ejecute `pilarmicro_mac_<version>_<perfil>_<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

`pilarmicro_<versión>.app`

## 1.3. USO

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

ej. `MICRO_27000_es.car`





13. 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.

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

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

### 1.3.1. PRIMERA PANTALLA



- [configuración] haga doble clic para cambiar el perfil (fichero CAR)
- [licencia] haga doble clic para cargar su licencia de uso (fichero LIC)
-  para empezar un proyecto nuevo
-  para volver a abrir un proyecto reciente
-  para abrir un proyecto ya existente (en un fichero MGR)
-  para abrir un proyecto ya existente (en base de datos)

### 1.3.2. PANTALLA DE DATOS DEL PROYECTO

15. Son datos administrativos. Aparecerán en los informes.

## 2. CAPÍTULO II - USO BÁSICO

16. μPILAR le llevará a lo largo de una secuencia de pantallas, usando los botones al pie:



para avanzar a la siguiente pantalla



para regresar a la pantalla anterior

### 2.1. ACTIVIDADES PRELIMINARES: EL CONTEXTO

17. Antes incluso de arrancar el programa, necesita saber el contexto del sistema de información. El contexto se define por medio de

- los activos esenciales que imponen requisitos de seguridad
- puntos de interconexión: socios con los que intercambiamos información y servicios
- proveedores, en los que externalizamos funciones y de cuyo desempeño dependemos

18. Los requisitos de seguridad los imponen los activos esenciales. Estos requisitos se trasladan a los sistemas interconectados y a los proveedores.

#### 2.1.1. ACTIVOS ESENCIALES

19. 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.

20. 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.

21. 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.

### 2.2. ACTIVOS ESENCIALES: IDENTIFICACIÓN Y CARACTERIZACIÓN

22. Esta pantalla permite introducir los activos esenciales:



Activos esenciales

Exportar

dimensión	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[example] Unidad administrativa	[4]	[4]	[7]	[7]	[7]		[1]
Activos esenciales							
I [INFO] Expedientes en curso		[4]	[7]	[4]	[4]		[1]
S [S_in_person] Tramitación presencial	[4]			[7]	[7]		
S [S_remote] Tramitación remota	[1]			[7]	[7]		
sistema de protección de frontera lógica							
[firewall] Cortafuegos	[4]	[4]	[7]	[7]	[7]		[1]
sistema de protección física del perímetro							
[offices] Oficinas	[4]	[4]	[7]	[7]	[7]		[1]
[dc] Sala de equipos	[4]	[4]	[7]	[7]	[7]		[1]
contratado a una tercera parte							
[archive] Archivo histórico central	[4]	[4]	[7]	[7]	[7]		[1]
[ADSL] Conexión a Internet	[4]	[4]	[7]	[7]	[7]		[1]

nuevo activo   editar   arriba   abajo   eliminar el activo

?

< >

Save, Print, Export icons

23. El formato es fijo:

- cada activo requiere un código único
- los activos de información y de servicio están en la zona de “activos esenciales”
- las interconexiones están en la zona de frontera lógica
- los servicios subcontratados están en la zona de terceras partes
- dentro de cada zona se pueden recolocar los activos [arriba] / [abajo]

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

Activos esenciales						
is [mission] Unidad de negocio	[1]	[4]	[7]	[4]	[4]	

