PILAR

Análisis y Gestión de Riesgos

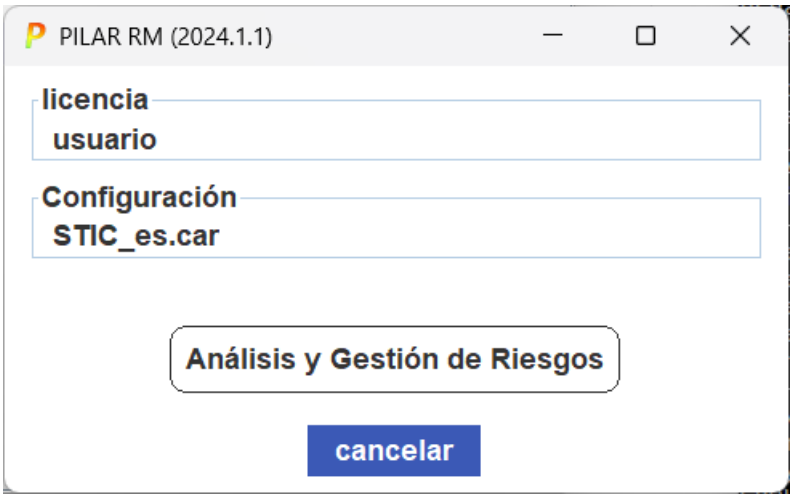
Ayuda

versión 2024.1

Febrero, 2024

General

1 Primera pantalla



licencia

Presenta la licencia en uso.

Haga clic para seleccionar una licencia.

configuración

Presenta la configuración en uso (CAR).

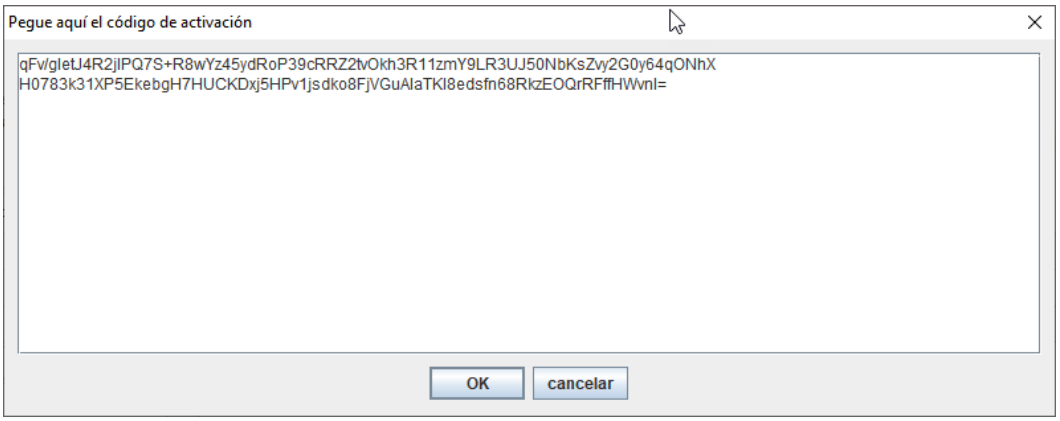
Haga clic para seleccionar una configuración diferente.

1.1 Licencia

Al hacer clic con el botón derecho en la cajita “licencia”, aparecen diferentes opciones:

código de activación

Si ha recibido un código de activación, ingréselo en la pantalla:



NOTA: la activación requiere conexión a Internet para disponer de una licencia válida.

fichero de licencia

Si ha recibido un fichero de licencia (LIC), elíjalo.

licencia de evaluación

Puede usted mismo generar una licencia temporal de evaluación. 30 días.

reset

PILAR olvida la última selección y reinicia el proceso de validación de licencia.

2 Editar / Opciones

El comportamiento de PILAR puede ser ajustado con varias opciones:

Opciones básicas:

- *Opciones / Valoración*
- *Opciones / A*
- *Opciones / T*
- *Opciones / Probabilidad*
- *Opciones / Efectos*
- *Opciones / Amenazas*
- *Opciones / Madurez*
- *Opciones / Fases especiales*

Opciones avanzadas:

- *Opciones / CSV*
- *Opciones / Modelo Valor*
- *Opciones / Fases del proyecto*
- *Opciones / Dominios y fases*
- *Opciones / xor*
- *Opciones / bucles*
- *Opciones / Guardar*
- *Opciones / Exportar: salvaguardas*
- *Opciones / Transferencia de valor entre dimensiones*
- *Opciones / Tiempos*
- *Opciones / PD risk*
- *Opciones / Riesgo residual*
- *Opciones / ENS*
- *Opciones / ROLL*

Estas opciones se especifican para cada proyecto; es por ello que solo se pueden seleccionar cuando hay un proyecto abierto, y solo afectan a dicho proyecto.

Algunas versiones personalizadas de la herramienta pueden proporcionar algunas opciones adicionales.

2.1 Opciones / Valoración

El sistema de información se puede valorar activo por activo (más dependencias) o por dominios de seguridad.

En ambos casos, se valoran los activos esenciales.

valoración / activos + dependencias

el valor de los activos esenciales se aplica a todos los activos del dominio de seguridad

valoración / dominios

el valor se propaga siguiendo las dependencias entre activos

La valoración por dominios es más rápida, mientras que la valoración por dependencias es más precisa.

valoración /mix: activos + dependencias + dominios

si el activo tiene dependencias, se usan; si no, por dominios

2.2 Opciones / Probabilidad

Cómo describir la probabilidad de que se materialice una amenaza.

potencial	probabilidad	nivel	facilidad	frecuencia
XL extra grande	CS casi seguro	MA muy alto	F fácil	100
L grande	MA muy alta	A alto	M medio	10
M medio	P posible	M medio	D difícil	1
S pequeño	PP poco probable	B bajo	MD muy difícil	0,1
XS muy pequeño	MR muy rara	MB muy bajo	ED extremadamente difícil	0.01

2.3 Opciones / Efectos

Cómo describir las consecuencias de la materialización de una amenaza.

nivel	porcentaje
T - total	100%
MA - muy alta	90%
A – alta	50%
M – media	10%
B – baja	1%

2.4 Opciones / Amenazas

amenazas / manual:

el usuario establece explícitamente la valoración de las amenazas (este es el comportamiento de PILAR en versiones anteriores a 4.4)

amenazas / automático:

el sistema aplica la valoración estándar cuando la necesita (este es el comportamiento en PILAR Basic)

amenazas / mix:

Una mezcla de manual y automático. En principio, las amenazas se valoran de forma automática; pero puede marcar activos o amenazas concretas sobre un activo para realizar una valoración manual. De esta forma PILAR respeta algunas valoraciones ajustadas manualmente.

