PILAR – Manual de Usuario (2023.2)

Noviembre, 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.

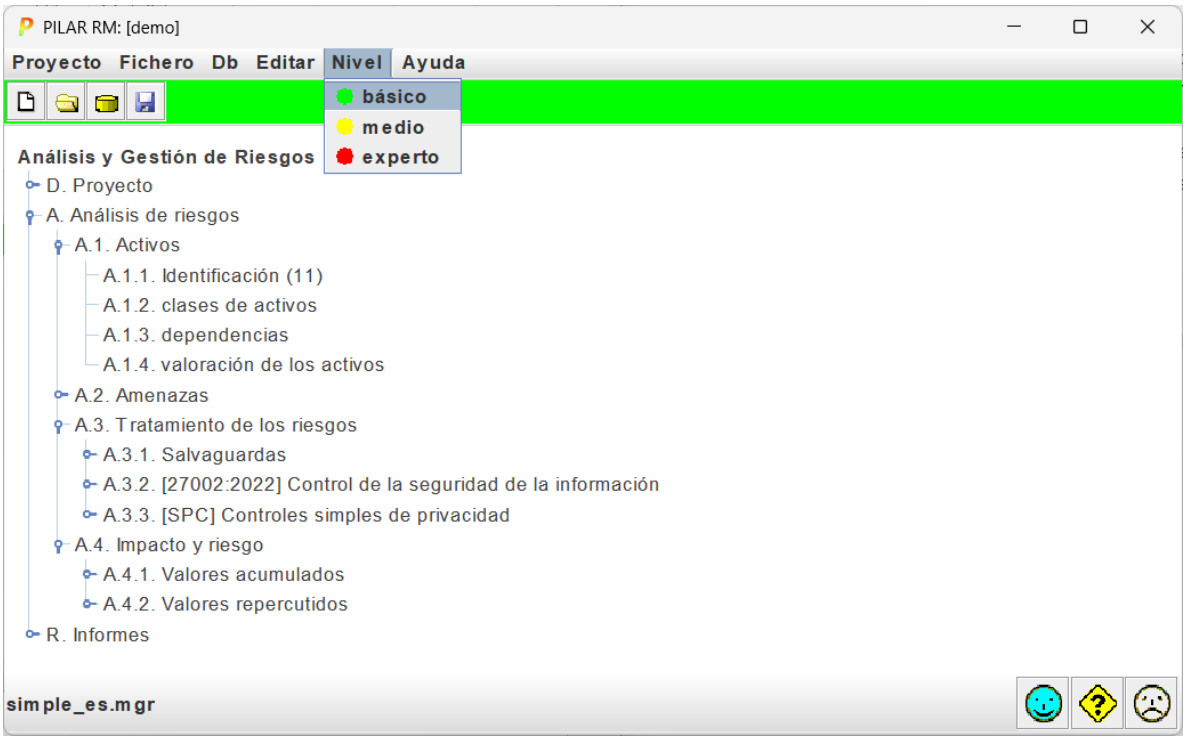
El análisis de riesgos proporciona información para decidir sobre la asignación de recursos, ya sean técnicos o de otro tipo, para proteger organización.

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



II.1. Configuración

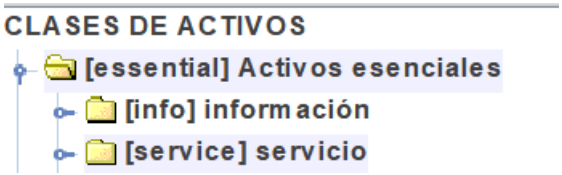
Estas son las opciones más utilizadas:

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

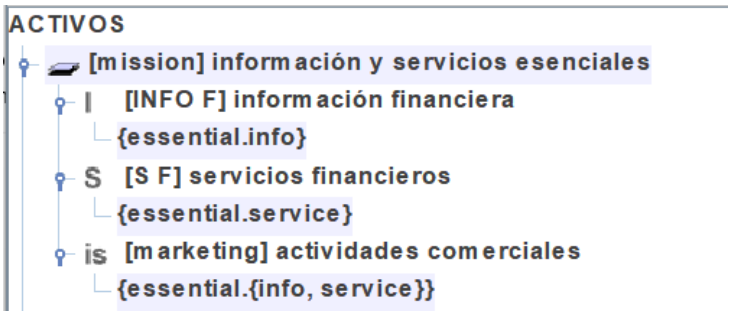
II.2. Activos esenciales

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

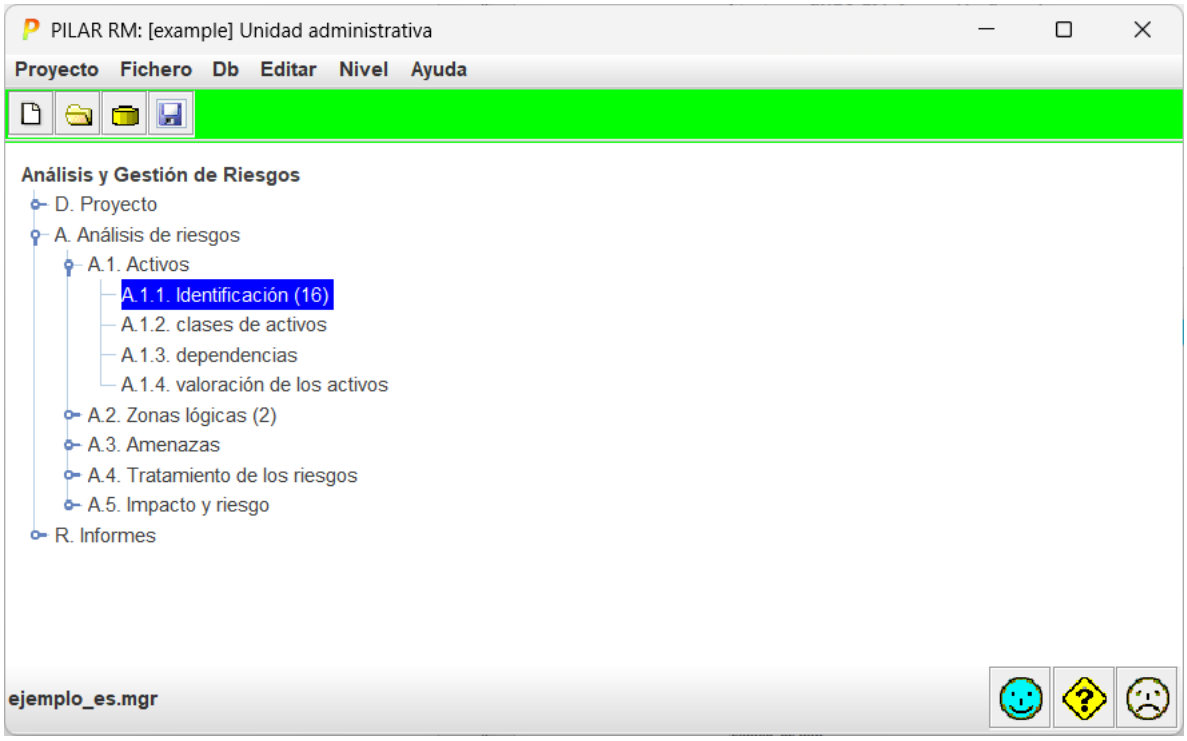


Los activos esenciales pueden ser de tipo 'información', o de tipo 'servicio', o una combinación de ambos. Lo importante es que tienen un nombre que los identifica y que es entendido por los niveles de gobierno y gestión de la empresa: los dueños del riesgo.