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

### 2.2.1. CARACTERÍSTICAS

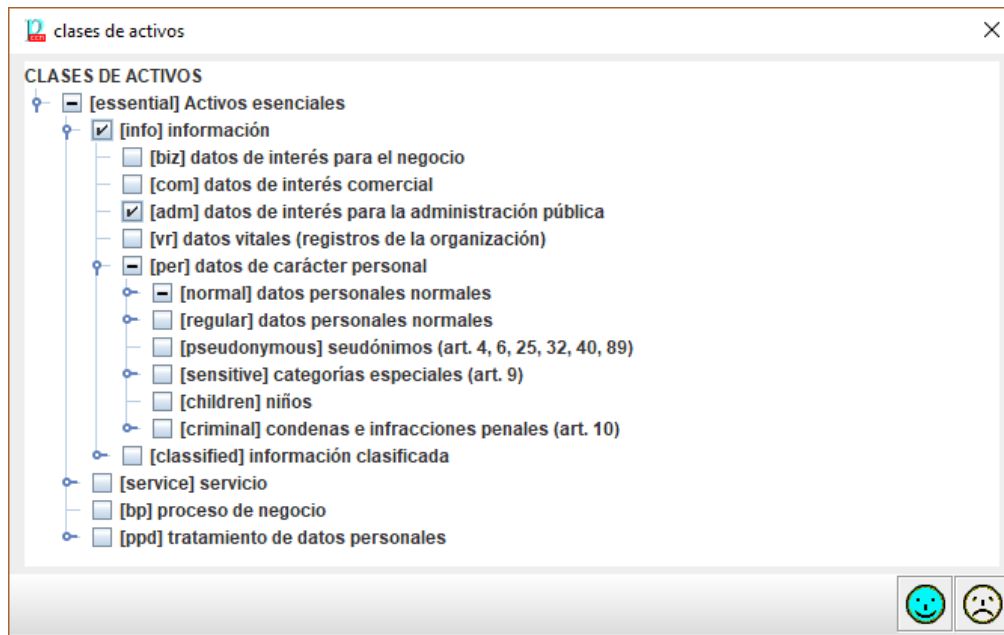
26. Tanto cuando crea un nuevo activo como cuando lo edita, puede clasificarlo

clase de activos

☒ Activos esenciales  
 ☐ sistema de protección de frontera lógica

{essential.{info.{adm, per.M}, service}}

27. Las opciones se limitan a lo que PILAR ofrece como árbol:



### 2.2.2. VALORACIÓN

28. 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)

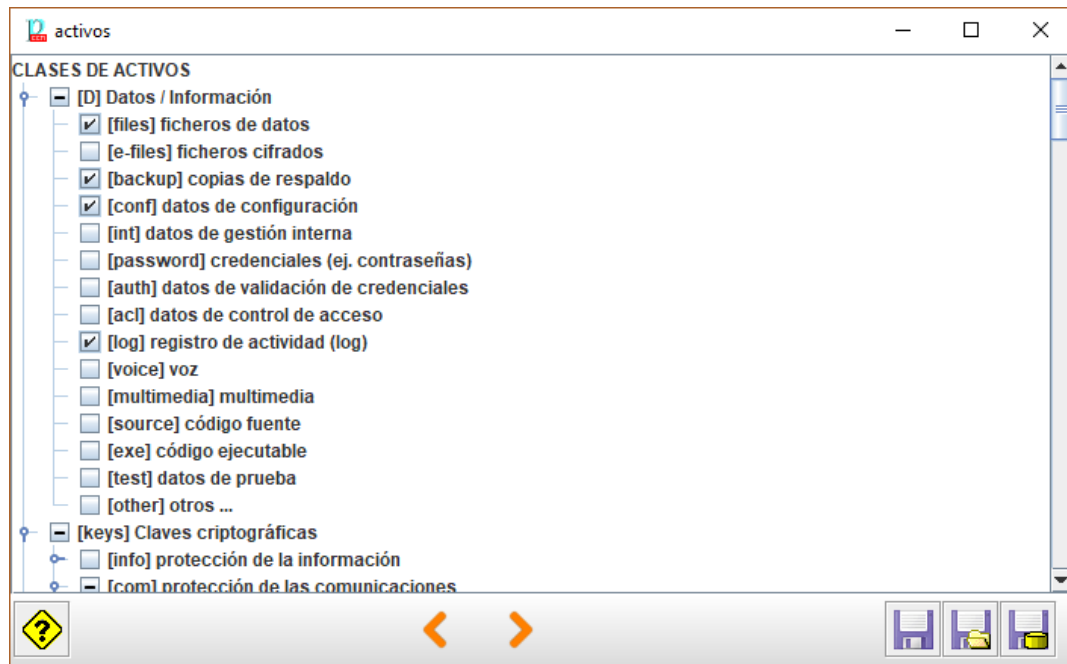
29. Para los activos de servicio:

- requisitos de disponibilidad

30. Los requisitos de seguridad del sistema son los máximos en cada dimensión de seguridad de los diferentes activos esenciales.

