µPILAR
Manual de Usuario (versión 2023.1)

Mayo, 2023

Contenido

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 la organización.

El análisis de riesgos requiere un enfoque metódico:

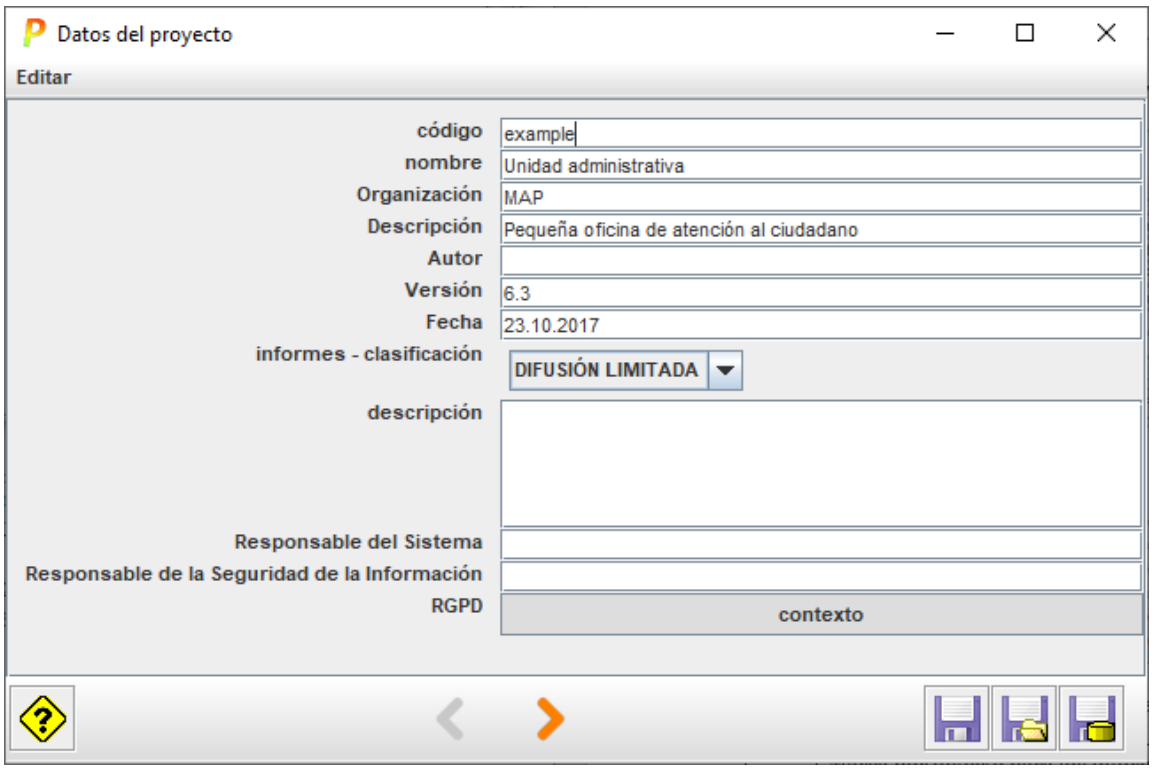
1. identificar el valor que hay que proteger,
2. Identificar los elementos del sistema que soportan ese valor; es decir, aquellos donde los ataques pueden causar daño,
3. establecer medidas de seguridad para protegernos contra los incidentes deliberados o accidentales y
4. estimar indicadores de la posición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

PILAR implementa la metodología Magerit: http://administracionelectronica.gob.es/.