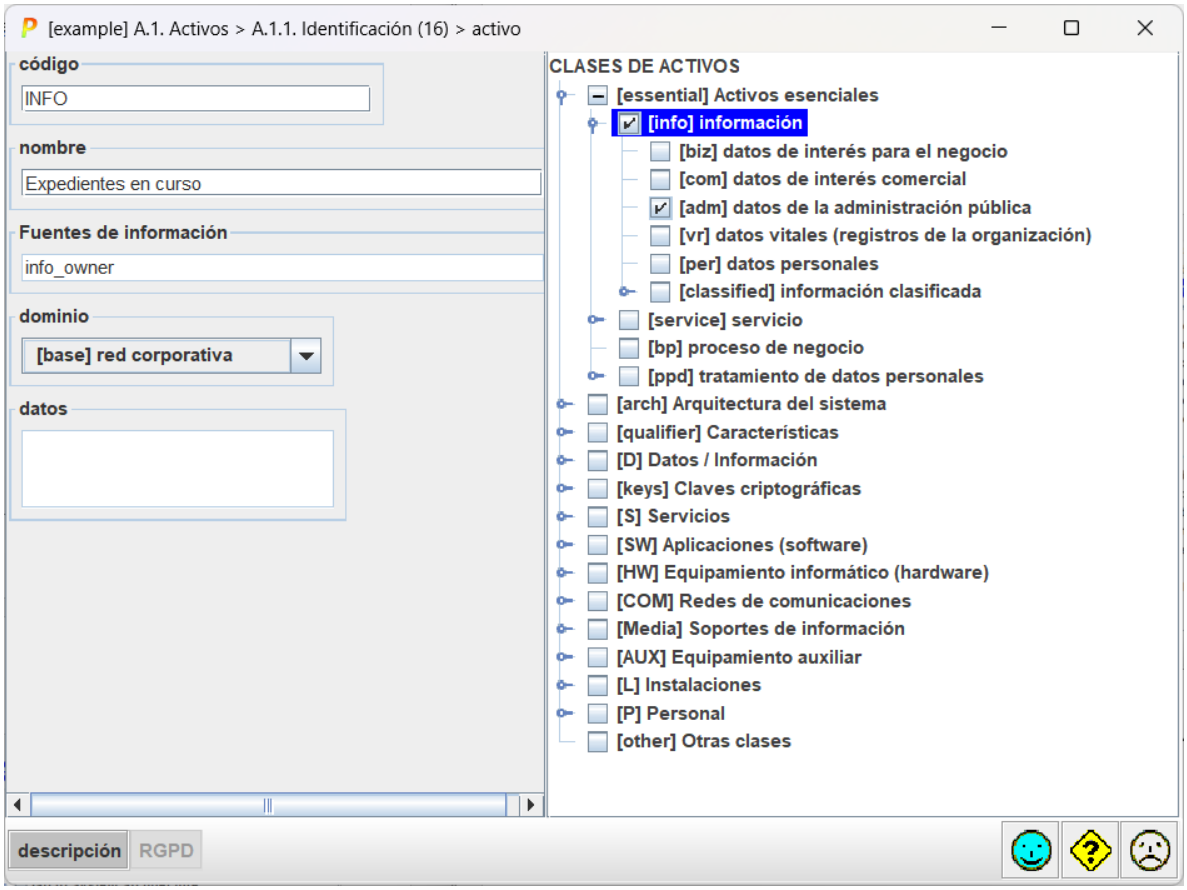


II.2.1. Identificación y caracterización

Análisis de riesgos > Activos > Identificación



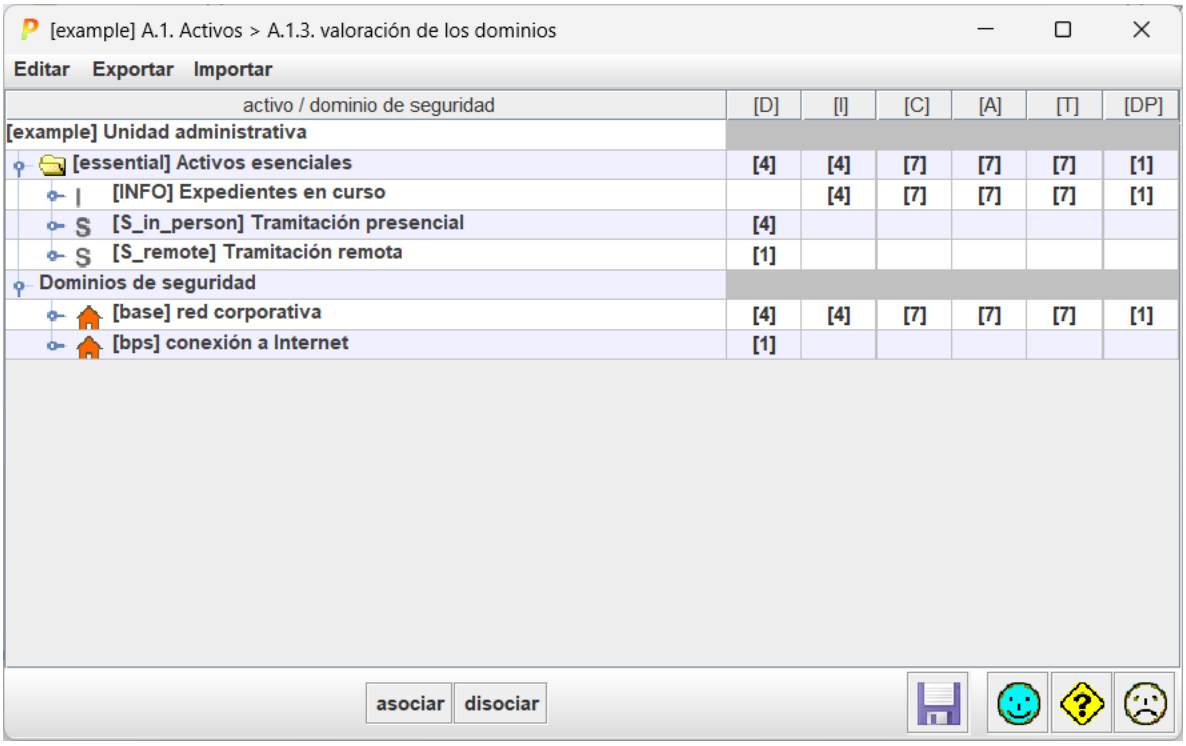
- Capas > Nueva capa
    - [B] Activos esenciales
- Activos > Nuevo activo
    - Seleccione un nombre corto (código) y una descripción sucinta (nombre)
    - Seleccione las clases que considere oportunas



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

II.2.2. 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 A y T, puede usar el máximo de I y C

Para los activos de servicio:

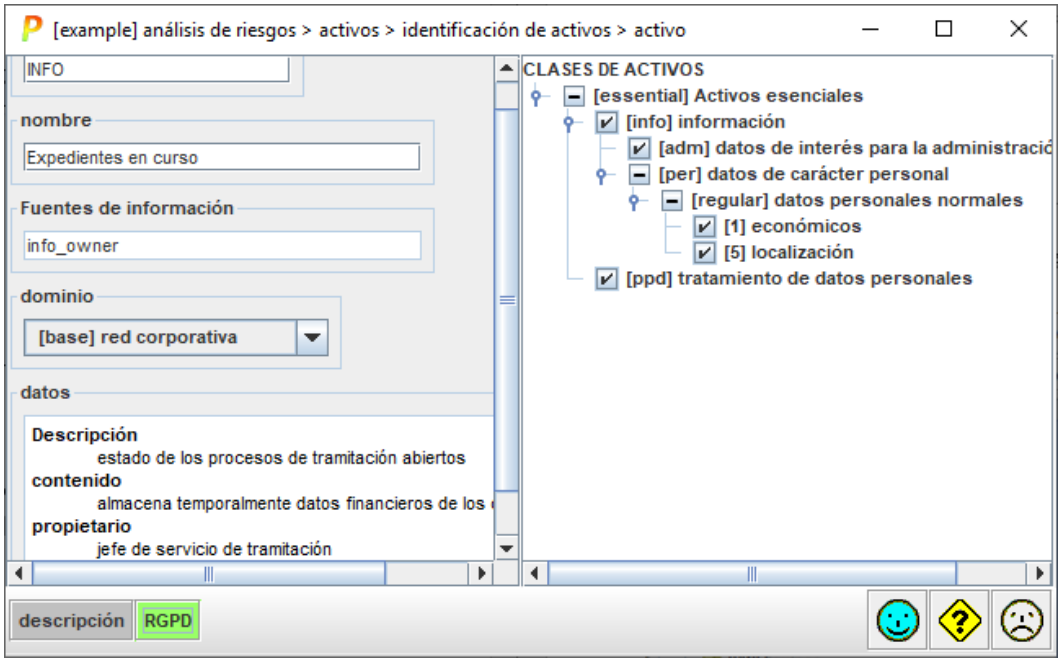
- requisitos de disponibilidad

Para los activos que manejan datos personales

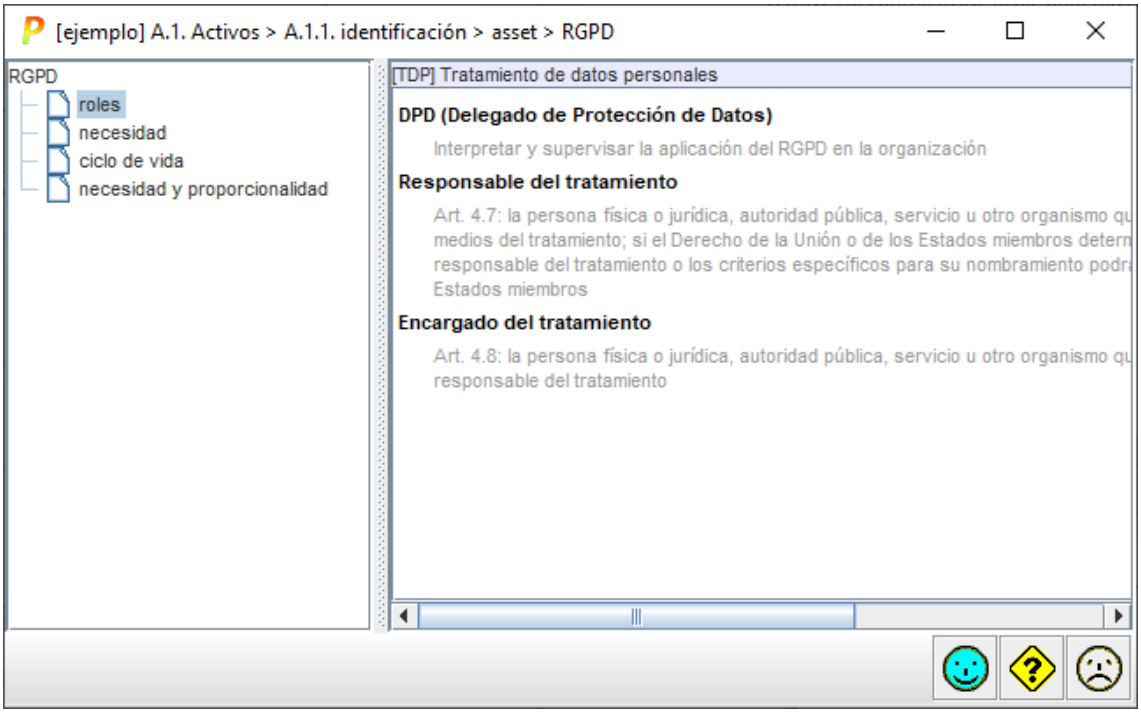
- requisitos de privacidad (DP)

II.2.3. Datos personales

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



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

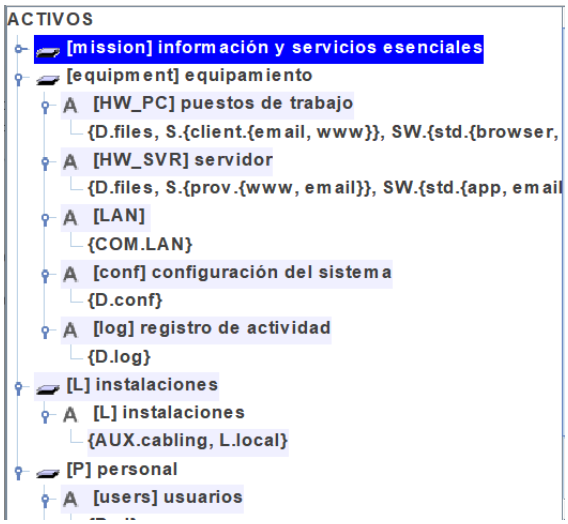


Los datos así recopilados se llevan a la documentación del sistema (informes).

II.3. Activos de soporte

Análisis de riesgos > Activos > Identificación

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



Cada activo debe calificarse con las clases que utiliza PILAR para proponer amenazas (oportunidades para los atacantes) y proponer medidas 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.4. Automatización

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

Análisis de riesgos > Activos > valoración de los activos

PILAR aplica un perfil típico de ataque; es decir,

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

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

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

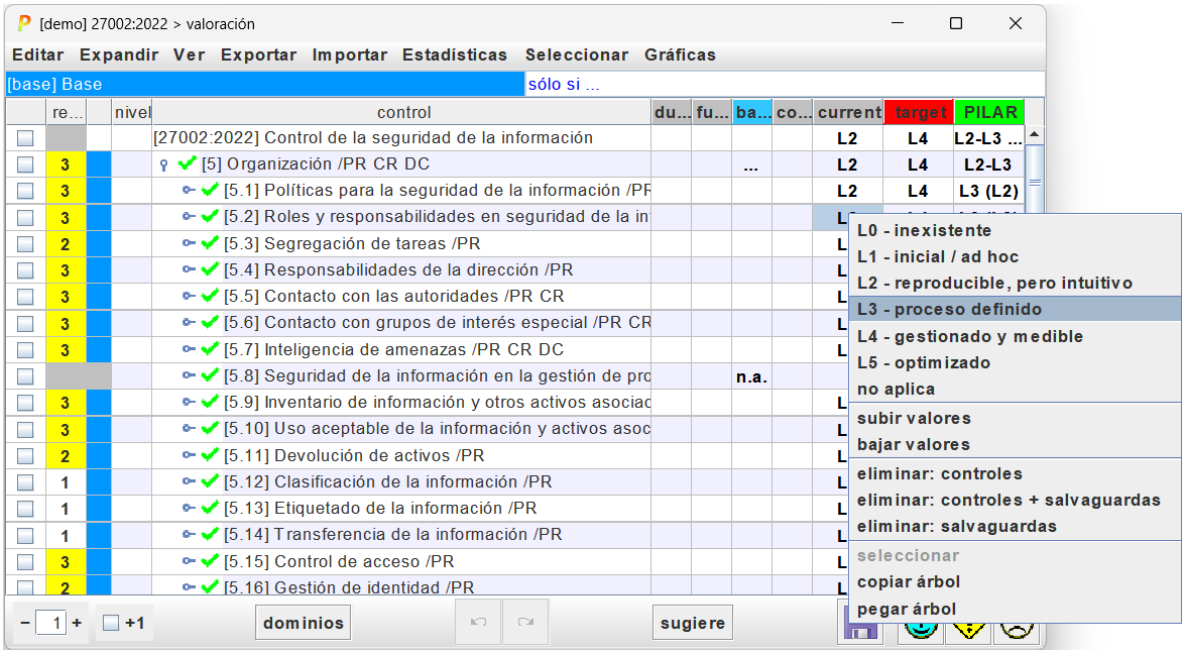
II.6. Perfiles de seguridad

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

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

Perfiles de seguridad > 27002:2013 > Valoración

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



II.6.1 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.6.2. 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.6.3. Valoración