### 2.3. ACTIVOS DE SOPORTE

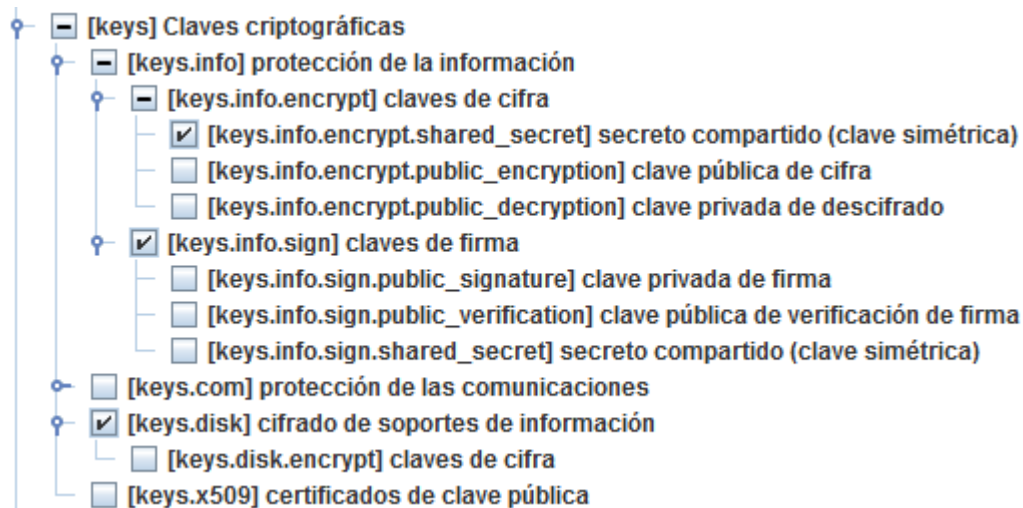
31. Esta pantalla recoge otros activos en el sistema. Marque los que necesite.



32. Las marcas indican

- ☒ Indica que en sistema hay al menos un activo con esta característica
- ☐ indica que alguna característica está marcada bajo esta
- ☐ indica que en el sistema no hay ningún activo con esta característica

**Ejemplo**



## 2.4. AGRAVANTES Y ATENUANTES

33. En esta pantalla puede calificar el sistema por medio de una serie de características que aumentan o reducen la exposición al riesgo:

factores agravantes | atenuantes

**CRITERIOS**

- ☐ [101] () Identificación del atacante
  - ☒ [101.a] () público en general
  - ☐ [101.b] (5%) competidor comercial
  - ☐ [101.c] (5%) proveedor de servicios
  - ☐ [101.d] (5%) grupos de presión política / activistas / extremistas
  - ☐ [101.e] (5%) periodistas
  - ☐ [101.f] (8%) criminales / terroristas
  - ☐ [101.g] (10%) personal interno
  - ☐ [101.h] (10%) bandas criminales
  - ☐ [101.i] (10%) grupos terroristas
  - ☐ [101.j] (20%) servicios de inteligencia
- ☐ [102] () Motivación del atacante
- ☐ [103] () Beneficio del atacante
  - ☒ [103.a] (5%) moderadamente interesado
  - ☐ [103.b] (10%) muy interesado
  - ☐ [103.c] (20%) extremadamente interesado
- ☐ [106] () Atracción del objetivo
- ☐ [104] () Motivación del personal interno
  - ☐ [104.a] (-10%) todo el personal está fuertemente motivado

34. Marque las características propias de su sistema.

## 2.5. MEDIDAS DE SEGURIDAD

35. Esta pantalla presenta el cumplimiento de un cierto perfil de seguridad, compuesto por controles (✓) que pueden ser refinados o alineados con salvaguardas (3).