Para marcar como manual, vaya a

Análisis >> Amenazas >> valoración

2.5 Opciones / Madurez

PILAR puede interpretar los niveles de madurez, bien como madurez, bien como el estado de la implementación de las salvaguardas. Es decir, se presenta un texto u otro junto a los niveles L0 a L5.

nivel	madurez	estado
L0	inexistente	inexistente
L1	inicial / ad hoc	iniciado
L2	reproducible, pero intuitivo	parcialmente realizado
L3	proceso definido	en funcionamiento
L4	gestionado y medible	monitorizado
L5	optimizado	mejora continua

PILAR también puede traducir los niveles de madurez a un índice entre 0.0 y 1.0, que a menudo denominamos porcentaje (de cumplimiento).

nivel	índice	porcentaje
L0	0.0	0%
L1	0.1	10%
L2	0.5	50%
L3	0.8	80%
L4	0.9	90%
L5	1.0	100%

2.6 Opciones / Fases especiales

Determina si PILAR presenta, o no, fases adicionales con recomendaciones para las salvaguardas.

Seleccione las que desea que aparezcan de las ofrecidas.

Dependiendo de la configuración elegida, PILAR evalúa una serie de recomendaciones de madures que se presentan como fases especiales; por ejemplo, PILAR. Estas fases no se pueden editar; el usuario simplemente puede verlas y usarlas como sugerencia de la madurez adecuada para cada salvaguarda.

2.7 Opciones – CSV

Puede seleccionar el carácter utilizado para separar columnas al exportar datos a CSV.

2.8 Opciones – Modelo de valor

Puede elegir entre valoración cualitativa o cuantitativa.

Un modelo cualitativo utiliza niveles (bajo, …, alto) y para agregar niveles se retiene el mayor nivel.

— Ver *Activos / Valoración / cualitativo*

Un modelo cuantitativo utiliza cantidades numéricas y para agregar cantidades se recurre a la suma aritmética.

— Ver *Activos / Valoración / cuantitativo*

2.9 Opciones / Fases del proyecto

Cómo se relacionan unas fases con otras.

fases del proyecto / conectadas

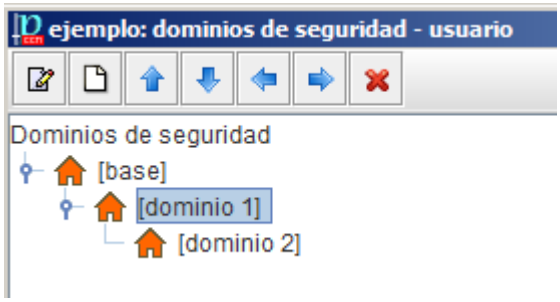
si una salvaguarda no está evaluada en una fase, hereda el valor de la fase anterior

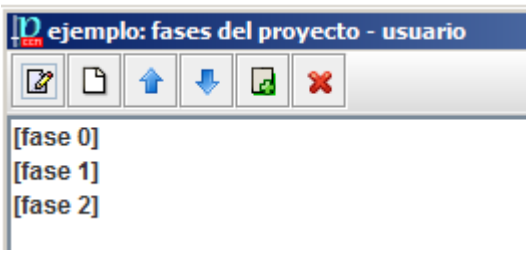
fases del proyecto / independientes

cada fase es independiente, sin heredar nada de otras fases

2.10 Opciones / Dominios de seguridad & fases del proyecto

Cuando se valoran salvaguardas, si una celda no tiene valor, PILAR intenta heredar el valor de otra celda.





primero, dominio inferior

cuando una salvaguarda no está valorada en un una fase en un dominio, PILAR intenta usar el valor del dominio inferior; si no existe, el de la fase anterior
(esta es el comportamiento de PILAR antes de la versión 4.4)

primero, fase anterior

cuando una salvaguarda no está valorada en un una fase en un dominio, PILAR intenta usar el valor de la fase anterior; si no existe, el del dominio inferior

	primero, por dominios			**primero, por fases**		
	fase 0	fase 1	fase 2	fase 0	fase 1	fase 2
dominio 2	7º	4º	**1º**	**3º**	**2º**	**1º**
dominio 1	8º	5º	**2º**	6º	5º	4º
base	9º	6º	**3º**	9º	8º	7º

Cuando un activo está sujeto a evaluación individual, se comporta como si dispusiera de su propio dominio de seguridad, individual). Es decir:

	primero, por dominios			**primero, por fases**		
	fase 0	fase 1	fase 2	fase 0	fase 1	fase 2
ACTIVO	7º	4º	**1º**	**3º**	**2º**	**1º**
dominio 1	8º	5º	**2º**	6º	5º	4º
base	9º	6º	**3º**	9º	8º	7º

2.11 Opciones / XOR

En las primeras versiones de PILAR, dentro de las salvaguardas marcadas como XOR, el usuario podía marcar varias opciones. PILAR se quedaba con la de mayor valoración, dentro de las marcadas como aplicables. A fin de marcar una de ellas como la que efectivamente mitigaba el riesgo, el usuario debía marcar las demás como n.a., o simplemente dejarlas con una valoración baja, o incluso sin valorar.

Actualmente, PILAR fuerza a que el usuario selecciones una opción y solamente una. Las demás aparecen como n.s. (no seleccionadas).

Cuando no hay riesgo en un dominio de seguridad, la selección no tiene sentido y el usuario no puede elegir. Esta característica se utiliza para establecer una evaluación de madurez general o de referencia en un dominio de base. Posteriormente, en los subdominios, se puede seleccionar una de las opciones.

