

PILAR Basic – Manual de Usuario (2023.2)

Noviembre, 2023

Contenido

| | |
|---|----|
| Capítulo I - Introducción..... | 3 |
| I.1. Presentación..... | 3 |
| Capítulo II - Uso Básico..... | 4 |
| II.1.1. Identificación y caracterización..... | 5 |
| II.1.2. Valoración | 6 |
| II.1.3. Datos personales..... | 7 |
| II.2. Activos de soporte..... | 8 |
| II.3. Automatización | 10 |
| II.4. Perfiles de seguridad..... | 10 |
| II.4.1 Recomendación..... | 11 |
| II.4.2. Aplicabilidad..... | 11 |
| II.4.3. Valoración | 12 |
| II.4.4. Semáforo | 14 |
| II.4.5. Dudas y comentarios..... | 15 |
| II.5. Informes | 15 |
| Capítulo III - Uso Medio..... | 16 |
| III.1. Dominios de seguridad..... | 16 |
| III.2. Salvaguardas..... | 17 |
| Capítulo IV - Uso Avanzado | 20 |
| IV.1. Amenazas..... | 20 |
| Capítulo V – Personalización | 21 |
| V.1. Fichero de configuración..... | 21 |
| V.2. Perímetros..... | 21 |
| V.3. Patrones para informes..... | 22 |
| Capítulo VI - Temas avanzados..... | 23 |
| VI.1. Zonas..... | 23 |
| Anexo A – Niveles de madurez..... | 24 |
| Anexo B - Glosario | 25 |
| Anexo C - Referencias..... | 29 |

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. En este manual nos centraremos en los incidentes que pueden causar un perjuicio en la información y los servicios de la organización.

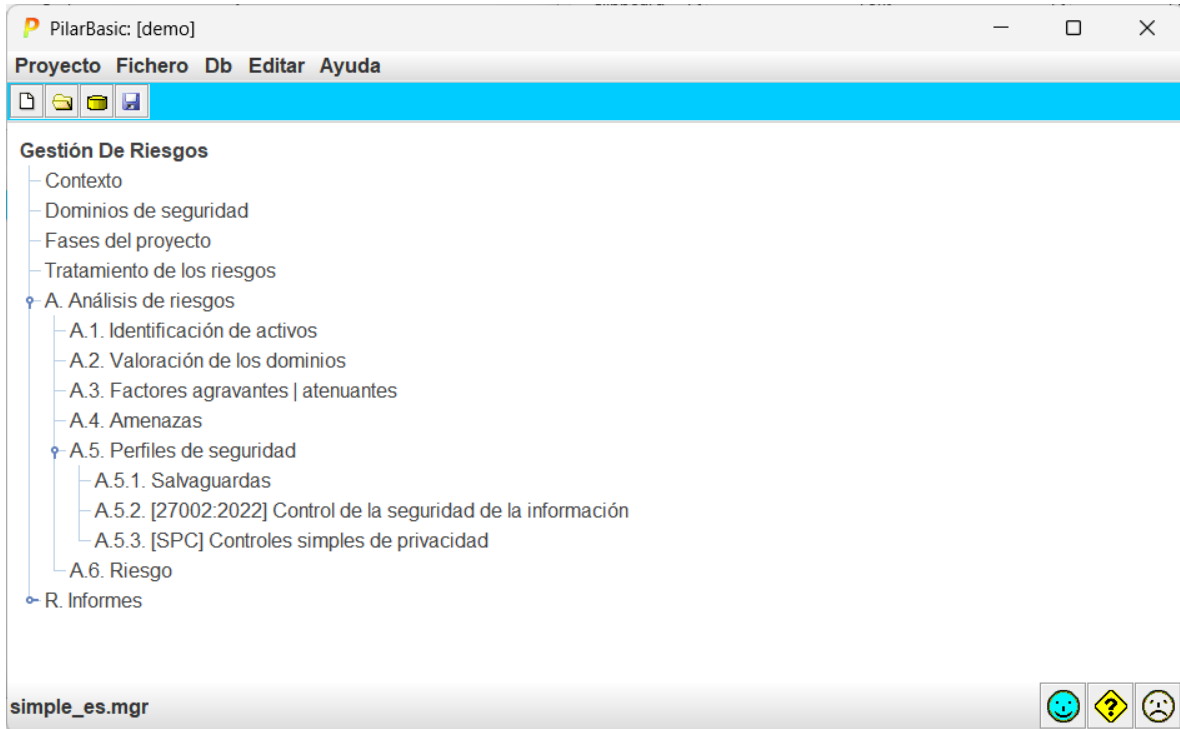
El análisis de riesgos proporciona información para decidir sobre la asignación de recursos, ya sean técnicos o de otro tipo, para proteger organización.

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/>].