[27002:2013] Código de prácticas para los controles de seguridad de la información

Expandir	Operación	~madurez	Exportar	control	du...	apl...	co...	current	target	PILAR
<input type="checkbox"/>				[27002:2013] Código de prácticas para los controles de seguridad de la información				L2	L3 (L4)	L3-
<input type="checkbox"/>	2			✓ [5] Políticas de seguridad de la información				L0	L5	L2
<input type="checkbox"/>	7			✓ [6] Organización de la seguridad de la información			...	L2- (L2)	L2 (L5)	L2 (L3-)
<input type="checkbox"/>				✓ [7] Seguridad relativa a los recursos humanos			n.a.			
<input type="checkbox"/>	7			✓ [8] Gestión de activos			...	L2	L3+ (L4)	L3 (L2+)
<input type="checkbox"/>	4			✓ [8.1] Responsabilidad sobre los activos			...	L2	L3- (L3)	L2
<input type="checkbox"/>	5			✓ [8.2] Clasificación de la información				L2-	L4+	L3 (L3-)
<input type="checkbox"/>	7			✓ [8.3] Manipulación de los soportes				L2	L4	L3+ (L3-)
<input type="checkbox"/>	7			✓ [8.3.1] Gestión de soportes extraíbles				L2	L4	L4 (L3-)
<input type="checkbox"/>	4			✓ [8.3.2] Eliminación de soportes				L2	L4	L3 (L3-)
<input type="checkbox"/>	4			✓ [MP.clean] Limpieza de contenidos				L2	L4	L3-
<input type="checkbox"/>	4			✓ [MP.end] Destrucción de soportes				L2	L4	L2+
<input type="checkbox"/>	5			✓ [8.3.3] Soportes físicos en tránsito				L2	L4	L3 (L3-)
<input type="checkbox"/>	7			✓ [9] Control de acceso				L2	L4	L3 (L3-)
<input type="checkbox"/>	8			✓ [10] Criptografía				L3-	L4	L4 (L3-)
<input type="checkbox"/>	6			✓ [11] Seguridad física y del entorno				L2-	L4- (L3+)	L3
<input type="checkbox"/>	8			✓ [12] Seguridad de las operaciones				L2	L4+	L3 (L3-)

### 2.5.1. RECOMENDACIÓN

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

37. 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.

38. 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

### 2.5.2. APLICABILIDAD

39. En la columna [aplica] indica 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). Cuando un control obligatorio se marca como 'n.a.', PILAR mantiene el color para recordar que es una situación singular.
40. Por ejemplo, si carece de servidores (porque usa servicios virtuales en la nube), entonces no hay que proteger ningún equipo físico. PILAR pone la recomendación en gris.
41. O puede ocurrir que el control sería útil, pero el sistema dispone de mejores medidas de protección.
42. 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.
43. 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.
44. 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.

### 2.5.3. VALORACIÓN POR FASES

[27002:2013] Código de prácticas para los controles de seguridad de la información

Expandir Operación ~madurez Exportar

rec...		control	du...	apl...	co...	current	target	PILAR
<input type="checkbox"/>	7	☑ [9] Control de acceso				L2	L4	L3 (L3-)
<input type="checkbox"/>	4	☑ [9.1] Requisitos de negocio para el control de acceso				L1 (L2-)	L5- (L4+)	L3- (L2+)
<input type="checkbox"/>	4	☑ [9.1.1] Política de control de acceso				L1 (L2)	L4 (L5-)	L3 (L3-)
<input type="checkbox"/>	2	☑ [AC.1.1] Se dispone de normativa para el control de accesos				L2	L4	L2
<input type="checkbox"/>	4	☑ [H.ST.3] Se definen roles con autorización exclusiva para realizar tareas		...		L2	L5	L3
<input type="checkbox"/>	2	☑ [9.1.2] Acceso a las redes y a los servicios de red				L1	L5 (L4)	L2
<input type="checkbox"/>	2	☑ [COM.op.1.1] Se dispone de normativa de uso de los servicios de red				L1	L4	L2
<input type="checkbox"/>	2	☑ [COM.op.1.1.1] Se identifican las redes y los servicios a los que se puede acceder				L1	L4	L2
<input type="checkbox"/>	2	☑ [COM.op.1.1.2] Se dispone de normativa relativa a las autorizaciones de acceso a las redes y servicios				L1	L4	L2
<input type="checkbox"/>	2	☑ [COM.op.1.1.3] Se dispone de normativa relativa a la protección de los accesos a las redes y servicios				L1	L4	L2
<input type="checkbox"/>	7	☑ [9.2] Gestión de acceso de usuario				L2+	L4	L3 (L3-)

?