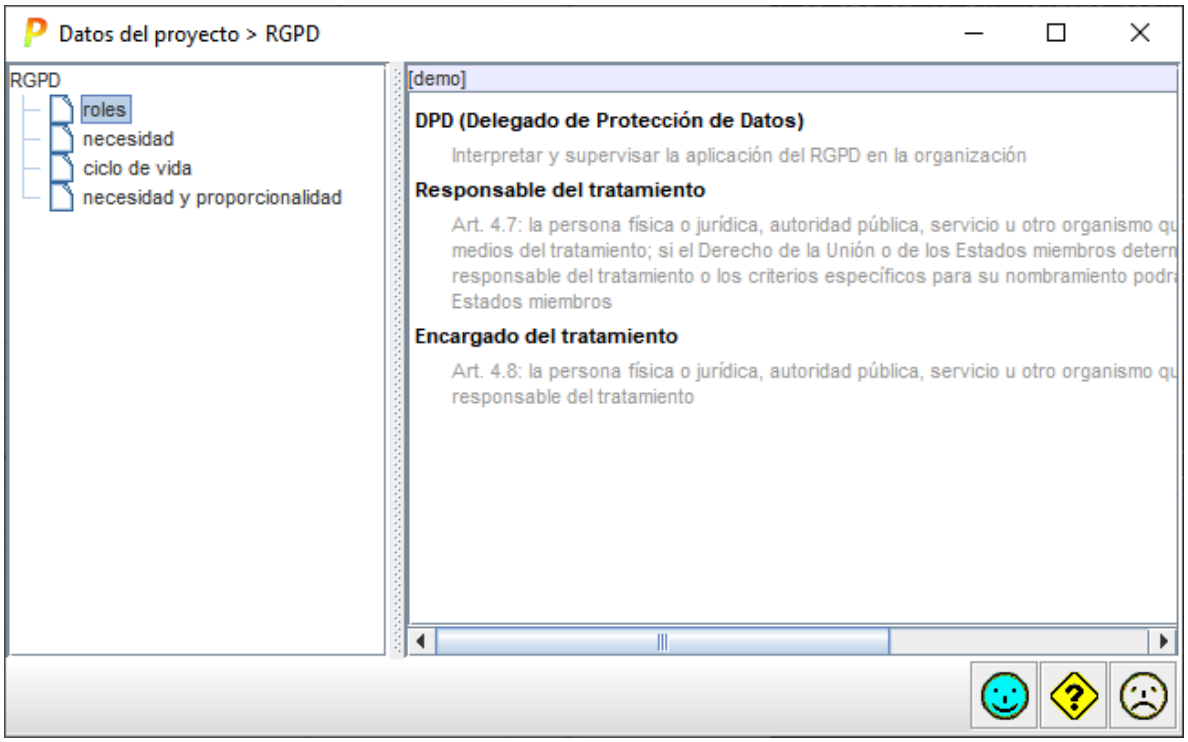
µPILAR es una versión de PILAR que se enfoca a sistemas pequeños con un planteamiento homogéneo de la seguridad. El análisis es rápido, aunque poco preciso. La información recogida en µPILAR puede ser analizada posteriormente en PILAR para un análisis más preciso.

I.2. Pantalla de datos del proyecto

Son datos administrativos. Aparecerán en los informes.



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



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

Capítulo II - Uso Básico

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

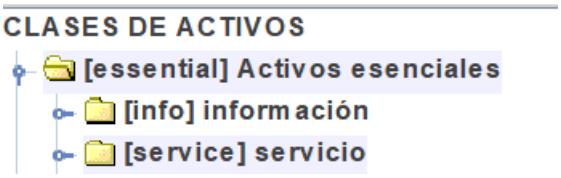
para avanzar a la siguiente pantalla

para regresar a la pantalla anterior

II.1. Activos esenciales

La primera actividad para realizar un análisis de riesgos es determinar lo que tenemos que proteger: información del negocio y servicios prestados por el sistema de información. Esta información y estos servicios se denominan esenciales y, en PILAR, se modelan como activos esenciales.

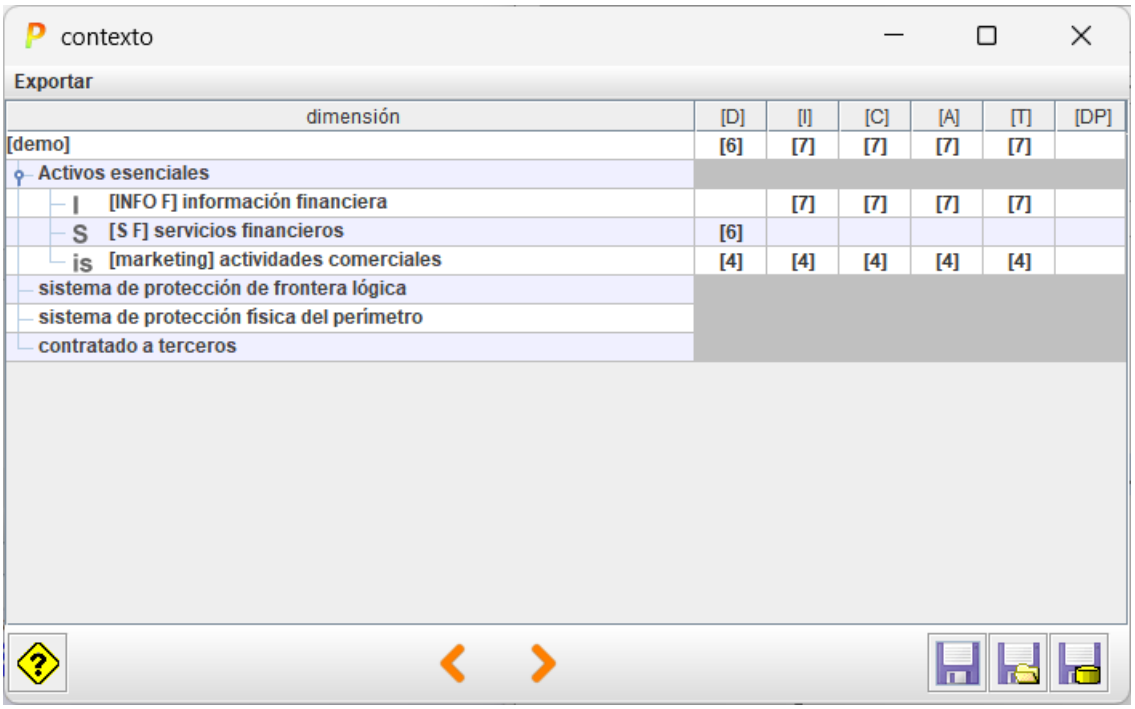
En PILAR usaremos activos esenciales de información para representar la información del negocio y activos esenciales de servicio para representar los servicios del negocio, o bien una combinación de ambos en un único activo