Capítulo II - Uso Básico

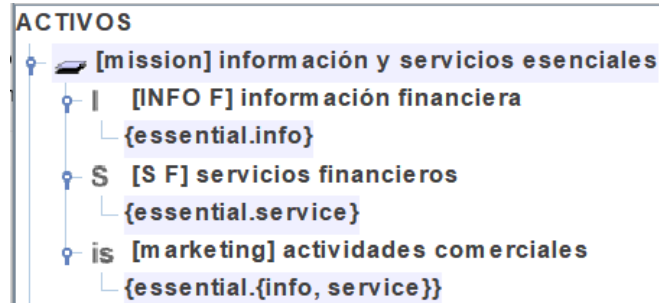


En PILAR usaremos activos esenciales de información para representar la información del negocio y activos esenciales de servicio para representar los servicios del negocio, o bien una combinación de ambos en un único activo

CLASES DE ACTIVOS

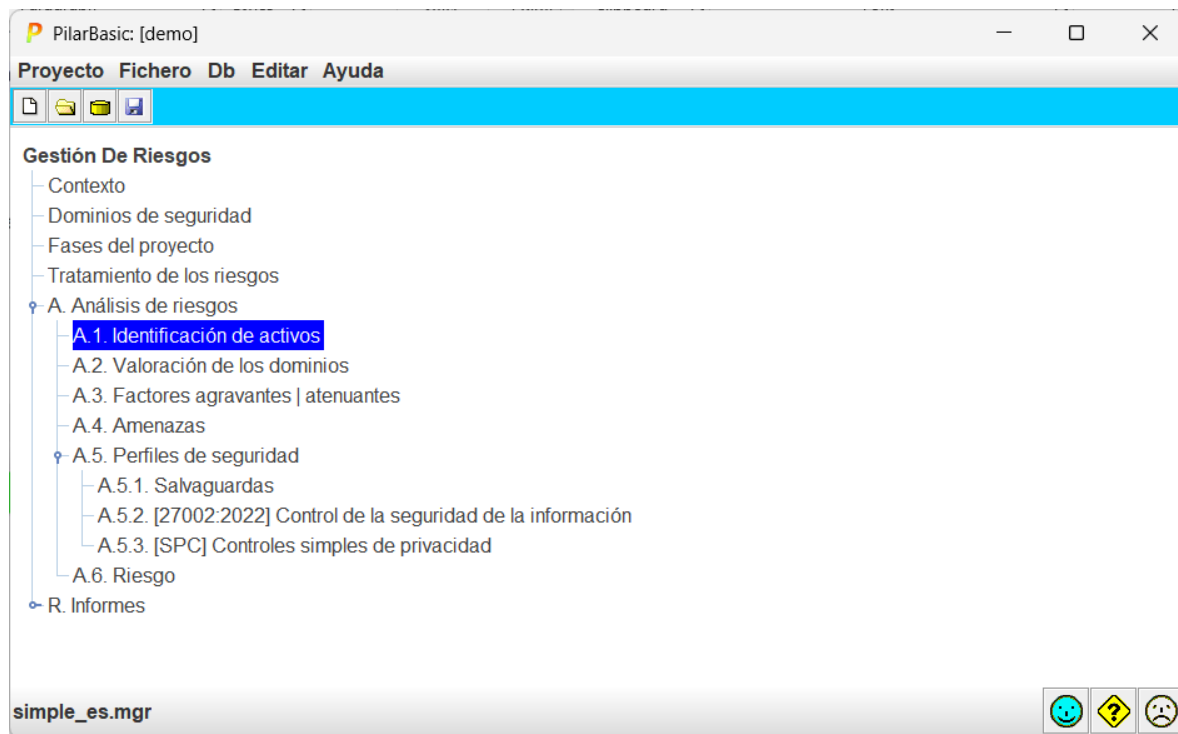


Los activos esenciales pueden ser de tipo 'información', o de tipo 'servicio', o una combinación de ambos. Lo importante es que tienen un nombre que los identifica y que es entendido por los niveles de gobierno y gestión de la empresa: los dueños del riesgo.