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

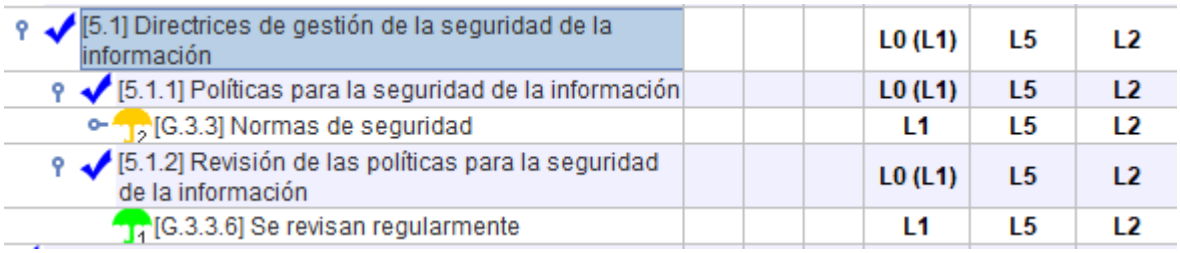
Cuando una medida se marca como XOR, se puede elegir cuál de los componentes optativos se va a utilizar en este sistema. PILAR marca n.s. (no seleccionado) lo que no se usa, valorándose la madurez de la opción en uso.

clic derecho > seleccionar

Presentación

Puede indicarle a PILAR que presente niveles de madurez, o un porcentaje de efectividad, o que compare la madurez presente con la sugerida.

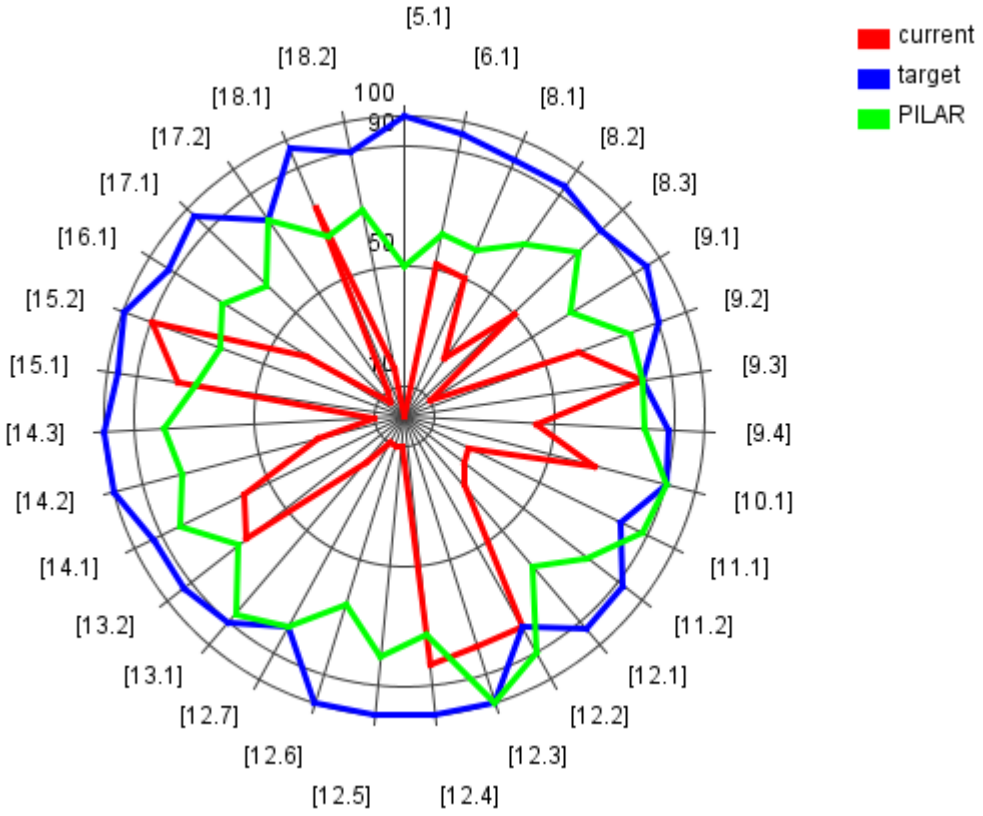
PILAR distingue entre la madurez de las salvaguardas (técnica) y la madurez de los controles (formal), presentado ambos valores simultáneamente si son diferentes.



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.6.4. 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	no es aplicable