2.12 Opciones / Bucles

PILAR permite establecer bucles de dependencias. Es una facilidad muy potente, pero se corre el riesgo de que desconcierte al analista si se pierde el control. El propósito de esta opción es hacer los bucles opcionales. Pero los bucles que ya existen no son opcionales, de forma que PILAR solamente puede llamar su atención.

permitir

se permiten bucles; esto es lo tradicional

advertir

los bucles se permiten, pero se le informa al usuario

no

los bucles no están permitidos; si hay bucles, PILAR los rompe

Esta opción requiere ayuda durante la carga de un proyecto que ya pudiera tener bucles. A fin de controlar el comportamiento de PILAR durante la carga, aparecen unas anotaciones en el fichero CAR:

load.loops= allow

se permiten bucles; esto es lo tradicional

load.loops= warn

los bucles se permiten, pero se le informa al usuario

load.loops= no

los bucles no están permitidos; si hay bucles, PILAR los rompe

La opción marcada en el fichero CAR solamente es válida durante la sesión en la que se carga ese CAR.

2.13 Opciones / Guardar

En modo manual, la valoración de las amenazas siempre se guarda; pero en modo automático se puede obviar, de forma que PILAR recalcule los valores cuando arranque de nuevo. A fin de seleccionar una como mecanismo de mitigación del riesgo, el usuario podría marcar las demás como n.a., o dejarlas marcadas con una baja valoración, o simplemente dejarlas sin valorar.

Actualmente, PILAR fuerza al usuario a elegir una de las salvaguardas, ignorando las demás como n.s. (no seleccionadas).

2.14 Opciones / Exportar: salvaguardas

Cuando se imprime la valoración de las diferentes fases, PILAR puede presentar el valor de cada salvaguarda en cada fase, o presentar como vacías las celdas no evaluadas explícitamente. En la interfaz gráfica, PILAR las deja vacías hasta que se valoran explícitamente. Se puede elegir en informes textuales, CSV y XML.

exportar: salvaguardas / todos los valores de madurez

imprime todos los valores, incluso si de heredan de otra fase o dominio

exportar: salvaguardas / mínimo (evitar duplicados)

solo imprime los valores explícitos

2.15 Opciones / Transferencia de valor entre dimensiones

Determina si PILAR propaga el valor de una dimensión de seguridad a otra(s). Por ejemplo, los requisitos sobre la trazabilidad del uso de un servicio, puede trasladarse a requisitos de integridad sobre los registros de actividad (logs).

El mecanismo se describe en la documentación: https://www.ar-tools.com/doc/

Transferencia de valor entre dimensiones / on

los valores se propagan entre dimensiones

Transferencia de valor entre dimensiones / off

los valores se restringen a una misma dimensión

2.16 Opciones / tiempos

En sistemas de protección física, el usuario puede realizar una estimación de cuánto tiempo lleva detectar, reaccionar y responder a un ataque. Si se tarda menos en reaccionar que lo que al atacante le lleva consumar su ataque, podemos eliminar el ataque como un riesgo.

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

2.17 Opciones / Riesgo en datos personales

Al aplicar perfiles de seguridad (EVL) para mitigar riesgos en datos personales, puede decidir si se mitiga la probabilidad (medida preventiva) o tanto la probabilidad como el impacto (medida mixta: preventiva y mitigadora).

Por defecto, solamente se mitigaba la probabilidad hasta la versión 6.2.4.

2.18 Opciones / Riesgo residual

PILAR realiza una estimación del riesgo residual teniendo en cuenta la madurez de las salvaguardas relevantes para el sistema. No existe una norma internacional que especifique cómo se realiza este cálculo.

PILAR usaba una fórmula hasta la versión 4.2.

A partir de la versión 4.3 se emplea un algoritmo mejorado.

2.19 Opciones – ROLL

Versionado de ficheros MGR.

PILAR mantiene una copia de las últimas N versiones de los ficheros mgr. O sea:

nombre.mgr	última versión – versión actual
nombre_1.mgr	penúltima
nombre_2.mgr	ante penúltima
… … …	
name_N.mgr	N-sima versión anterior (la más antigua retenida)

Cuando se guarda un fichero, con el número de versiones puesto a 3, se ejecuta la siguiente secuencia

basura ← xxx_3.mgr ← xxx_2.mgr ← xxx_1.mgr ← xxx.mgr

2.20 Opciones / ENS

Si se trabaja con el perfil ENS.

PILAR calcula los índices de madurez descritos en la guía CCN_STIC 824. El cálculo de estos índices cambió en 2016. Anteriormente se tomaban literalmente los intervalos de madurez y a partir de 2016 se consideran los pesos relativos de los componentes desglosados de cada medida de seguridad.

versión 5

trabaja con el intervalo de madurez agregado de cada medida de seguridad

versión 6

trabaja con la madurez y el peso relativo de cada elemento del desglose de cada medida de seguridad

2.21 No disponibles

Opciones eliminadas de antiguas versiones.

2.21.1 Opciones / Autenticidad

Se elimina la opción. Valoración manual.

2.21.2 Opciones / Trazabilidad

Se elimina la opción. Valoración manual.

2.21.3 Opciones / LOG (experimental)

Eliminada.

3 Informes

3.1 Por patrón

Permite generar informes en RTF a partir de un patrón escrito en RTF. Use cualquier procesador de textos para generar el patrón en formato RTF. En el proceso se combina el patrón con información proporcionada por PILAR.

El formato se describe en

https://www.ar-tools.com/doc/

3.2 Informes textuales

Textos en RTF o en HTML que se utilizarán directamente como informes, o que puede incorporar a sus propios informes.

La documentación recoge la información introducida en PILAR, y la resume en diversas presentaciones.

Los informes son útiles durante la fase de análisis para validar que los elementos del sistema están bien recogidos y cada responsable está de acuerdo con el modelo.

Los informes son útiles durante la fase de tratamiento para hacer un seguimiento de los indicadores de impacto y riesgo según se despliegan y se mejoran las salvaguardas.

Resumen de riesgos

Un informe estándar que incluye la información más relevante del análisis.

Modelo de valor (corto)

Modelo de valor (largo)

El informe recopila los activos, sus dependencias, y sus valores propios y acumulados, dimensión por dimensión.

- La versión corta presenta solamente la lista de activos, y el valor de los activos con valor propio.
- La versión larga agrega el detalle completo, activo por activo.

Zonas

El informe presenta las zonas definidas y los elementos que las conectan entre sí.