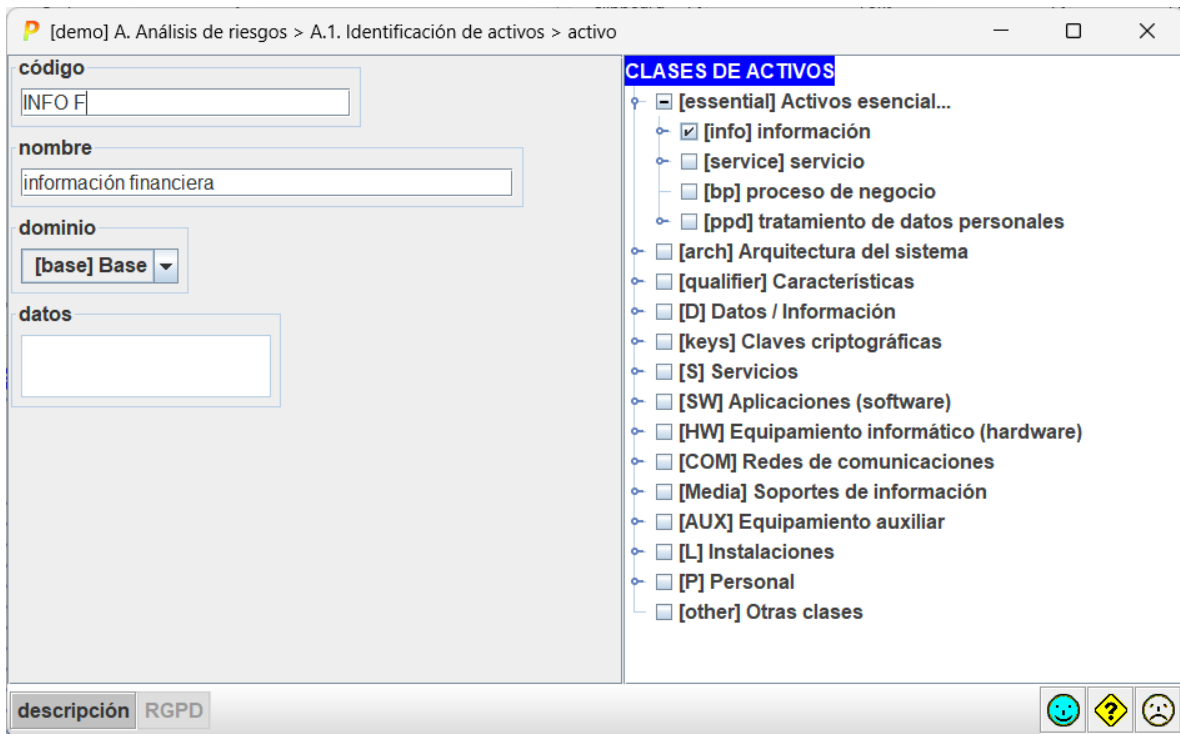


II.1.1. Identificación y caracterización

Análisis de riesgos > Activos > Identificación



- Capas > Nueva capa
 - [B] Activos esenciales
- Activos > Nuevo activo
 - [INFO] Información del negocio
 - Seleccione las clases que considere oportunas



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

II.1.2. 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

[demo] A. Análisis de riesgos > A.2. Valoración de los dominios

Editar Exportar Importar

| activo / dominio de seguridad | [D] | [I] | [C] | [A] | [T] | [DP] |
|--|-----|-----|-----|-----|-----|------|
| [demo] | | | | | | |
| [-] [essential] Activos esenciales | [6] | [7] | [7] | [7] | [7] | |
| [-] I [INFO F] información financiera | | [7] | [7] | [7] | [7] | |
| [-] S [S F] servicios financieros | [6] | | | | | |
| [-] is [marketing] actividades comerciales | [4] | [4] | [4] | [4] | [4] | |
| [-] Dominios de seguridad | | | | | | |
| [-] [base] Base | [6] | [7] | [7] | [7] | [7] | |

asociar disociar

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.1.3. Datos personales

Cuando manejamos datos personales, hay que indicar su naturaleza y, su tratamiento

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

INFO

nombre
Expedientes en curso

Fuentes de información
info_owner

dominio
[base] red corporativa

datos

Descripción
estado de los procesos de tramitación abiertos

contenido
almacena temporalmente datos financieros de los propietarios

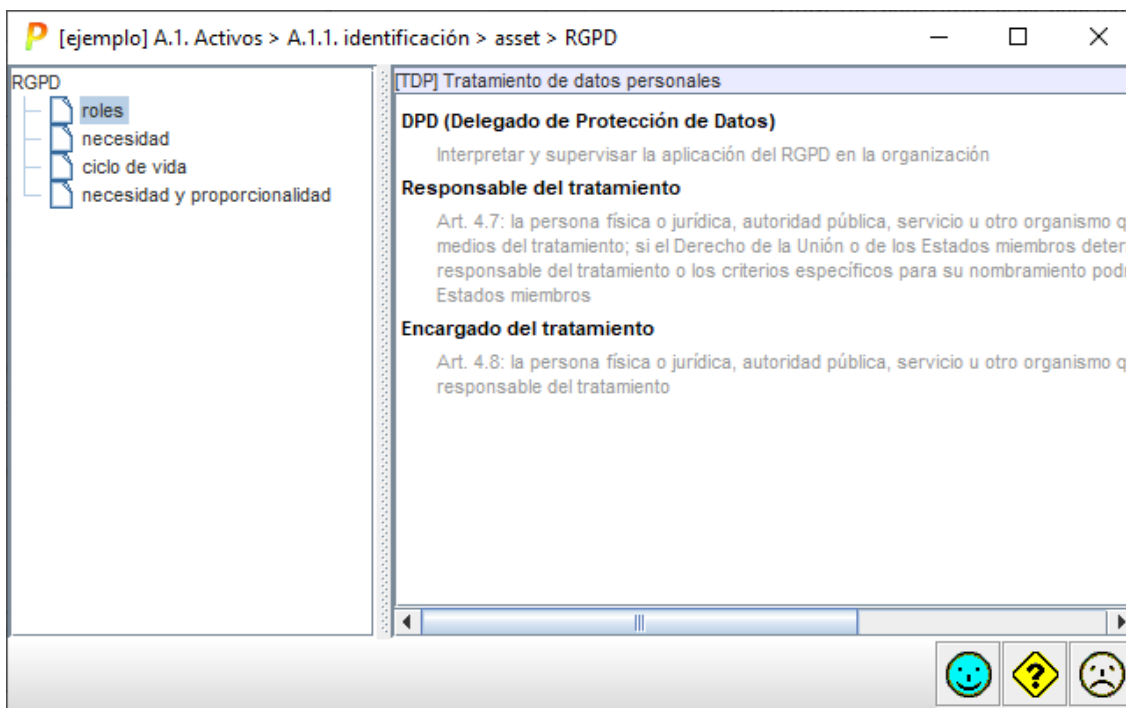
propietario
jefe de servicio de tramitación