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.2. Activos esenciales: identificación y caracterización

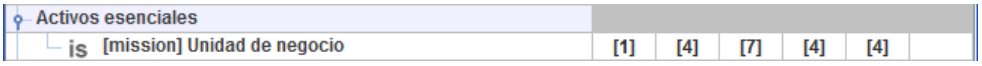
Esta pantalla permite introducir los activos esenciales:



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 se terceras partes
- dentro de cada zona se pueden recolocar los activos [arriba] / [abajo]

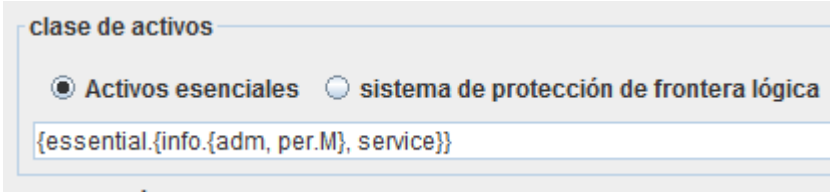
Puede ser útil combinar información y servicios en un único activo:



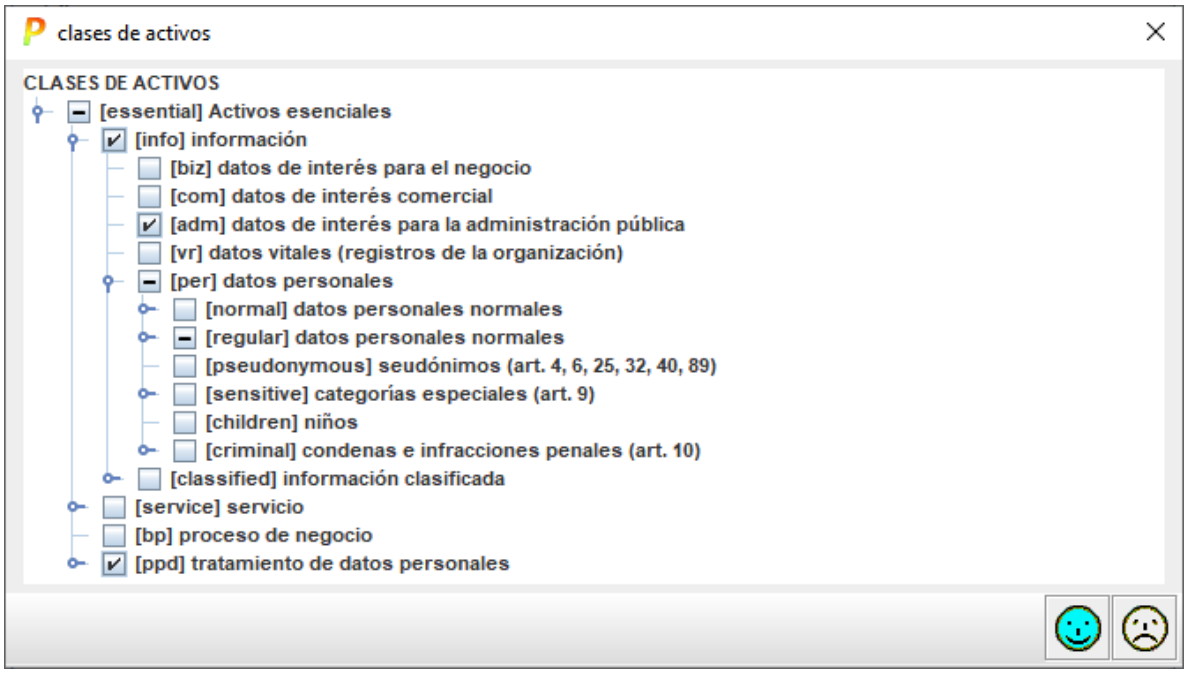
Ha terminado cuando tenga suficientes elementos de información y de servicio para hablar con sus directores de los requisitos de seguridad del sistema.

II.2.1. Características

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



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



II.2.2. Valoración

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)