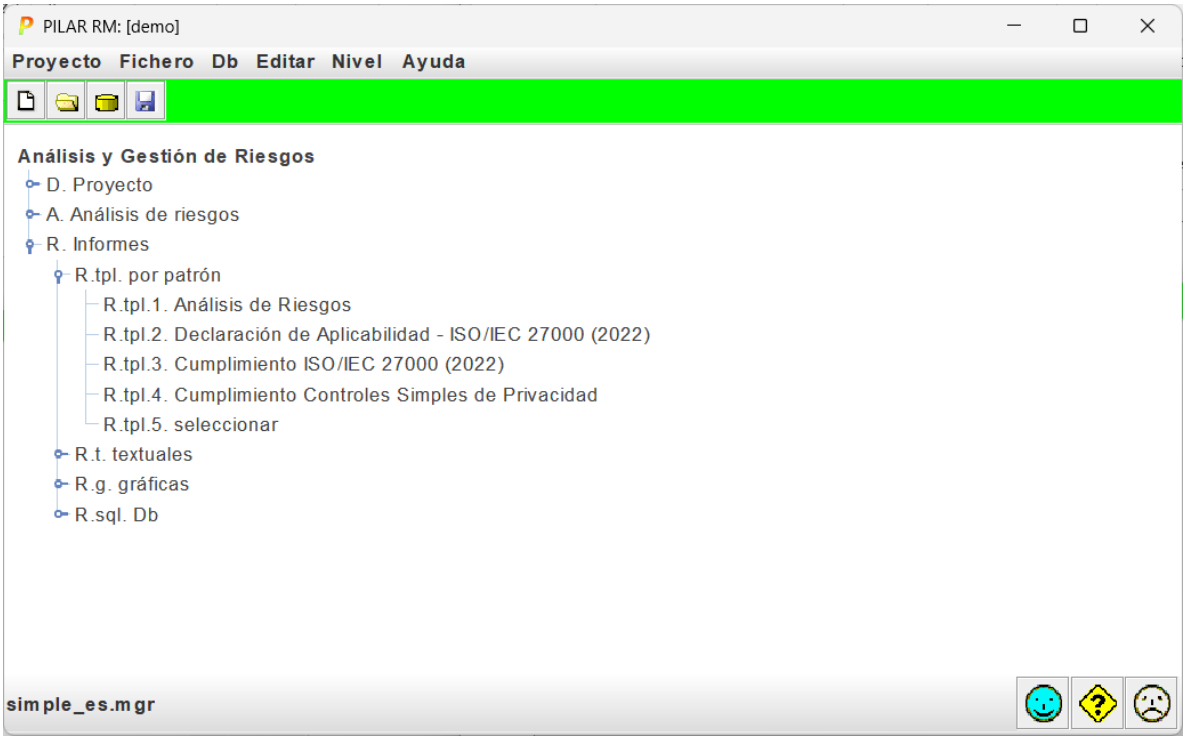
II.6.5. Dudas y comentarios

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.7. Informes

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



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

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

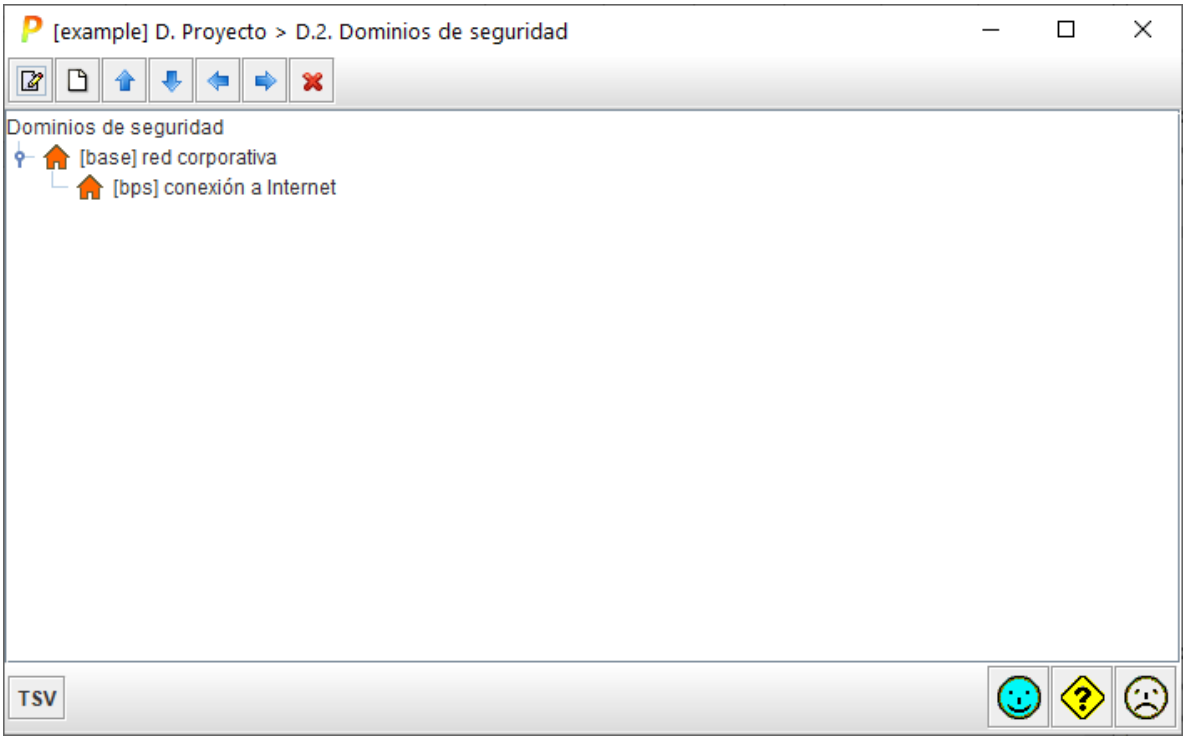
Capítulo III - Uso Medio

III.1. Dominios de seguridad

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

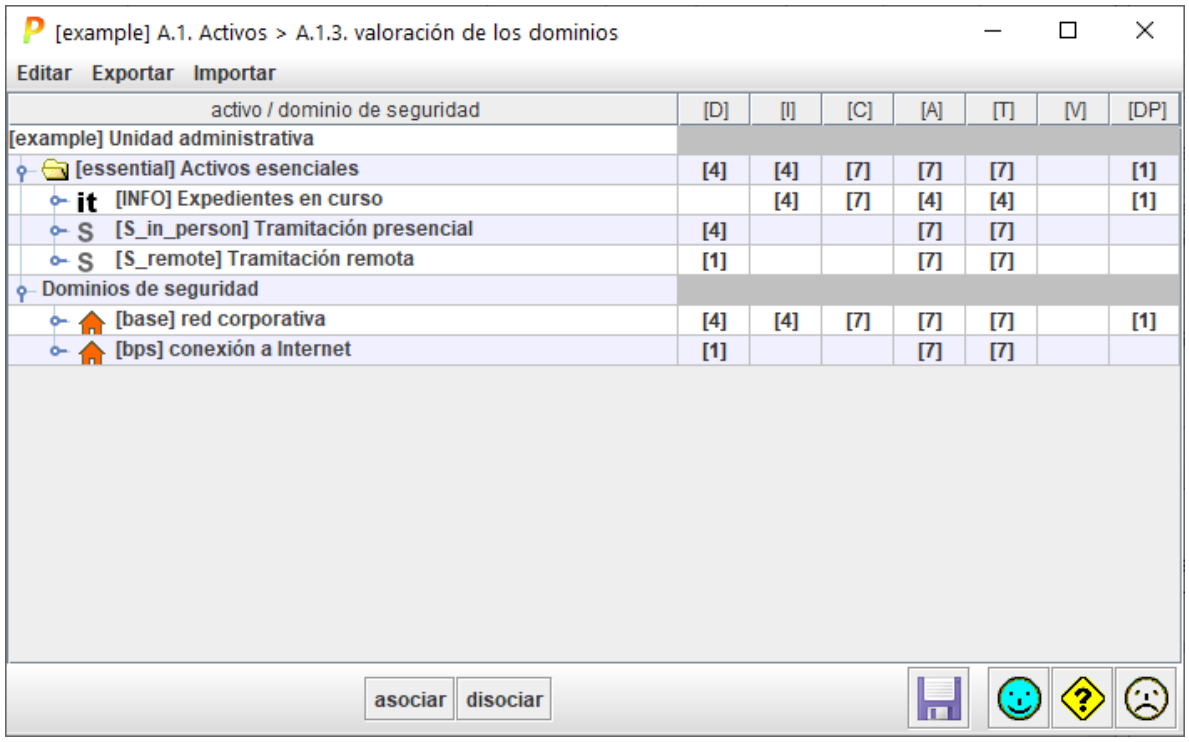
Proyecto > Dominios de seguridad

Para identificar dominios de seguridad



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

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

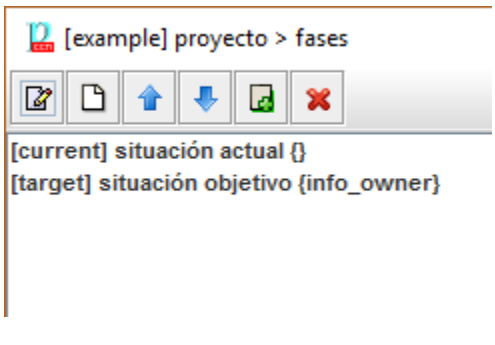


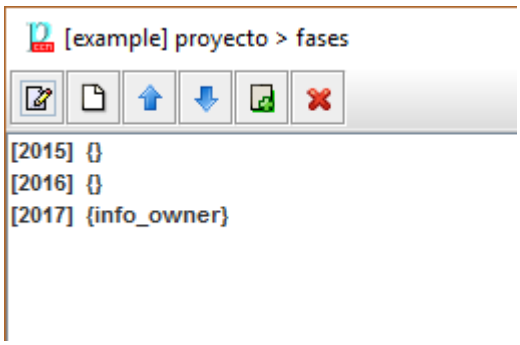
III.2. Fases del proyecto

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

Proyecto > Fases del proyecto

Para identificar y ordenar las fases.





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

III.3. Salvaguardas

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

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

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

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

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

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.