CLASES DE ACTIVOS

- [essential] Activos esenciales
 - [info] información
 - [adm] datos de interés para la administración
 - [per] datos de carácter personal
 - [regular] datos personales normales
 - [1] económicos
 - [5] localización
 - [ppd] tratamiento de datos personales

descripción RCPD

A través del botón RGDP al pie podemos caracterizar el activo desde su punto de vista legal

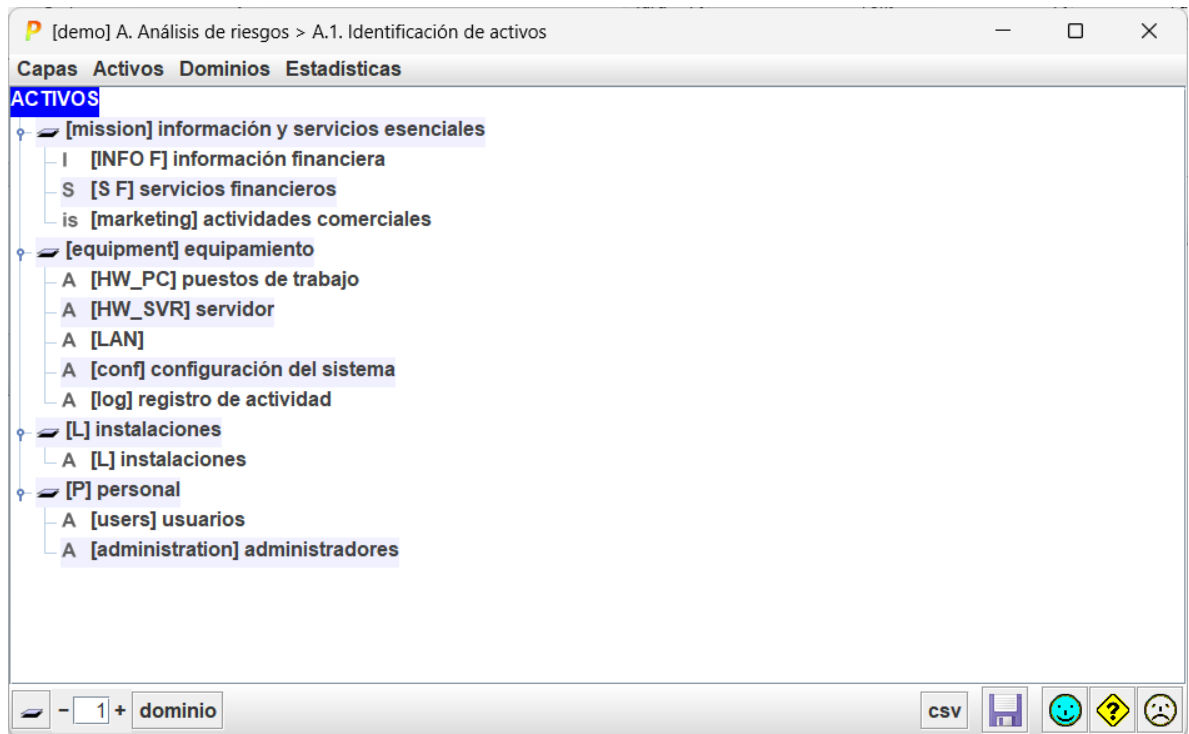


Los datos así recopilados se llevan a la documentación del sistema (informes).