Informe de amenazas

El informe recopila los activos y las amenazas, mostrando las amenazas sobre cada activo, y los activos expuestos a cada amenaza.

Evaluación de las salvaguardas

El informe presenta la madurez de cada salvaguarda en cada fase.

Informe de insuficiencias (informe de vulnerabilidades)

Similar “al informe de evaluación de las salvaguardas”, pero se filtran las salvaguardas que no alcanzan un determinado nivel de madures. Es decir: selecciona un umbral de preocupación, y se presentan las salvaguardas por debajo del umbral.

Análisis de impacto

Presenta el impacto, acumulado y repercutido, sobre cada activo en cada fase.

Análisis de riesgos

Presenta el riesgo, acumulado y repercutido, sobre cada activo en cada fase.

Perfil de seguridad (EVL)

Se presenta la evaluación de los controles de seguridad específicos del perfil.

3.3 Gráficas

Valor / dominio de seguridad

Valoración de los dominios de seguridad

- seleccione uno o más dominios a la izquierda
  (haga clic en la raíz para seleccionar / deseleccionar todos)
- seleccione una o más dimensiones a la derecha
  (haga clic en la raíz para seleccionar / deseleccionar todos)
- clic en GRÁFICO

Valor / activo

Valoración de activos individuales

- seleccione uno o más activos a la izquierda
  (haga clic en la raíz para seleccionar / deseleccionar todos)
- seleccione una o más dimensiones a la derecha
  (haga clic en la raíz para seleccionar / deseleccionar todos)
- clic en GRÁFICO

Salvaguardas / aspecto

Presentación de la eficacia de las salvaguardas en cada grupo

- seleccione uno o más dominios a la izquierda
  (haga clic en la raíz para seleccionar / deseleccionar todos)
- seleccione una o más fases a la derecha
  (haga clic en la raíz para seleccionar / deseleccionar todos)
- clic en GRÁFICO

Salvaguardas / estrategia

Presentación de la eficacia de las salvaguardas en cada grupo

- seleccione uno o más dominios a la izquierda
  (haga clic en la raíz para seleccionar / deseleccionar todos)

- seleccione una o más fases a la derecha
  (haga clic en la raíz para seleccionar / deseleccionar todos)
- clic en GRÁFICO

Salvaguardas / tipo de protección

Presentación de la eficacia de las salvaguardas en cada grupo

- seleccione uno o más dominios a la izquierda
  (haga clic en la raíz para seleccionar / deseleccionar todos)
- seleccione una o más fases a la derecha
  (haga clic en la raíz para seleccionar / deseleccionar todos)
- clic en GRÁFICO

Impacto acumulado / activo

Muestra la evolución del impacto fase a fase, activo por activo

- seleccione uno o más activos a la izquierda
  - haga clic en la raíz para seleccionar / deseleccionar todos
  - haga clic en la cabecera de un grupo de activos para seleccionar / deseleccionar todos
  - haga clic en LIMPIAR para deseleccionarlos todos
  - haga clic en TODOS para seleccionarlos todos
  - haga clic en DOMINIOS para seleccionar los activos en un cierto dominio
- seleccione una o más fases a la derecha
  - haga clic en la raíz para seleccionar / deseleccionar todas
  - haga clic en LIMPIAR para deseleccionarlas todas
  - haga clic en TODOS para seleccionarlas todas
- haga clic en GRÁFICO para una presentación en pantalla
- haga clic en CSV para generar un fichero en formato csv

Para colapsar el árbol. Solo mostrará el primer nivel.

Para ajustar el nivel de despliegue del árbol.

Impacto acumulado / dimensión

Muestra la evolución del impacto fase a fase, activo por activo

- seleccione una o más dimensiones a la izquierda
  (haga clic en la raíz para seleccionar / deseleccionar todas)

- seleccione una o más fases a la derecha
  (haga clic en la raíz para seleccionar / deseleccionar todos)
- clic en GRÁFICO para presentación en pantalla
- clic en CSV para exportar en formato CSV

Riesgo acumulado / activo

Muestra la evolución del riesgo fase a fase, activo por activo

- seleccione uno o más activos a la izquierda
  - haga clic en la raíz para seleccionar / deseleccionar todos
  - haga clic en la cabecera de un grupo de activos para seleccionar / deseleccionar todos
  - haga clic en LIMPIAR para deseleccionarlos todos
  - haga clic en TODOS para seleccionarlos todos
  - haga clic en DOMINIOS para seleccionar los activos en un cierto dominio
- seleccione una o más fases a la derecha
  - haga clic en la raíz para seleccionar / deseleccionar todas
  - haga clic en LIMPIAR para deseleccionarlas todas
  - haga clic en TODOS para seleccionarlas todas
- haga clic en GRÁFICO para una presentación en pantalla
- haga clic en CSV para generar un fichero en formato csv

Para colapsar el árbol. Solo mostrará el primer nivel.

Para ajustar el nivel de despliegue del árbol.

Riesgo acumulado / dimensión

Muestra la evolución del riesgo, fase a fase, activo por activo.

- seleccione una o más dimensiones a la izquierda
  (haga clic en la raíz para seleccionar / deseleccionar todas)
- seleccione una o más fases a la derecha
  (haga clic en la raíz para seleccionar / deseleccionar todos)
- clic en GRÁFICO para presentación en pantalla
- clic en CSV para exportar en formato CSV

Riesgo acumulado / dimensión / fase

Muestra el riesgo que soportan os activos en una cierta fase. Se genera un TreeMap que es una representación bidimensional donde el área de cada activo es proporcional al riesgo que soporta.

- seleccione una dimensión a la izquierda
- seleccione una fase a la derecha
- clic en GRÁFICO para presentación en pantalla

Impacto repercutido

Muestra la evolución del impacto fase a fase, activo por activo

- seleccione uno o más activos a la izquierda
    - haga clic en la raíz para seleccionar / deseleccionar todos
    - haga clic en la cabecera de un grupo de activos para seleccionar / deseleccionar todos
    - haga clic en LIMPIAR para deseleccionarlos todos
    - haga clic en TODOS para seleccionarlos todos
    - haga clic en DOMINIOS para seleccionar los activos en un cierto dominio
- seleccione una o más fases a la derecha
    - haga clic en la raíz para seleccionar / deseleccionar todas
    - haga clic en LIMPIAR para deseleccionarlas todas
    - haga clic en TODOS para seleccionarlas todas
- haga clic en GRÁFICO para una presentación en pantalla
- haga clic en CSV para generar un fichero en formato csv

Para colapsar el árbol. Solo mostrará el primer nivel.