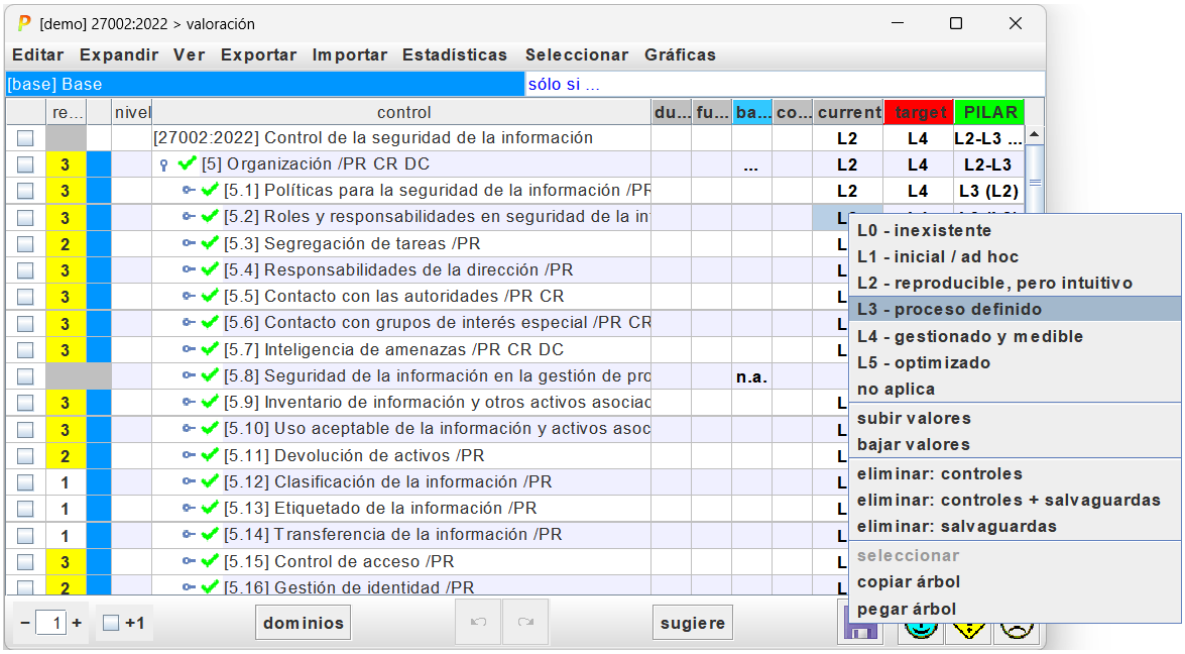
La columna [tdp] presenta el tipo de protección que proporciona la salvaguarda

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

No todas las salvaguardas son igual de importantes:

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

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

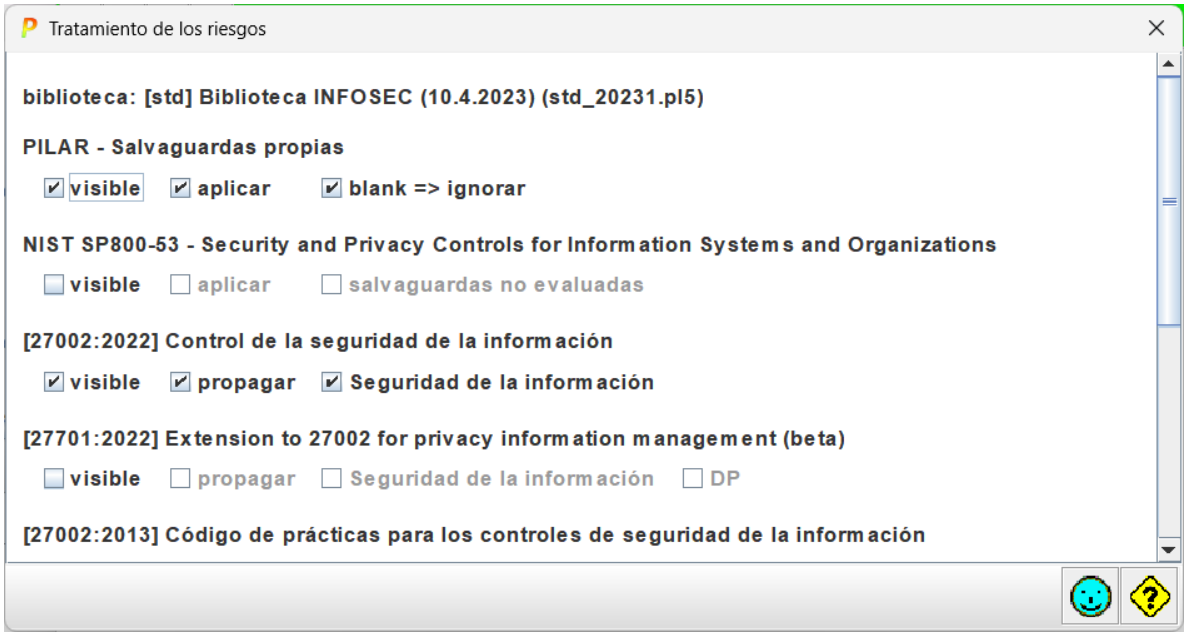


La opción seleccionada aparece [entre corchetes]. La selección no se hereda entre dominios: son independientes.

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.

III.4. Tratamiento del riesgo



Puede seleccionar las medidas de seguridad que usa para tratar el riesgo y las medidas de seguridad que usa para cumplimiento.

Para la colección de salvaguardas propias de PILAR,

- los usuarios pueden ignorarlas por completo
- o verlas, pero no usarlas para tratar el riesgo
- o verlas y aplicarlas para tratar el riesgo

Para la colección de salvaguardas NIST 800-53 rev.5,

- los usuarios pueden ignorarlas por completo
- o verlas, pero no usarlas para tratar el riesgo
- o verlas y aplicarlas para tratar el riesgo

Algunos perfiles de seguridad de EVL pueden usarse directamente para tratar el riesgo

- los usuarios pueden ignorarlos por completo
- o verlos y aplicarlos para tratar el riesgo
- además, la valoración de un control puede propagarse a las salvaguardas asociadas

Algunos perfiles de seguridad EVL solo están disponibles para cumplimiento

- los usuarios pueden ignorarlos por completo
- además, la valoración de un control puede propagarse a las salvaguardas asociadas

Muchos perfiles de EVL vinculan los controles a las salvaguardas, y los usuarios pueden valorar ambos en paralelo.

La versión anterior de PILAR usaba ÚNICAMENTE la colección de protecciones de PILAR para tratar el riesgo y usaba perfiles EVL para el cumplimiento. Puede volver a ese modo de trabajo seleccionando opciones como esta

- PILAR: visible + aplicar
- NIST SP800-53: invisible

Capítulo IV - Uso Avanzado

IV.1. Dependencias entre activos

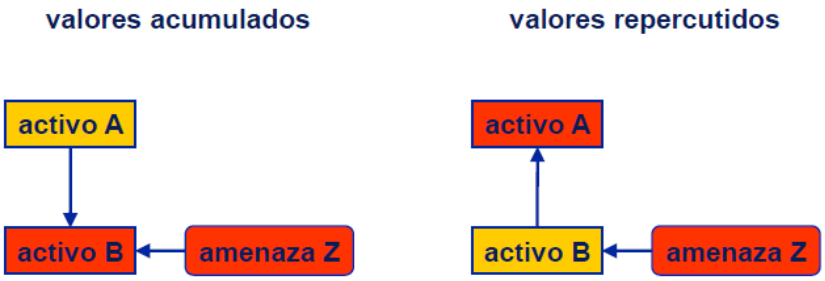
La aproximación de trasladar uniformemente los requisitos de seguridad a todos los activos en el mismo dominio es muy rápida, pero a veces puede resultar excesivamente simplista. Por ejemplo, cuando cada información y cada servicio usan sólo algunos servidores, no todos.

Las dependencias proporcionan una transferencia controlada de valor.