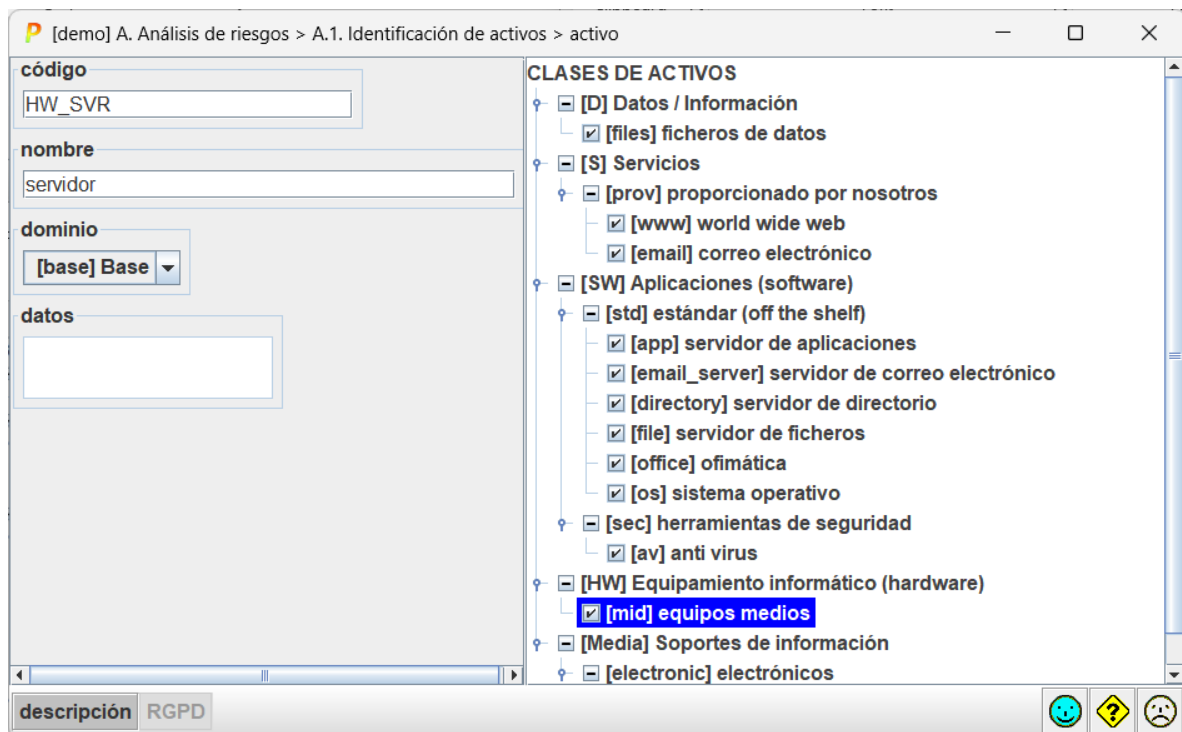
II.2. Activos de soporte

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).



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.3. 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 estudiar más adelante.

II.4. 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

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

[demo] evl > valoración

Editar Expandir Ver Exportar Importar Estadísticas Seleccionar Gráficas

[base] Base

| | rec... | nivel | control | du... | ba... | co... | current | target | PILAR |
|--------------------------|--------|-------|--|-------|-------|-------|-----------|----------|-------------|
| <input type="checkbox"/> | | | [27002:2022] Control de la seguridad de la información | | | | L2 [-L... | L4 [-L4] | L2-L3 (...) |
| <input type="checkbox"/> | 3 | | ✓ [5] Organización /PR CR DC | ... | ... | | L2 | L4 | L2-L3 |
| <input type="checkbox"/> | 3 | | ✓ [5.1] Políticas para la seguridad de la información /PR | | | | L2 | L4 | L3 (L2) |
| <input type="checkbox"/> | 3 | | ✓ [5.2] Roles y responsabilidades en seguridad de la información /PR | | | | L2 | L4 | L3 (L2) |
| <input type="checkbox"/> | 2 | | ✓ [5.3] Segregación de tareas /PR | | | | L2 | L4 | L2 (L2-... |
| <input type="checkbox"/> | 3 | | ✓ [5.4] Responsabilidades de la dirección /PR | ?...? | | | L2 | L4 | L3 (L2) |
| <input type="checkbox"/> | | | ✓ [5.5] Contacto con las autoridades /PR CR | | | | L2 | L4 | n.a. (L2) |
| <input type="checkbox"/> | 3 | | ✓ [5.6] Contacto con grupos de interés especial /PR CR | | | | L2 | L4 | L3 (L2-... |
| <input type="checkbox"/> | 3 | | ✓ [5.7] Inteligencia de amenazas /PR CR DC | | | | L2 | L4 | L3 |
| <input type="checkbox"/> | | | ✓ [5.8] Seguridad de la información en la gestión de proyectos /F | | | n.a. | | | |
| <input type="checkbox"/> | 3 | | ✓ [5.9] Inventario de información y otros activos asociados /PR | | | | L2 | L4 | L3 (L2-... |
| <input type="checkbox"/> | 3 | | ✓ [5.10] Uso aceptable de la información y activos asociados /PF | | | | L2 | L4 | L3 (L2) |
| <input type="checkbox"/> | 2 | | ✓ [5.11] Devolución de activos /PR | | | | L2 | L4 | L2 (L3) |
| <input type="checkbox"/> | 1 | | ✓ [5.12] Clasificación de la información /PR | | | | L2 | L4 | L2 |
| <input type="checkbox"/> | 1 | | ✓ [5.13] Etiquetado de la información /PR | | | | L2 | L4 | L2 (L2-... |
| <input type="checkbox"/> | 1 | | ✓ [5.14] Transferencia de la información /PR | | | | L2 | L4 | L2 (L2-... |
| <input type="checkbox"/> | 3 | | ✓ [5.15] Control de acceso /PR | | | | L2 | L4 | L3 (L2) |
| <input type="checkbox"/> | 2 | | ✓ [5.16] Gestión de identidad /PR | | | | L2 | L4 | L2 (L2-... |

- 1 + +1 dominios sugiere

II.4.1 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.4.2. 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. 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.4.3. Valoración