Para ajustar el nivel de despliegue del árbol.

Riesgo repercutido

Muestra la evolución del riesgo fase a fase, activo por activo

- seleccione uno o más activos a la izquierda
    - haga clic en la raíz para seleccionar / deseleccionar todos
    - haga clic en la cabecera de un grupo de activos para seleccionar / deseleccionar todos
    - haga clic en LIMPIAR para deseleccionarlos todos
    - haga clic en TODOS para seleccionarlos todos
    - haga clic en DOMINIOS para seleccionar los activos en un cierto dominio

- seleccione una o más fases a la derecha
    - haga clic en la raíz para seleccionar / deseleccionar todas
    - haga clic en LIMPIAR para deseleccionarlas todas
    - haga clic en TODOS para seleccionarlas todas
- haga clic en GRÁFICO para una presentación en pantalla
- haga clic en CSV para generar un fichero en formato csv

Para colapsar el árbol. Solo mostrará el primer nivel.

Para ajustar el nivel de despliegue del árbol.

Pareto

Se trata de un histograma vertical para ordenar la contribución de cada activo al riesgo total. Los activos se ordenan en el eje X. La gráfica muestra tanto la contribución de cada activo, como el total acumulado. Esta gráfica solo está disponible en análisis cuantitativo.

3.4 Bases de datos

La información para usar PILAR con bases de datos está disponible en

https://www.ar-tools.com/doc/

4 Perímetros

Los perímetros son patrones de expansión de árboles. Sirven para darle a un nombre a un determinado nivel de expansión en árboles de salvaguardas y perfiles de seguridad (EVL).