< >

Save Print Export

45. 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”.
46. 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.
47. 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
48. Cuando una medida se marca como XOR, se puede elegir cuál de los componentes optativos se va a utilizar en este sistema. PILAR marca n.s. (no seleccionado) lo que no se usa, valorándose la madurez de la opción en uso.

clic derecho > seleccionar

[27002:2013] Código de prácticas para los controles de seguridad de la información

Expandir Operación ~madurez Exportar

	rec...	control	du...	apl...	co...	current	target	PILAR
<input type="checkbox"/>	8	[K.comms] Protección de claves de comunicaciones				L3	L4	L4-
<input type="checkbox"/>	3	[K.comms.1] Se dispone de normativa de gestión de claves				L3	L4	L3
<input type="checkbox"/>	3	[K.comms.2] Se dispone de procedimientos de gestión de claves				L3	L4	L3
<input type="checkbox"/>	3	[K.comms.3] Se identifican las personas responsables de cada clave				L3	L4	L3
<input type="checkbox"/>	5	[K.comms.4] Operación				L3	L4	L3
<input type="checkbox"/>	8	[K.comms.5] Las claves se generan en un entorno separado del de explotación				L3	L4	L5
<input type="checkbox"/>	6	[K.comms.6] {xor} Generación de claves				L3	L4	L4
<input type="checkbox"/>	5 (u)	[K.comms.6.1] Aplicación informática				[ L3 ]	[ L4 ]	L3
<input type="checkbox"/>	6	[K.comms.6.2] Dispositivo criptográfico				n.s.	n.s.	[ L4 ]
<input type="checkbox"/>	8	[K.comms.7] {xor} Distribución de claves				L3	L4	L5
<input type="checkbox"/>	8	[K.comms.7.1] Contenedor seguro				[ L3 ]	[ L4 ]	[ L5 ]
<input type="checkbox"/>	8	[K.comms.7.2] Canal seguro de comunicaciones				n.s.	n.s.	L5

### 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.

PILAR distingue entre la madurez de las salvaguardas (técnica) y la madurez de los controles (formal), presentado ambos valores simultáneamente si son diferentes.

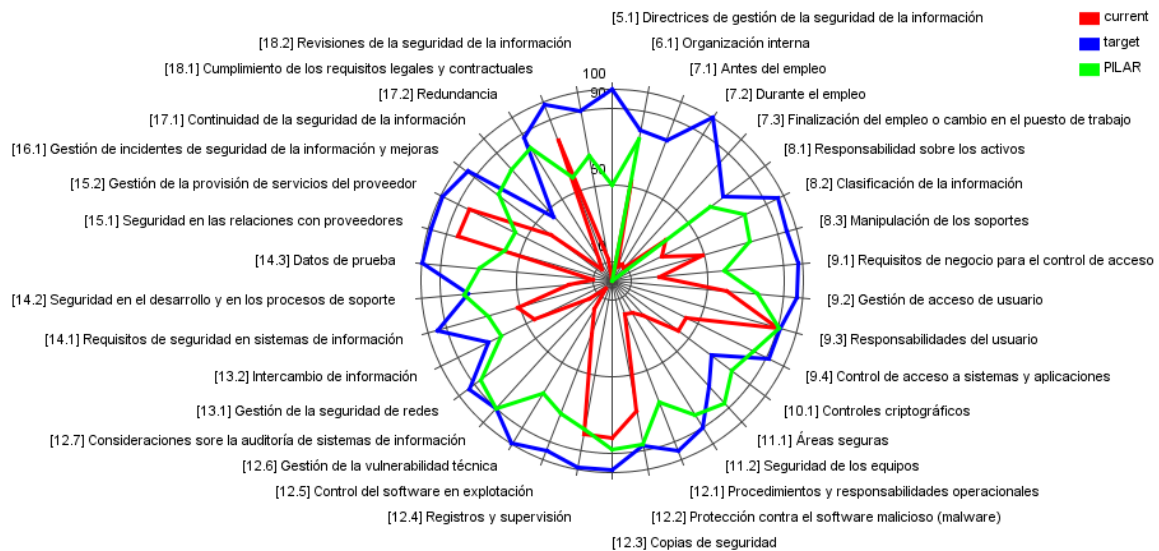
		[5.1] Directrices de gestión de la seguridad de la información				L0 (L1)	L5	L2
		[5.1.1] Políticas para la seguridad de la información				L0 (L1)	L5	L2
		[G.3.3] Normas de seguridad				L1	L5	L2
		[5.1.2] Revisión de las políticas para la seguridad de la información				L0 (L1)	L5	L2
		[G.3.3.6] Se revisan regularmente				L1	L5	L2

El valor entre paréntesis es el que se deriva de las salvaguardas inferiores. Usted puede “subir” el valor de las salvaguardas a los controles asociados (botón derecho).