| rec... | nivel | control | du... | ba... | co... | current | target | PILAR |
|--------|-------|---|-------|-------|-------|---------|--------|-------------|
| | | [27002:2022] Control de la seguridad de la información | | | | L2 | L4 | L2-L3 (...) |
| 3 | | o ✓ [5] Organización /PR CR DC | | | | L2 | L4 | L2-L3 |
| 3 | | o ✓ [6] Controles de personas /PR CR DC | | | | L2 | L4 | L2-L3 |
| 3 | | o ✓ [7] Controles físicos /PR DC | | | | L2 | L4 | L2-L3 |
| 1 | | o ✓ [7.1] Perímetro de seguridad física /PR | | | | L2 | L4 | L2 (n.a.) |
| 2 | | o ✓ [7.2] Controles físicos de entrada /PR | | | | L2 | L4 | L2 (n.a.) |
| 2 | | o ✓ [7.3] Seguridad de oficinas, despachos y recursos /PR | | | | L2 | L4 | L2 (L3) |
| 2 | | o ✓ [7.4] Monitorización de la seguridad física /PR DC | | | | L2 | L4 | L2 (n.a.) |
| 1 | | o ✓ [7.5] Protección contra las amenazas externas y ambientales /PR | | | | L2 | L4 | L2 (L2-...) |
| 2 | | o ✓ [7.6] El trabajo en áreas seguras /PR | | | | L2 | L4 | L2 |
| 3 | | o ✓ [7.7] Puesto de trabajo despejado y pantalla limpia /PR | | | | L2 | L4 | L3 (L2-...) |
| 4 | | o [AC.2.14.2] Bloqueo de la pantalla al dejar desatendido el e | | | | L2 | L4 | L3 |
| | | o [HW.PCD.5.3] Los dispositivos portátiles se guardan en lug | | | | L2 | L4 | n.a. |
| 5 | | o [M.2.1.2] Los soportes se guardan en lugar seguro cuando r | | | | L2 | L4 | L3 |
| 5 | | o [PPE] Protección física de los equipos | | | | L2 | L4 | L2-L3 |
| | | o [L.AC.10] Se exige que los puestos de trabajo están despej | | | | L2 | L4 | n.a. |
| 3 | | o ✓ [7.8] Emplazamiento y protección de equipos /PR | | | | L2 | L4 | L3 |
| 2 | | o ✓ [7.9] Seguridad de los equipos fuera de las instalaciones /PR | | | | L2 | L4 | L2 (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. PILAR marca n.s. (no seleccionado) lo que no se usa, valorándose la madurez de la opción en uso.

clic derecho > seleccionar

| rec... | nivel | control | du... | apl... | co... | current | target | PILAR |
|--------|-------|--|-------|--------|-------|---------|--------|--------|
| 8 | | [K.comms] Protección de claves de comunicaciones [SC-12(2)] | | | | L3 | L4 | L2-L5 |
| 2 | | [K.comms.1] Se dispone de normativa de gestión de claves | | | | L3 | L4 | L2 |
| 2 | | [K.comms.2] Se dispone de procedimientos de gestión de claves | | | | L3 | L4 | L2 |
| 2 | | [K.comms.3] Se identifican las personas responsables de cada clave | | | | L3 | L4 | L2 |
| 4 | | [K.comms.4] Operación | | | | L3 | L4 | L3 |
| 5 | | [K.comms.5] {xor} Generación de claves | | | | L3 | L4 | L3 |
| 2 (u) | | [K.comms.5.1] Aplicación informática | | | | [L3] | [L4] | L2 |
| 5 | | [K.comms.5.2] Dispositivo criptográfico | | | | n.s. | n.s. | [L3] |
| | | [K.comms.6] {xor} Distribución de | | | | | | |

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.

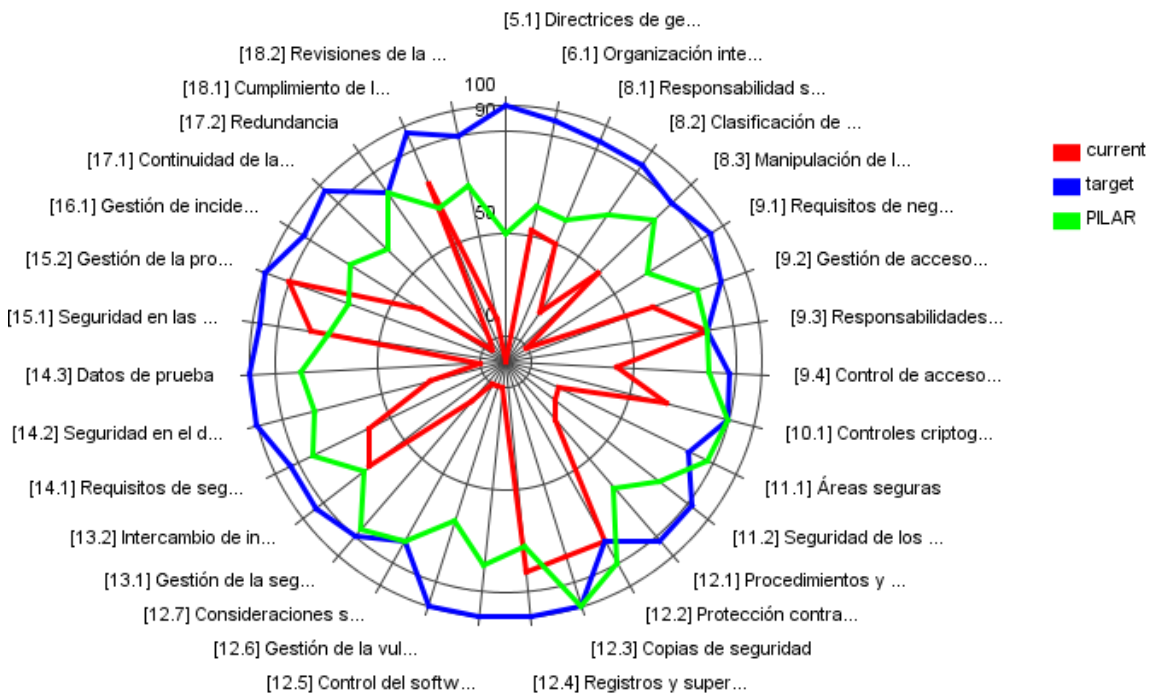
PILAR distingue entre la madurez de las salvaguardas (técnica) y la madurez de los controles (formal), presentado ambos valores simultáneamente si son diferentes.

| | | | | | | | | |
|---|---|---|--|--|--|---------|----|----|
| ? | ✓ | [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:



II.4.4. 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.4.5. 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.5. 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.