Hay que activar el uso de dependencias:

> Editar > Opciones > Valoración > activos + dependencias

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

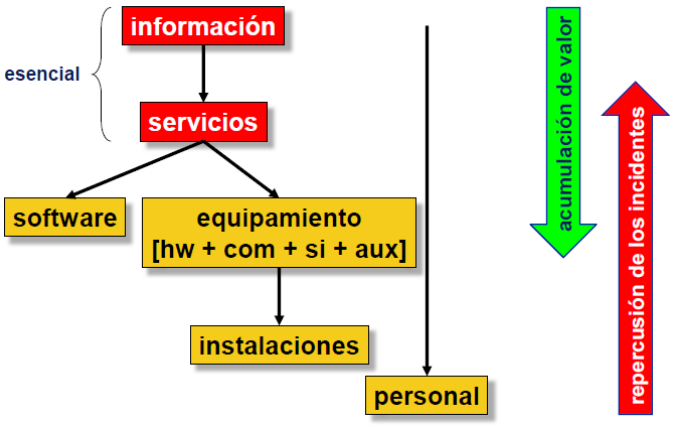


- los requisitos de seguridad (niveles de valoración) del activo A se transfieren al activo B
- los ataques en el activo B tienen un efecto directo sobre el valor acumulado en B
- los ataques en el activo B tienen un efecto indirecto (repercutido) en el activo A

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

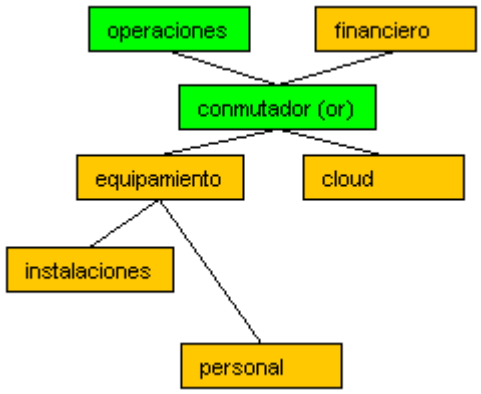
Como reglas generales:

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



IV.1.1. Nodos OR

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



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

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

IV.2. Valoración activo a activo

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

IV.3. Amenazas

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

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

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

También puede modificar las amenazas manualmente dentro de PILAR

Editar > Opciones > Amenazas > manual

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

Editar > Opciones > Amenazas > mix

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

IV.4. Perfiles de seguridad – Cumplimiento

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

Este mecanismo de propagación automática puede inhibirse

Proyecto > Tratamiento > Perfil de seguridad: propagar > no

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

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

madurez_del_control (madurez_de_las_salvaguardas)

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

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

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

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

Capítulo V – Personalización

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

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

> "Personalización" en https://www.ar-tools.com/doc/

V.1. Fichero de configuración

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

> STIC_es.car

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

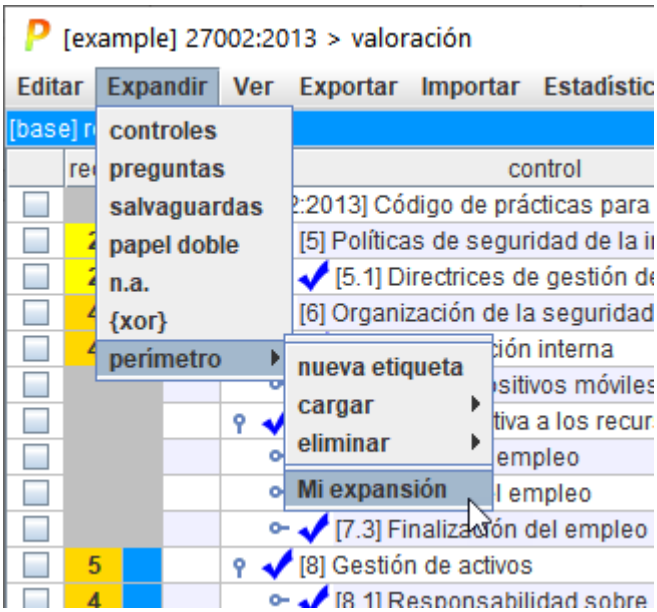
Algunos ajustes que se pueden hacer:

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

V.2. Perímetros

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

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



Los pasos a seguir son los siguientes:

1. Cree una nueva etiqueta con un nombre de su elección

   `Expandir > perímetro > nueva etiqueta`

2. En el árbol, expanda o contraiga nodos hasta obtener el grado de detalle que le sea útil
3. Cargue el perímetro en su etiqueta

   `Expandir > perímetro > cargar > su etiqueta`

4. Para cambiar el perímetro, repita los pasos 2-3

Par usar una etiqueta

`Expandir > perímetro > su etiqueta`

Para eliminar una etiqueta

`Expandir > perímetro > eliminar > su etiqueta`

V.3. Patrones para informes

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

Ver “Patrones” en https://www.ar-tools.com/doc/

Puede establecer los patrones por defecto para sus análisis:

Ver “Personalización” en https://www.ar-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:

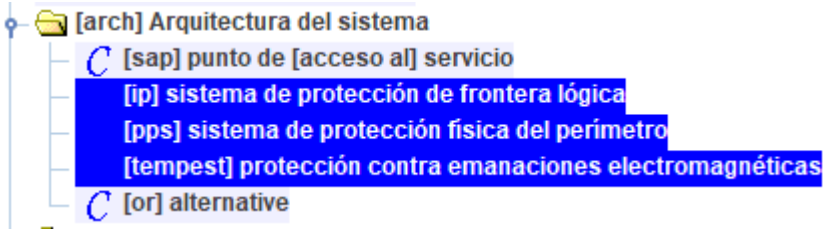
- tenemos 2 zonas
  - dentro del área
  - fuera del área
- y una frontera, el local

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

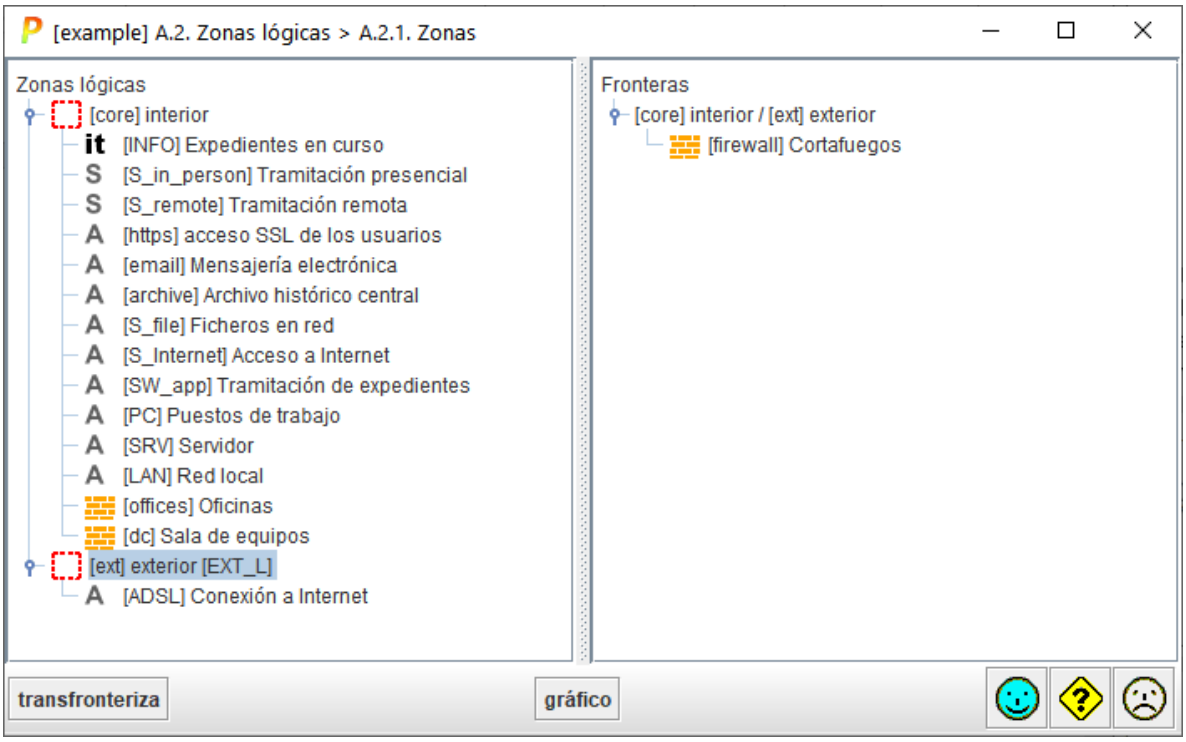
PILAR proporciona

- 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] y que esté ubicado entre las zonas que protege