### Presentación gráfica

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





### 2.5.4. SEMÁFORO

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

50. 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

51. 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

### 2.5.5. DUDAS Y COMENTARIOS

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

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



## 2.6. RIESGO

54. Esta pantalla presenta las estimaciones de riesgo. No es editable: es la salida del proceso de análisis. Hay varias pestañas para presentar el riesgo inherente al sistema, el riesgo en cada fase del proyecto, y el riesgo en la pseudo-fase PILAR.

riesgos

Exportar

potencial current target PILAR

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	{4,2}	{4,3}	{6,4}	{6,4}	{6,3}		{2,4}
[INFO] Expedientes en curso		{4,3}	{6,4}	{4,6}	{4,5}		{2,4}
[I] integridad de los datos		{4,3}					
[C] confidencialidad de los datos			{6,4}				
[archive] Archivo histórico central			{4,6}				
[ADSL] Conexión a Internet			{4,6}				
[D.files] ficheros de datos			{6,4}				
[E.19] Fugas de información			{3,4}				
[A.5] Suplantación de la identidad			{5,5}				
[A.6] Abuso de privilegios de acceso			{5,6}				
[A.11] Acceso no autorizado			{6,4}				
[D.backup] copias de respaldo			{6,4}				
[D.conf] datos de configuración		{4,3}		{6,0}			
[keys.com.channel] claves de cifrado del canal			{6,4}	{6,0}			
[keys.com.authentication] claves de autenticación			{6,4}	{6,0}			
[keys.com.verification] claves de verificación de			{6,4}	{6,0}			

niveles de criticidad

{9} - catástrofe
{8} - desastre
<b>{7} - extremadamente crítico</b>
{6} - muy crítico
{5} - crítico
{4} - muy alto
{3} - alto
{2} - medio
{1} - bajo
{0} - despreciable

55. El riesgo se presenta como un valor entre 0.0 y 10, y como un color que destaca su gravedad.

56. El árbol proporciona acceso a:

57. Nivel 1: activos esenciales: riesgo repercutido

58. Nivel 2: por dimensión de seguridad (repercutido)

59. Nivel 3: activos de soporte: riesgo acumulado

60. Nivel 4: amenazas: riesgo acumulado

## 2.7. INFORMES

61. PILAR proporciona una serie de informes predefinidos. Los informes se generan en formato RTF, un formato que puede editarse con los procesadores de texto habituales.