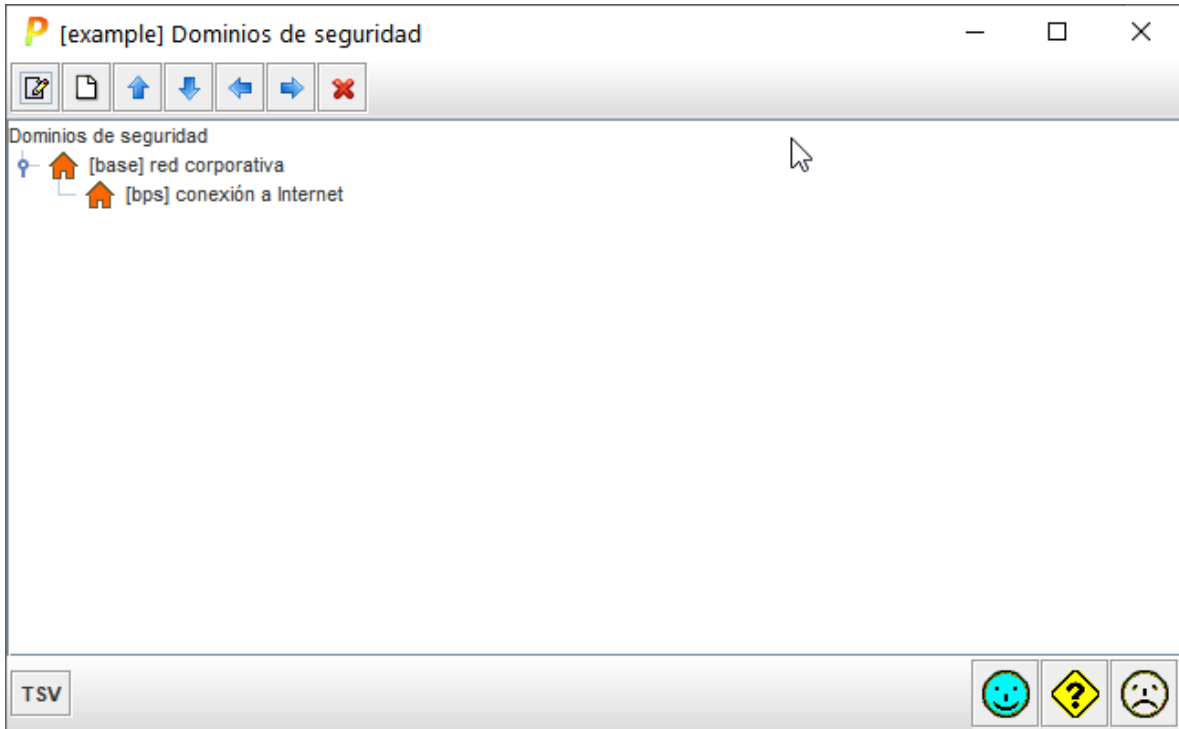
Capítulo III - Uso Medio

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.

[example] A. Análisis de riesgos > A.2. Valoración de los dominios

Editar Exportar Importar

| activo / dominio de seguridad | [D] | [I] | [C] | [A] | [T] | [V] | [DP] |
|--|-----|-----|-----|-----|-----|-----|------|
| [example] Unidad administrativa | | | | | | | |
| 📁 [essential] Activos esenciales | [4] | [4] | [7] | [7] | [7] | | [1] |
| 📁 it [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] | | |
| 📁 Dominios de seguridad | | | | | | | |
| 📁 🏠 [base] red corporativa | [4] | [4] | [7] | [7] | [7] | | [1] |
| 📁 🏠 [bps] conexión a Internet | [1] | | | [7] | [7] | | |

asociar disociar

III.2. 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

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 |
| | — proc – procedimiento |

— RC – recuperación

— 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 | |

Algunas salvaguardas tienen diferentes formas de implementarse, formas que son alternativas y se etiquetan como XOR. En cada dominio de seguridad solo se aplica una de esas opciones, quedando las demás marcadas como n.s. (no seleccionadas). Se selecciona la que debe usando el botón derecho del ratón



La opción seleccionada aparece [entre corchetes]. La selección no se hereda entre dominios: son independientes.

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.