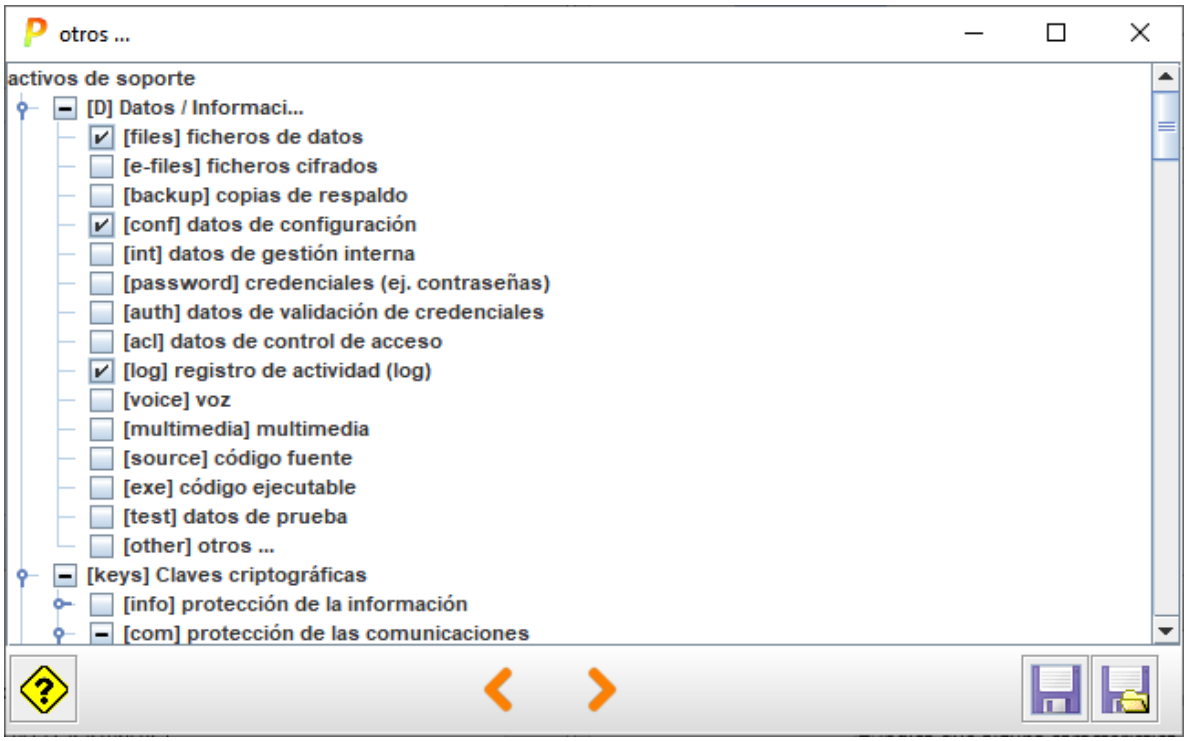
Para los activos de servicio:

- requisitos de disponibilidad

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

II.3. Activos de soporte

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



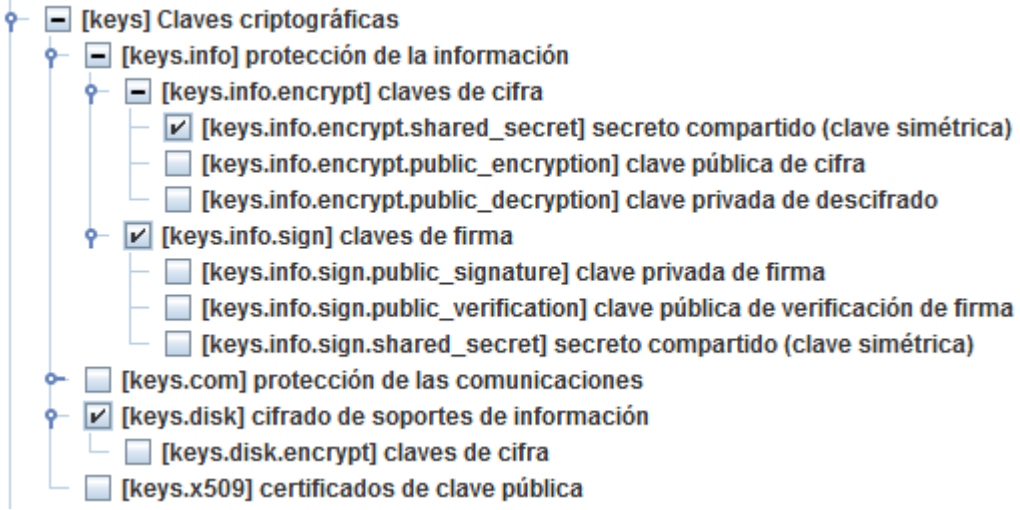
Las marcas indican

☑ Indica que en sistema hay al menos un activo con esta característica

▬ indica que alguna característica está marcada bajo esta

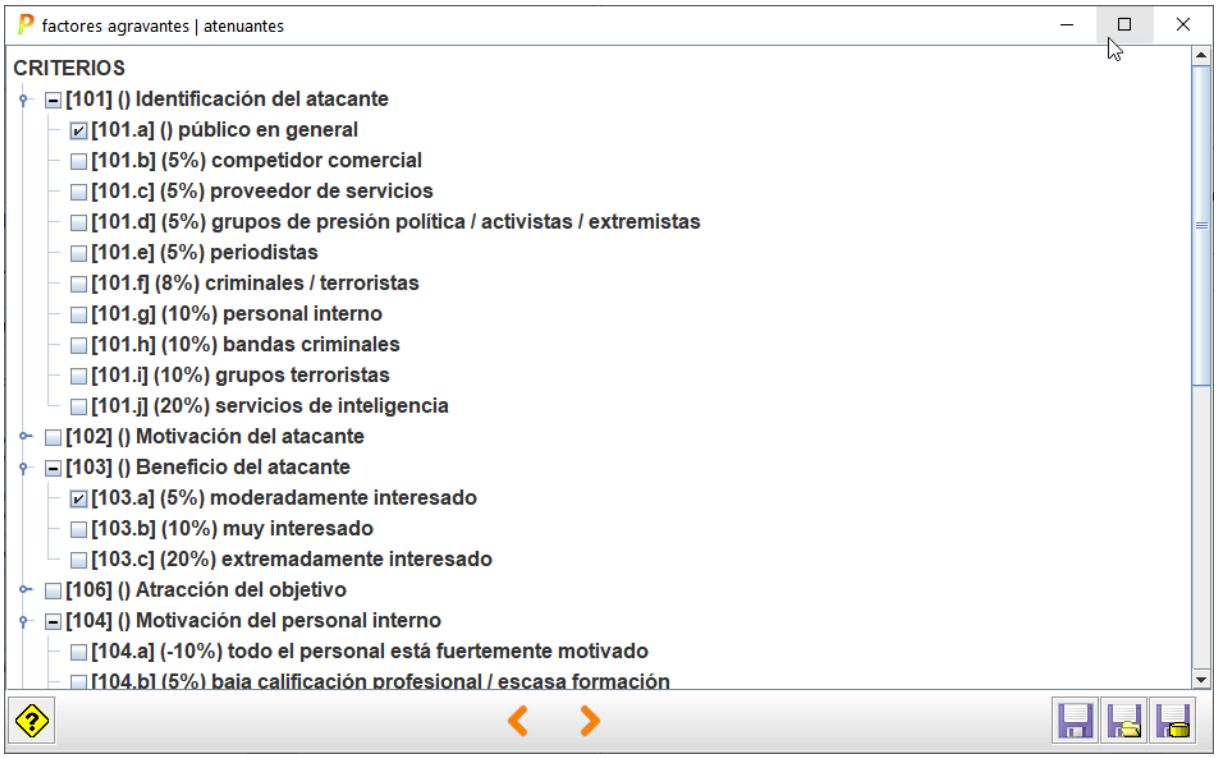
☐ indica que en el sistema no hay ningún activo con esta característica

Ejemplo



II.4 Agravantes y atenuantes

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

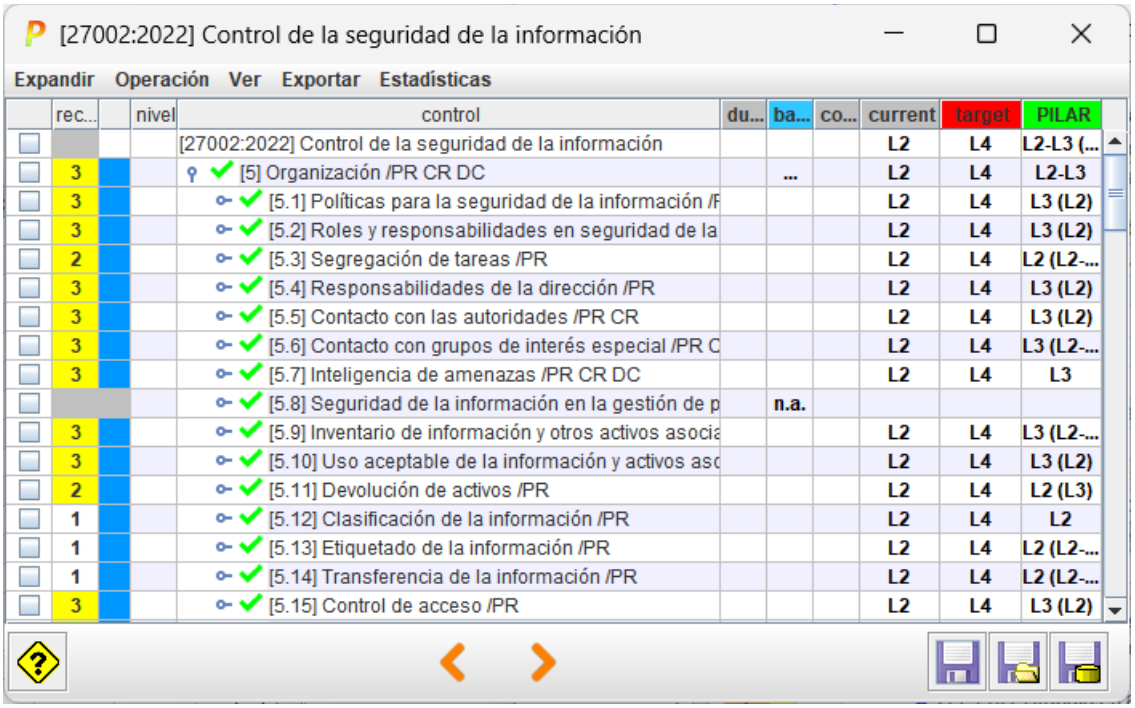


Marque las características propias de su sistema.

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

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



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

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] indica 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). Cuando un control obligatorio se marca como 'n.a.', PILAR mantiene el color para recordar que es una situación singular.