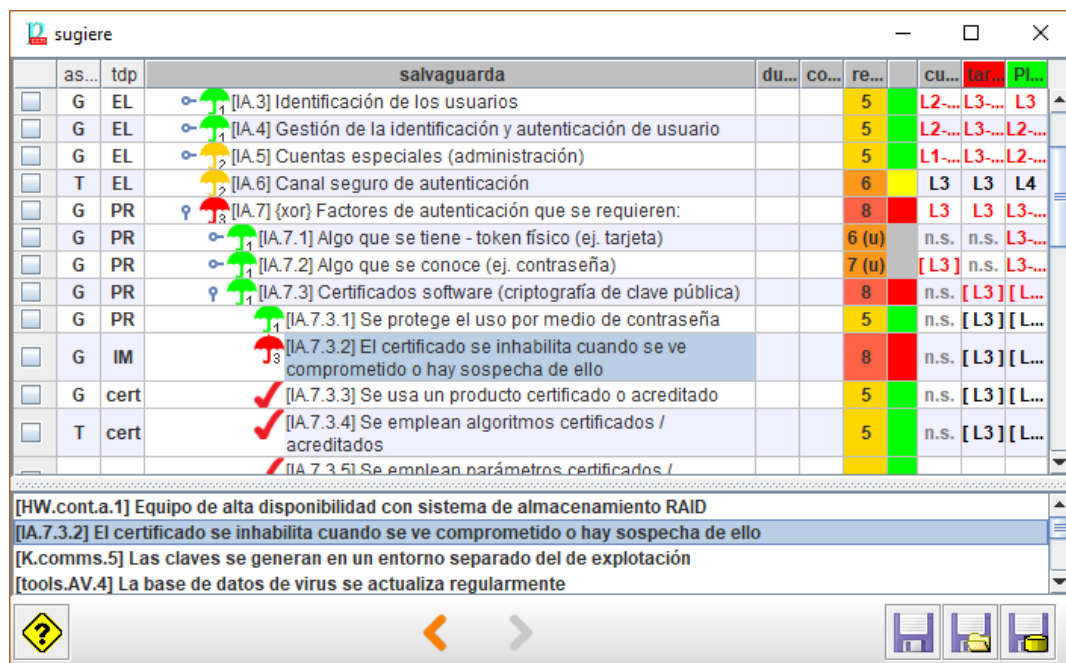


62. Haga clic en el informe que desea generar.

63. Los informes se generan en base a plantillas. Vea opciones de personalización.

## 2.8. MEJORAS

64. 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.



### 3. CAPÍTULO III – PERSONALIZACIÓN

65. Se puede personalizar PILAR editando varios ficheros en el directorio de librería.
66. A continuación, se muestran algunas posibilidades. Consulte la documentación para más detalle:

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

#### 3.1. FICHERO DE CONFIGURACIÓN

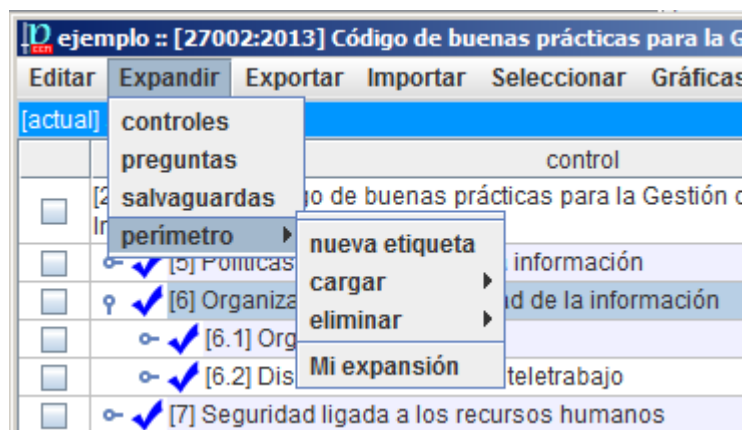
67. PILAR se distribuye con una serie de ficheros de configuración estándar. Los ficheros CAR. Por ejemplo

MICRO\_...\_es.car

68. Este fichero es de texto: puede visualizarlo y editarlo y tener su propia versión del mismo.
69. 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)
  - ...

#### 3.2. PERÍMETROS

70. 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.
71. Algunos perímetros son parte de la librería estándar. El usuario puede añadir los suyos propios.



72. 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

73. Par usar una etiqueta

`Expandir > perímetro > su etiqueta`

74. Para eliminar una etiqueta

`Expandir > perímetro > eliminar > su etiqueta`

### 3.3. PATRONES PARA INFORMES

75. 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/>

76. Puede establecer los patrones por defecto para sus análisis:

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

77. 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

### 3.4. PERFILES DE ATAQUE

78. Por defecto, μPILAR 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.

79. 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

## 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.

## **zonas**

Las zonas se utilizan para determinar la posición del ataque. Un ataque se origina en una zona y puede progresar a otras zonas a través de los elementos de frontera.

Un activo pertenece a una o más zonas, siendo objeto directo de los ataques desde la zona a la que pertenece y objeto indirecto de ataques originados en otra zona, a través de los activos de frontera.

PILAR dispone de zonas lógicas (separadas, por ejemplo, por cortafuegos), de zonas físicas (separadas por defensas físicas perimetrales) y zonas TEMPEST (separadas por barreras anti-emisiones).