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] A. Análisis de riesgos > A.5. Medidas técnicas y organizativas: Seguri... - □ ×

Editar Expandir Ver Exportar Importar Estadísticas

[base] red corporativa

| | as... | tdp | re... | nivel | salvaguarda | du... | ap... | co... | cu... | tar... | Pl... |
|--------------------------|-------|------|-------|-------|--|-------|-------|-------|-------|--------|-------|
| <input type="checkbox"/> | G | proc | 2 | | [COM.3] Se dispone de procedimientos de uso de las comunicaciones [SC-1] | | | | L0 | L3 | L2 |
| <input type="checkbox"/> | G | EL | 4 | | [COM.start] Entrada en servicio | | | | -L1 | -L5 | L2... |
| <input type="checkbox"/> | T | EL | 9 | | [COM.SC] Se aplican perfiles de seguridad [CM-6] | | | | L0... | L4... | L3... |
| <input type="checkbox"/> | T | PR | 4 | | [COM.SC.1] Se reducen las opciones a las mínimas necesarias | | | | L0 | L5 | L3 |
| <input type="checkbox"/> | T | EL | 5 | | [COM.SC.2] Se eliminan, o modifican, las cuentas estándar de usuario | | | | L0 | L5 | L3 |
| <input type="checkbox"/> | T | EL | 9 | | [COM.SC.3] Se eliminan, o modifican, las cuentas estándar de administrador [IA-5(5)] | | | | L0 | L5 | L5 |

28,4 :: [COM.SC.3] Se eliminan, o modifican, las cuentas estándar de administrador [IA-5(5)]

26,9 :: [IAb] IDENTIFICATION AND AUTHENTICATION [IA, IAb]

20,2 :: [tools.CM] CM: Monitorización continua

20,2 :: [ACb] ACCESS CONTROL [AC, ACb]

20,2 :: [COM.SC.5] Los servicios activados se configuran de forma segura

18,1 :: [IA.8.3] (xor) AAI 3: proporciona una muy alta garantía

- 1 + operación sugiere buscar >>

Capítulo IV - Uso Avanzado

IV.1. 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

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 <https://www.pilar-tools.com/doc/>

V.1. Fichero de configuración

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

BASIC_es.car

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

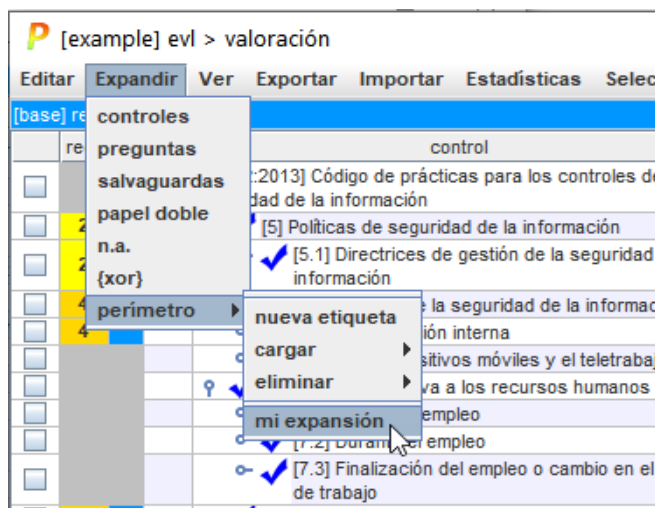
Algunos ajustes que se pueden hacer:

- añadir un icono de su organización
- añadir una pantalla de inicio (splash)
- 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/>

Puede establecer los patrones por defecto para sus análisis:

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

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

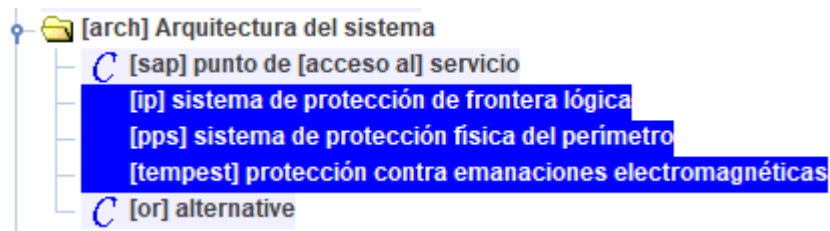


El atacante necesita entrar, superando el perímetro de protección física (la protección que aportan paredes, puertas, ventanas, etc.) y luego podría atacar el servidor.

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)

Respecto de la frontera, los activos de frontera son de alguno de estos tipos



Nótese que la frontera puede ser un activo singular (como un cortafuegos) o un conjunto de elementos singulares (varios cortafuegos, un proxy, servidores en la DMZ, etc.). En este último caso se recomienda definir un activo que defina la funcionalidad de la frontera como una función integrada. En el caso de una frontera lógica, este activo basta que sea de tipo [arch.ip].

PILAR establece automáticamente una zona interna y una zona externa a ambos lados de las fronteras y aplica automáticamente los perfiles de ataque especificados en el fichero de configuración (CAR).

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.

información

Una instancia de un tipo de información.

Una categoría específica de información (por ejemplo, administración de seguridad privada, médica, de propiedad, financiera, de investigación, sensible al contratista) definida por una organización o, en algunos casos, por una ley específica, Orden ejecutiva, directiva, política o regulación.

[<https://csrc.nist.gov/glossary/term/information-type>]

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 directo – acumulado

El riesgo calculado sobre los activos de soporte; es decir, donde impacta la amenaza.

riesgo indirecto – repercutido

El riesgo trasladado a los activos de negocio; es decir, donde impacta en el negocio.

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]

salvuardas

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

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

servicio

Una capacidad o función proporcionada por una entidad.
[<https://csrc.nist.gov/glossary/term/service>]

sistema de información

Un conjunto discreto de recursos de información organizados para la recopilación, procesamiento, mantenimiento, uso, intercambio, difusión y disposición de la información.

[<https://csrc.nist.gov/glossary/term/System>]

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).

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