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
```

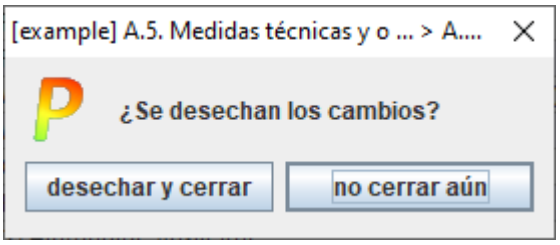
Pantallas

5 Aceptar, Cancelar, Ayuda

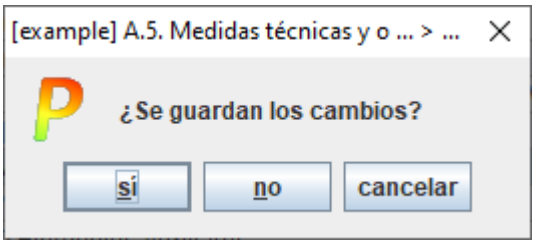
La mayoría de las pantallas incluyen los siguientes botones:

	ACEPTAR. Se guardan los cambios realizados y se cierra la ventana.
	CANCELAR. Se desestiman los cambios y se cierra la ventana.
	AYUDA. Abre un navegador con estas páginas de ayuda.

Si hay cambios y hace clic en CANCELAR, PILAR aún solicita una confirmación:



Si hay cambios e intenta cerrar la ventana, PILAR pregunta qué hacer:



donde puede elegir

CANCELAR	se mantiene la ventana, sin salir
NO	se desestiman los cambios y se cierra la ventana
SI	se guardan los cambios y se cierra la ventana

6 Panel de control

6.1 Controles básicos

Menú superior PROYECTO

Nuevo	Crea un nuevo proyecto, vacío.
Recientes	Recarga proyectos abiertos recientemente
Recargar	Recarga el proyecto
Guardar	Guarda el proyecto en su fichero o en su base de datos.
Importar (xml)	Importa datos en formato XML Ver https://www.ar-tools.com/doc/
Exportar (xml)	Exporta datos en formato XML Ver https://www.ar-tools.com/doc/
Traducción	Se puede generar una tabla de traducción para organizar los nombres de los eleentos en diferentes idiomas y, en un momento dado, cargarla para adaptarse al lenguaje. Ver manual de usuario
Guardar y cerrar	Guarda el proyecto y termina
Cancelar y cerrar	Termina sin guardar los datos

Menú superior FICHERO

Abrir	Abre un proyecto guardado en un fichero (.mgr)
Importar	Importa los datos de otros proyecto sobre este
Guarda como ...	Guarda una copia. Se puede elegir un fichero y una contraseña
subconjuntos	Genera un fichero XML en el que se recogen las dimensiones, clases de activos, amenazas y criterios de valoración que se han marcado como OFF en las pantallas de selección de cada uno de ellos. Posteriormente, puede referenciar el fichero desde el fichero de configuración (.car) y PILAR se configura excluyendo los elementos guardados. subsets = subsets.xml

Menú superior DB

Las opciones para trabajar con una base de datos se desarrollan en la documentación

https://www.ar-tools.com/doc/

Abrir	Abre un proyecto guardado en una base de datos
Importar	Importa los datos de otros proyecto sobre este
Guarda como ...	Guarda una copia. Se puede elegir la base de datos

Menú superior EDITAR

Preferencias	tipo y tamaño de letra