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.

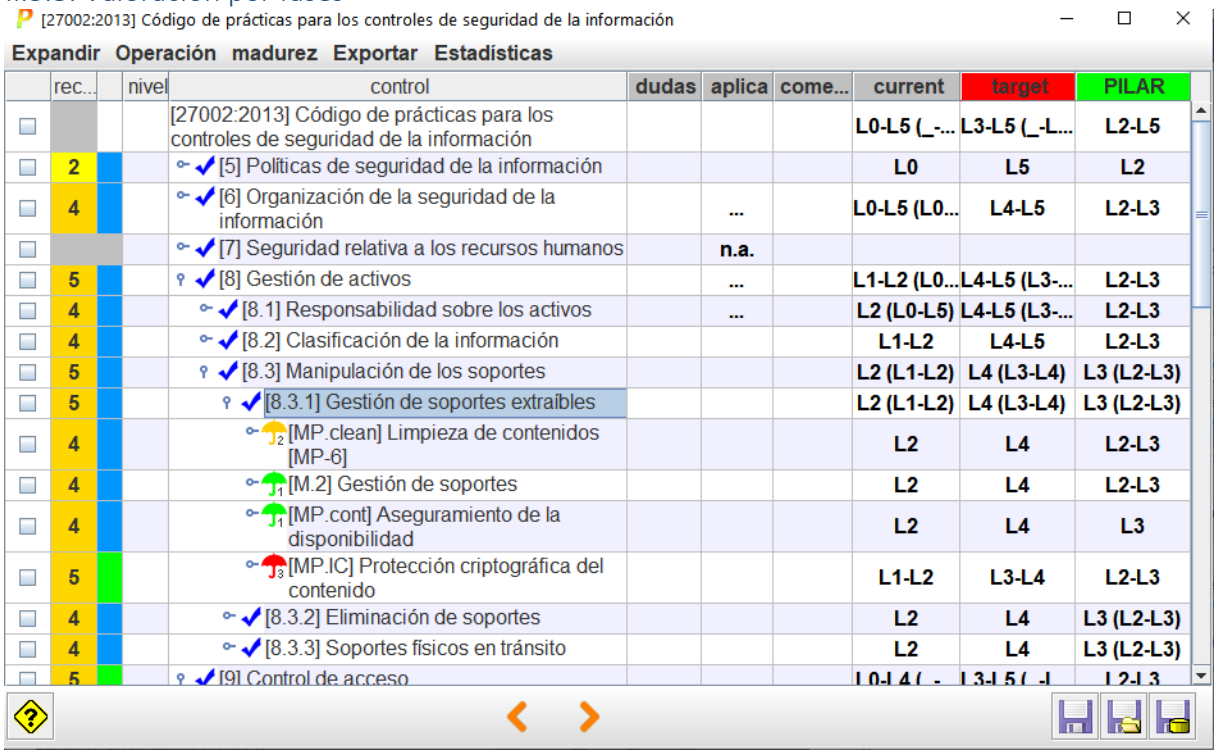
O puede ocurrir que el control sería útil, pero el sistema dispone de otras medidas de protección.

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.

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 por fases



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 sendillas, 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

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.

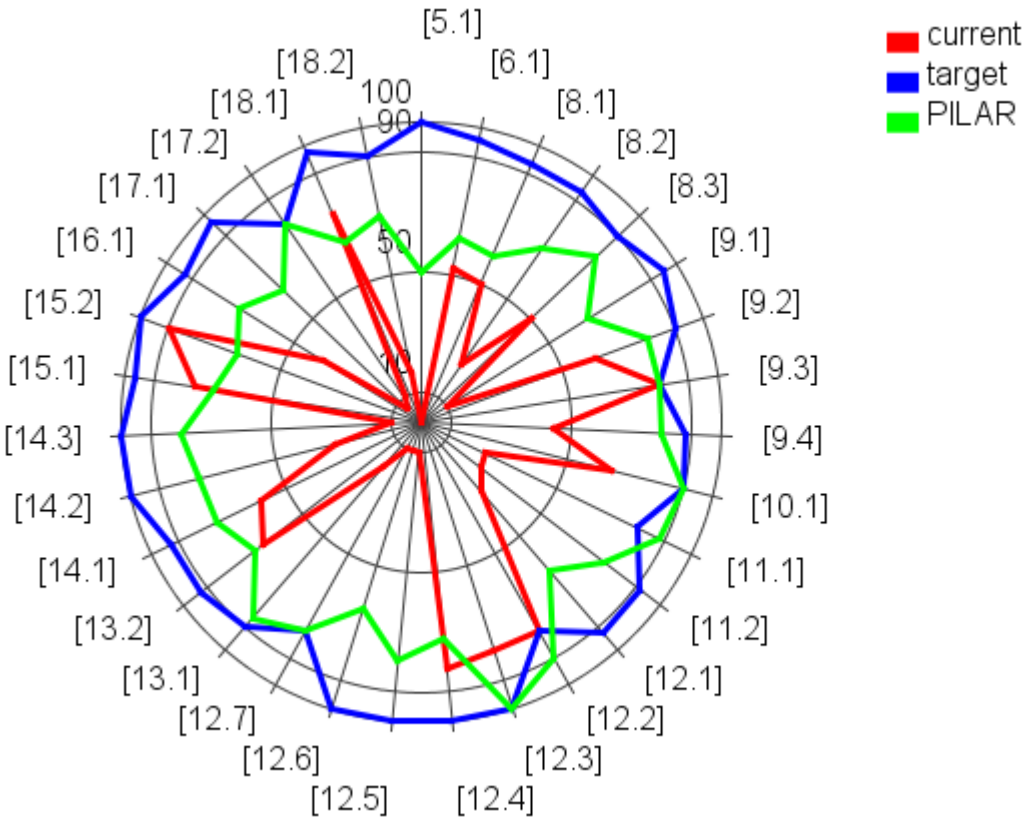
PILAR distingue entre la madurez de las salvaguardas (técnica) y la madurez de los controles (formal), presentado ambos valores simultáneamente si son diferentes.