VI.2. Vulnerabilidades

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

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

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

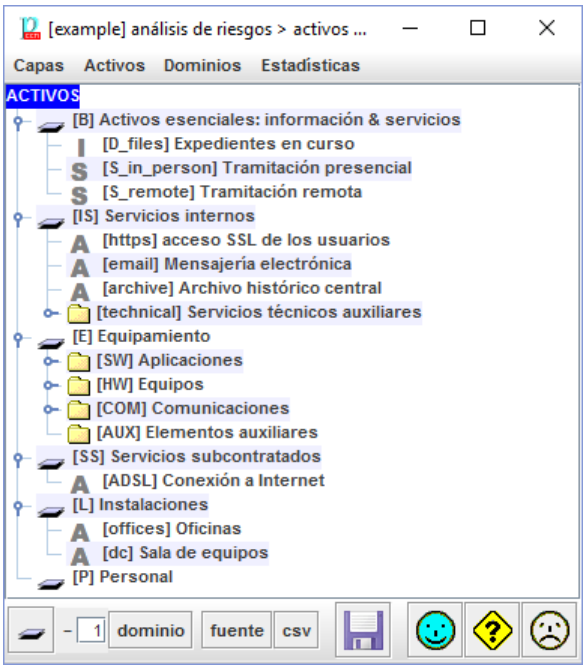
En el mundo CVE, una vulnerabilidad es un estado del sistema de información que

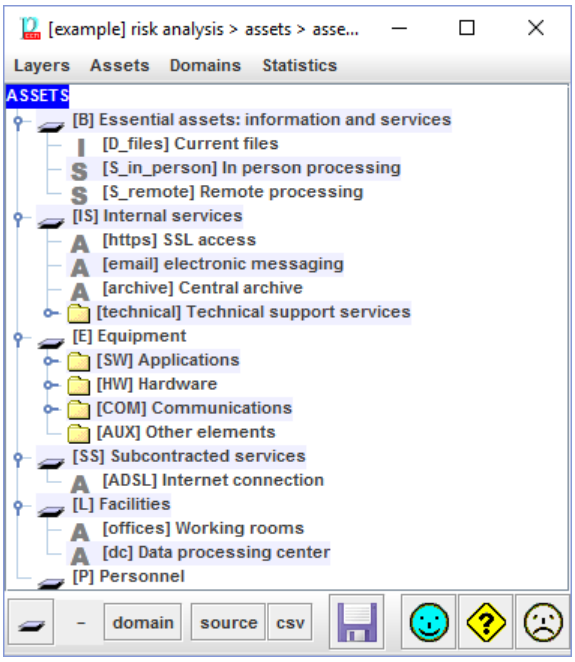
- permite a un atacante ejecutar acciones como si fuera otro usuario, o
- permite a un atacante acceder a datos violando las restricciones especificadas de control de acceso, o
- permite a un atacante suplantar la personalidad de otra entidad, i
- permite a un atacante llevar a cabo un ataque de denegación de servicio.

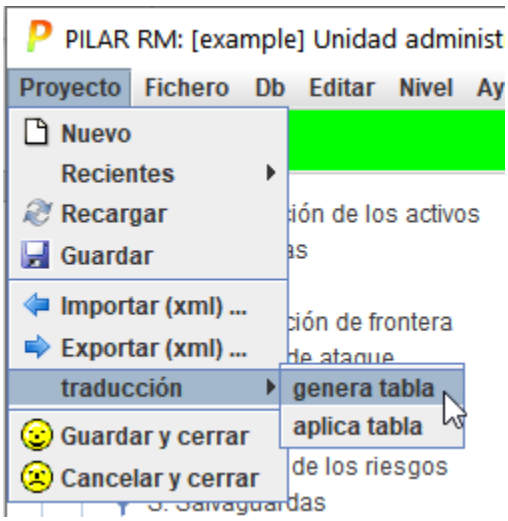
Ver "vulnerabilidades" en https://www.ar-tools.com/doc/

VI.3. Idiomas

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







En la ventana principal

Proyecto > Traducción > generación

Seleccione un fichero

ejemplo.rw

El resultado es un fichero de texto con reglas de traducción, una por línea, que el usuario puede editar. Las reglas se aplican secuencialmente.

Alternativamente puede usar el formato CSV (Excel), tanto para generar la tabla como para aplicarla. Para ello, indique ".csv" como extensión del fichero de reglas.

Ejemplo,

```
asset: [mission] System mission -> [] Misión del sistema
```

PILAR busca un activo con código 'mission'. No cambia el código, pero cambia el nombre a español. También podría indicar un nuevo código en el lado derecho:

```
asset: [mission] System mission -> [misión] Misión del
sistema
```

VI.4. Control de acceso

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

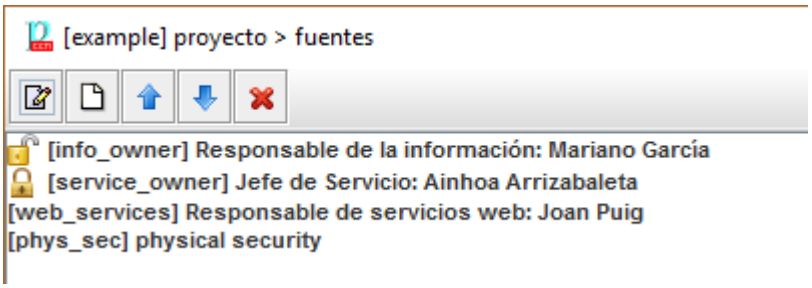
Conceptos básicos:

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

Los siguientes elementos tienen control de acceso

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

VI.4.1. Contraseñas



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

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

Para establecer o eliminar una contraseña.

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

Para abrir una sesión. Se solicita la contraseña.

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

Para cerrar una sesión.

VI.4.2. Restricciones de acceso: dominios de seguridad

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

- modificar las fuentes
- modificar el código, el nombre o la descripción
- modificar activos (en ese dominio)
    - crear, cambiar de dominio o eliminar

    - modificar fuentes
    - modificar el código, el nombre, la descripción o atributos administrativos
    - modificar las clases
- modificar las salvaguardas para el dominio
    - modificar las fuentes
    - modificar aplicabilidad, comentarios o valoración
- modificar controles para el dominio
    - modificar las fuentes
    - modificar aplicabilidad, comentarios o valoración

VI.4.3. Restricciones de acceso: fases del proyecto

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

- modificar las fuentes
- modificar el código, el nombre o la descripción
- modificar las salvaguardas para la fase
    - modificar las fuentes
    - modificar aplicabilidad, comentarios o valoración
- modificar controles para la fase
    - modificar las fuentes
    - modificar aplicabilidad, comentarios o valoración

VI.4.4. Restricciones de acceso: zonas

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

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

VI.5. Bases de datos

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

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

Ver “tablas SQL” en https://www.ar-tools.com/doc/

VI.6. Modo batch

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

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

Ver “modo batch” en https://www.ar-tools.com/doc/

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.

Las 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 la materialización de una amenaza.

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/
- ISO 31000:2018
  Gestión del riesgo – Principios y directrices.
- ISO/IEC Guía 73:2010
  Gestión del riesgo – Vocabulario.
- IEC 31010:2009
  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
- AS/NZS 4360:2004
  Risk management