Opciones	Ver *Editar / Opciones*

Menú superior NIVEL

Basico	Solo se presentan las opciones básicas. Menús sencillos. Para principiantes.
Medio	Punto medio entre básico y experto
Experto	Se presentan todas las opciones

Menú superior AYUDA

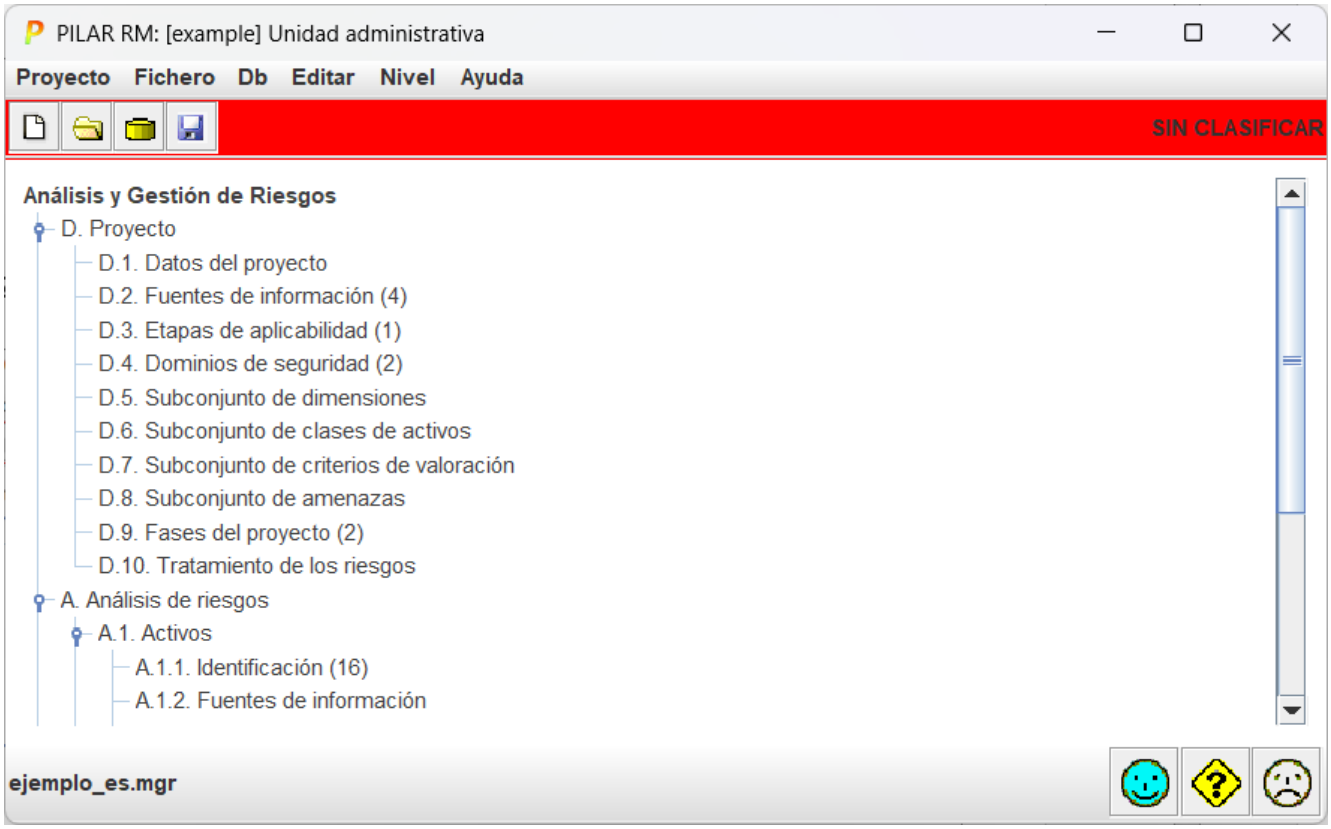
ayuda	abre un navegador con la ayuda en línea
referencias	algunas normas internacionales relativas al análisis y gestión de riesgos
acerca de PILAR	información de la versión en ejecución
¿última versión?	conecta al sitio web de PILAR y chequea si hay nuevas versiones
estado del sistema	presenta el uso de recursos del sistema

Barra superior de herramientas

	Crea un nuevo proyecto, vacío.
	Selecciona un proyecto de un fichero (.mgr)

	Selecciona un proyecto de una base de datos. Solo si la licencia incluye acceso a bases de datos SQL.
	Guarda el proyecto en su fichero o en su base de datos.

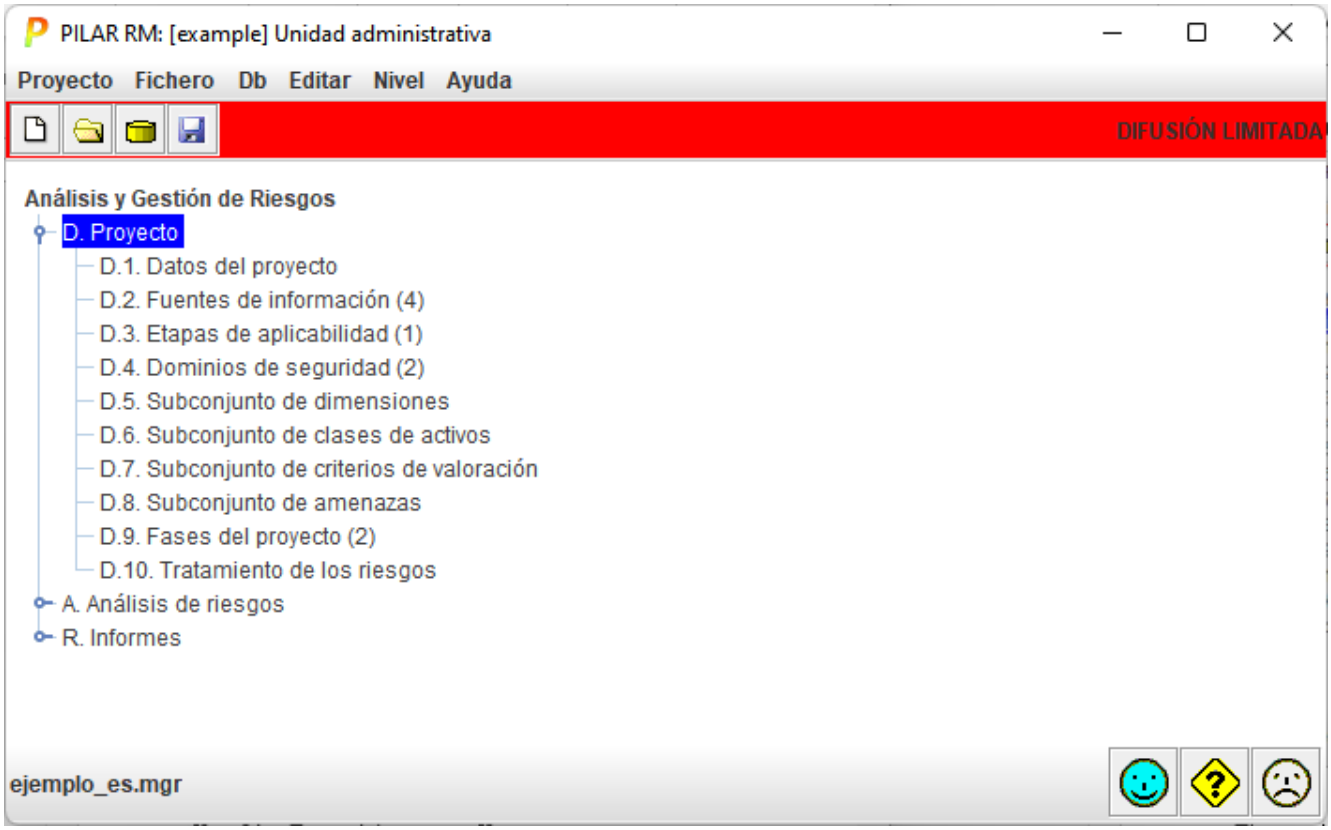
6.2 Controles del proyecto



La barra inferior presenta el nombre del fichero, o el URL de la base de datos.

El árbol en el interior presenta las actividades. Expándalo según necesite para saltar a la actividad correspondiente.

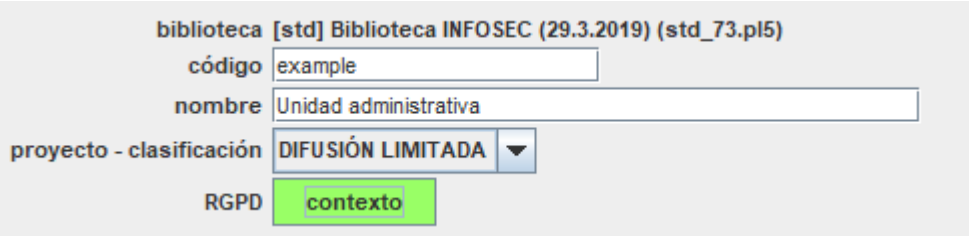
7 Proyecto



Los números entre paréntesis muestran cuántos elementos hay definidos en cada sección. En el ejemplo mostrado, hay 4 fuentes de información, 1 etapa de aplicabilidad, 2 dominios de seguridad y 2 fases de proyecto.

7.1 Datos del proyecto

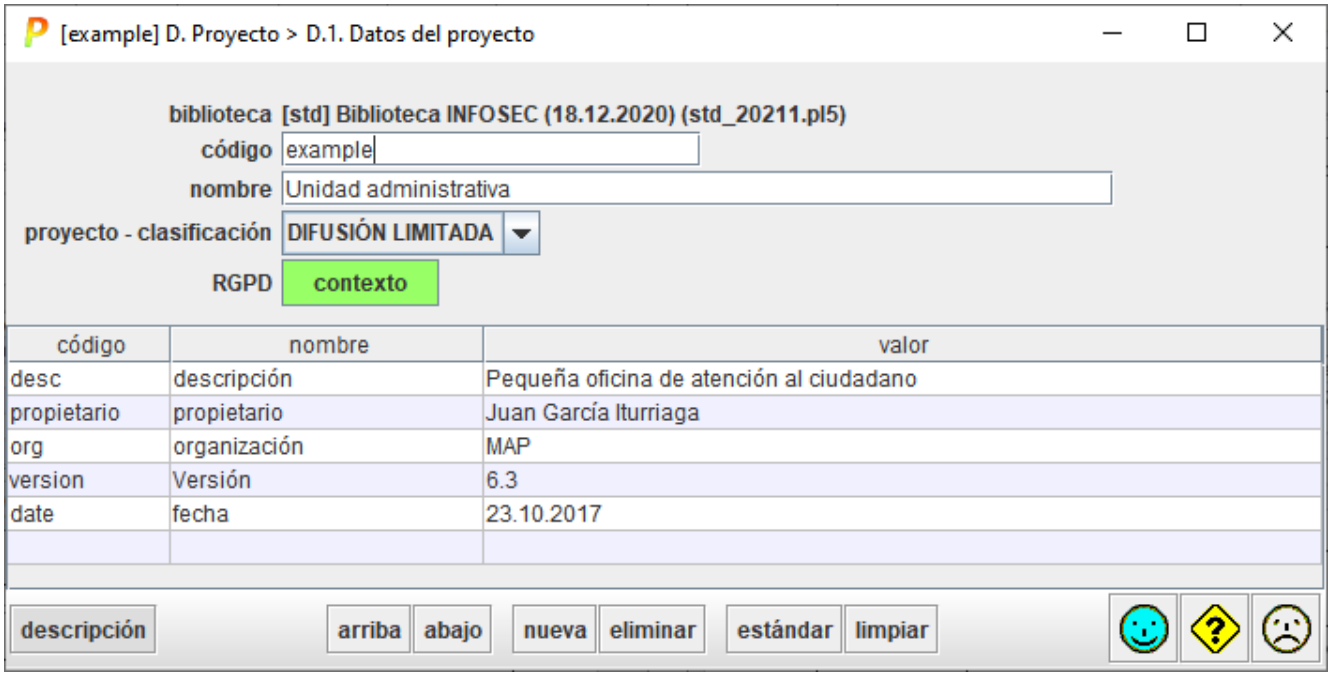
Para empezar rápidamente
Seleccione un código y un nombre descriptivo. Seleccione **OK** para continuar.



biblioteca	La biblioteca. Se selecciona al arrancar. Fichero CAR.
código	Código del proyecto. Debería ser único.
nombre	El nombre del proyecto. Una descripción sucinta.
clasificación	La marca de clasificación, por defecto, de los informes.

RGPD contexto	Puede introducir información administrativa para cumplir los requisitos del RGPD. Esta información puede aparecer aquí, de forma común para todo el sistema de información, o refinarla en activos específicos dedicados al tratamiento. Ver *rgpd_info*

Se puede añadir información administrativa: pares clave-valor.

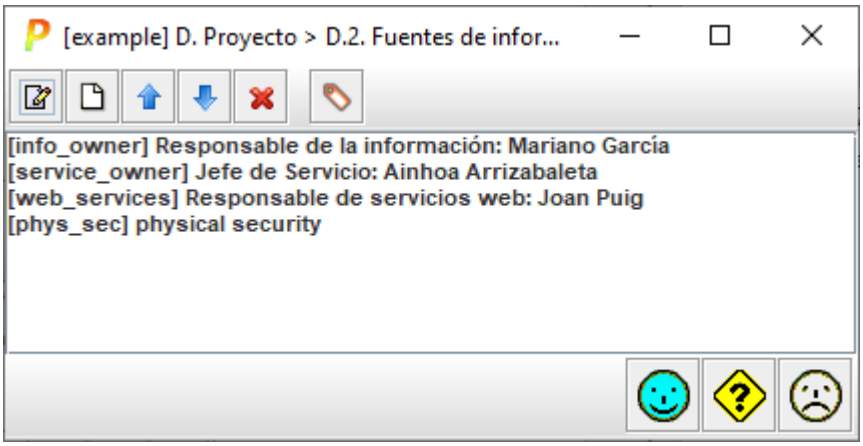


código	Claves para las parejas clave-valor. Haga clic para editar.
nombre	Nombres para las parejas clave-valor. Haga clic para editar.
valor	Valores para las parejas clave-valor. Haga clic para editar.