[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 hacer 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

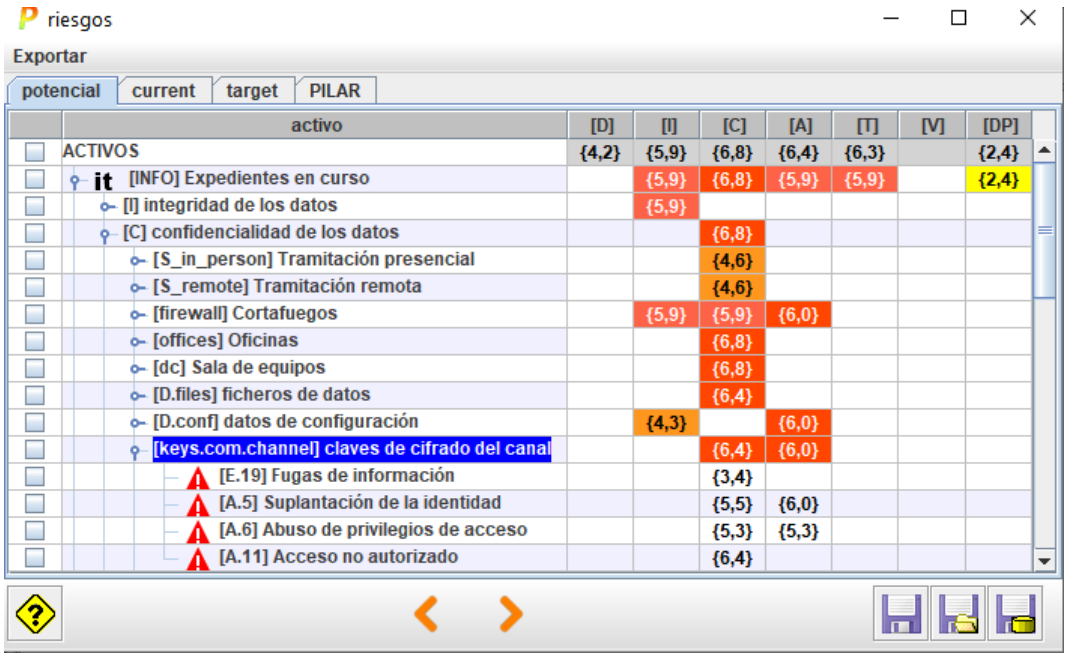
II.5.5. Dudas y comentarios

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

La columna [comentario] puede albergar comentarios referentes a la medida.

II.6 Riesgo

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.



activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	{4,2}	{5,9}	{6,8}	{6,4}	{6,3}		{2,4}
it [INFO] Expedientes en curso		{5,9}	{6,8}	{5,9}	{5,9}		{2,4}
[I] integridad de los datos		{5,9}					
[C] confidencialidad de los datos			{6,8}				
[S_in_person] Tramitación presencial			{4,6}				
[S_remote] Tramitación remota			{4,6}				
[firewall] Cortafuegos		{5,9}	{5,9}	{6,0}			
[offices] Oficinas			{6,8}				
[dc] Sala de equipos			{6,8}				
[D.files] ficheros de datos			{6,4}				
[D.conf] datos de configuración		{4,3}		{6,0}			
[keys.com.channel] claves de cifrado del canal			{6,4}	{6,0}			
[E.19] Fugas de información			{3,4}				
[A.5] Suplantación de la identidad			{5,5}	{6,0}			
[A.6] Abuso de privilegios de acceso			{5,3}	{5,3}			
[A.11] Acceso no autorizado			{6,4}				

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

El árbol proporciona acceso a:

Nivel 1: activos esenciales: riesgo repercutido

Nivel 2: por dimensión de seguridad (repercutido)

Nivel 3: activos de soporte: riesgo acumulado

Nivel 4: amenazas: riesgo acumulado

II.7. Informes

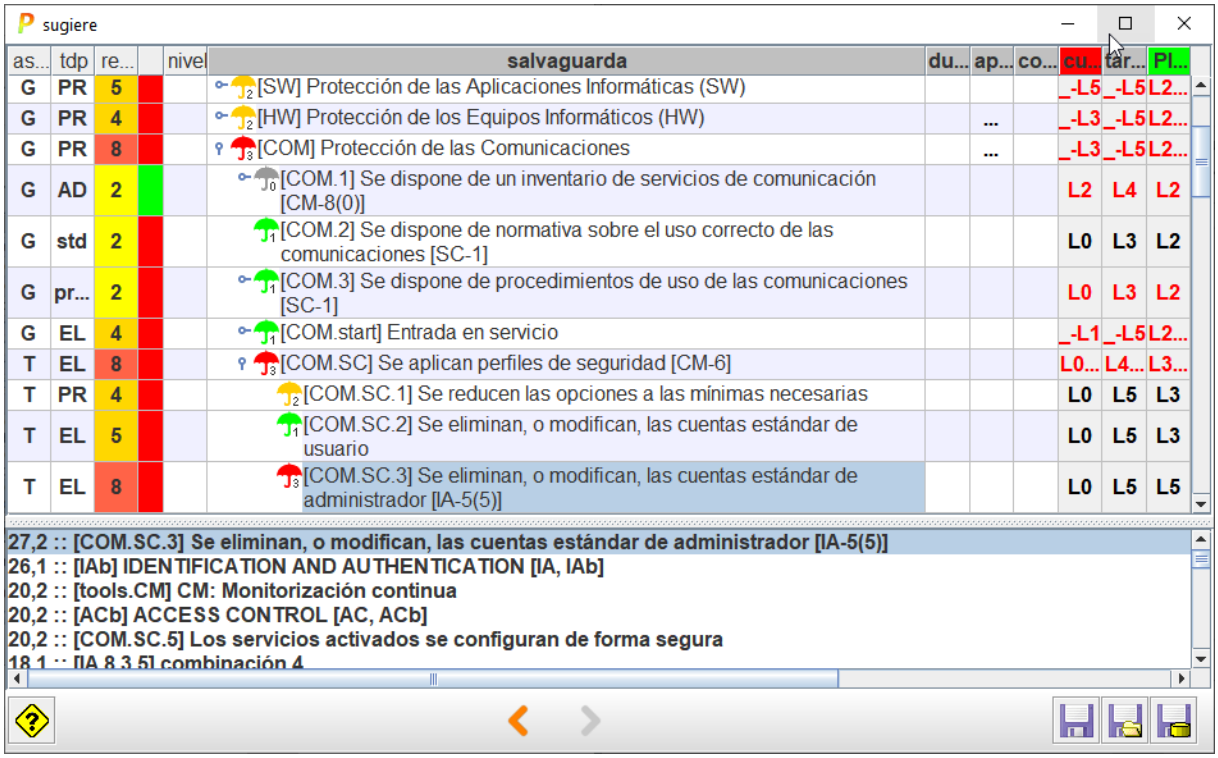
PILAR proporciona una serie de informes predefinidos. Los informes se generan en formato RTF, un formato que puede editarse con los procesadores de texto habituales.

Haga clic en el informe que desea generar.

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

II.8. Mejoras

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.



La columna [aspecto] presenta una G para medidas de gestión, T para medidas técnicas, F para seguridad física y P para personal.

La columna [tdp] presenta el tipo de protección

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

Por último, el color denota la importancia relativa de la medida:

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

Capítulo III – Personalización

Se puede personalizar PILAR editando varios ficheros en el directorio de librería.

A continuación, se muestran algunas posibilidades. Consulte la documentación para más detalle:

> "Personalization" en https://www.pilar-tools.com/doc/

III.1. Fichero de configuración

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

> MICRO_..._es.car

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

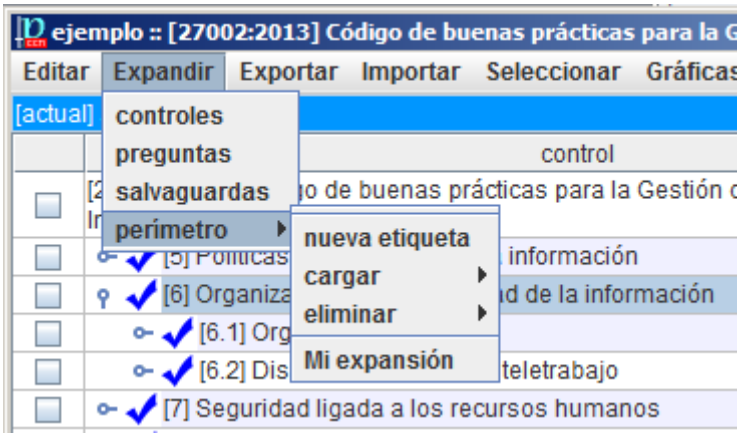
Algunos ajustes que se pueden hacer:

- 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)
- …

III.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
```

III.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 https://www.pilar-tools.com/doc/

Puede establecer los patrones por defecto para sus análisis:

> Ver “Personalización” en https://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

III.4. Perfiles de ataque

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.

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.

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]

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.

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 sueco 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).