arriba	Seleccione un par clave-valor y haga clic para subirlo en la lista.
abajo	Seleccione un par clave-valor y haga clic para bajarlo en la lista.
nueva	Crea una nueva fila
eliminar	Elimina una fila
estándar	Añade las claves estándar. Fichero INFO.
limpiar	Elimina las filas sin valor.
descriptión	Descripción extensa del proyecto.

	La descripción puede incluir hiperenlaces (URLs). Para ir a la página enlazada, CLIC con el botón derecho, y después

7.2 Fuentes de información

Esta pantalla se utiliza para identificar y para gestionar fuentes de información.

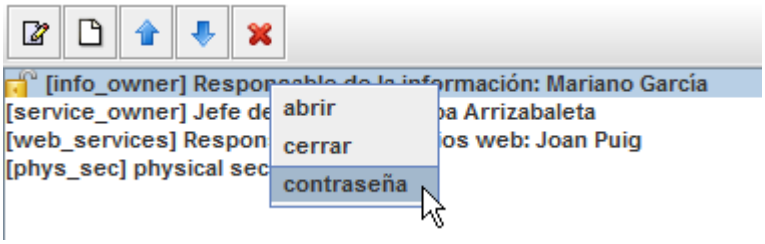


	editar: seleccione una fuente y haga clic para pasar a modo edición
	nueva: seleccione una fuente y haga clic para crear una nueva fuente
	subir: seleccione una fuente y haga clic para subirla en la lista también: MAYÚSCULAS + FLECHA_ARRIBA
	bajar: seleccione una fuente y haga clic para bajarla en la lista también: MAYÚSCULAS + FLECHA_ABAJO
	eliminar: seleccione una fuente y haga clic para eliminarla también: SUPR

	añade etiquetas estándar. Las etiquetas estándar son las que define el usuario en el fichero de configuración INFO. Los valores por defecto son:
	`<sources>`
	`  <source c="lr">restricciones legales</source>`
	`  <source c="nj">no se justifica</source>`
	`  <source c="nj.1">no vale la pena el coste</source>`
	`  <source c="nj.2">más inconvenientes que beneficios</source>`
	`  <source c="nj.3">no es práctico (no es realista)</source>`
	`</sources>`

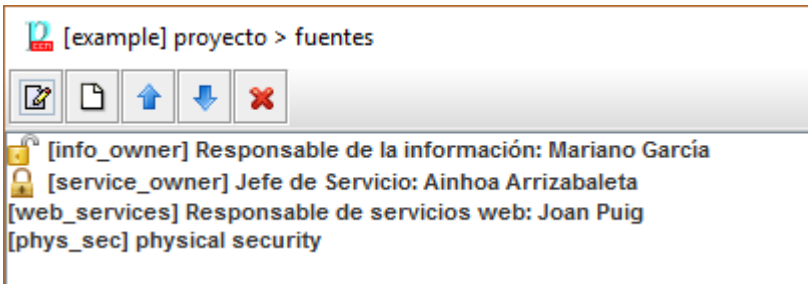
panel	panel con la lista de fuentes de información declaradas seleccione y haga clic-clic para editarla

Puede hacer clic con el botón derecho para gestionar una contraseña asociada a la fuente de información:



contraseña	establece (o elimina) una contraseña para la fuente
abrir	se solicita una contraseña para abrir una sesión con la fuente
cerrar	se cierra la sesión

Cuando una fuente tiene una contraseña asociada, podemos tener sesiones abiertas.



Una sesión abierta en una fuente permite modificar los elementos asociados a esa fuente. Una sesión cerrada deja el elemento en modo solo lectura.

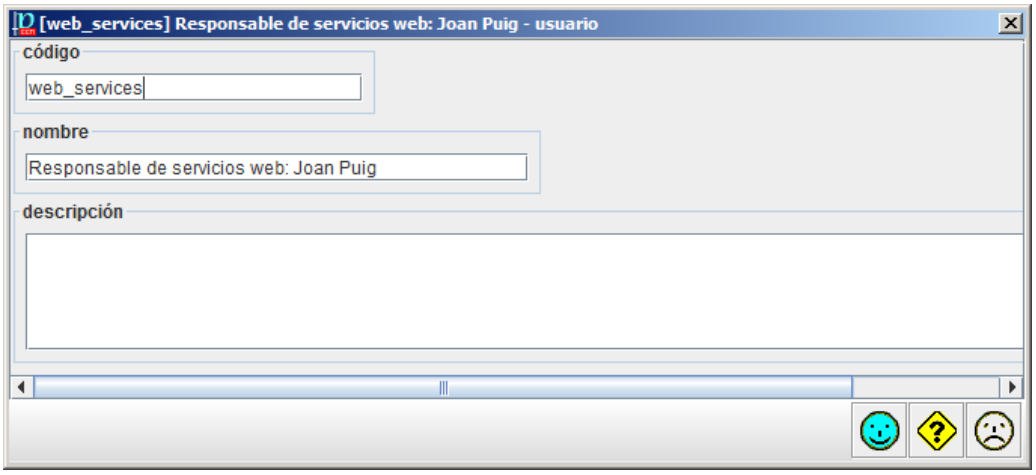
Ver manual de usuario.

7.2.1 Edición

Cuando esté editando una fuente de información, puede especificar:

- el código: debe ser único
- el nombre: una descripción sucinta
- una descripción más larga

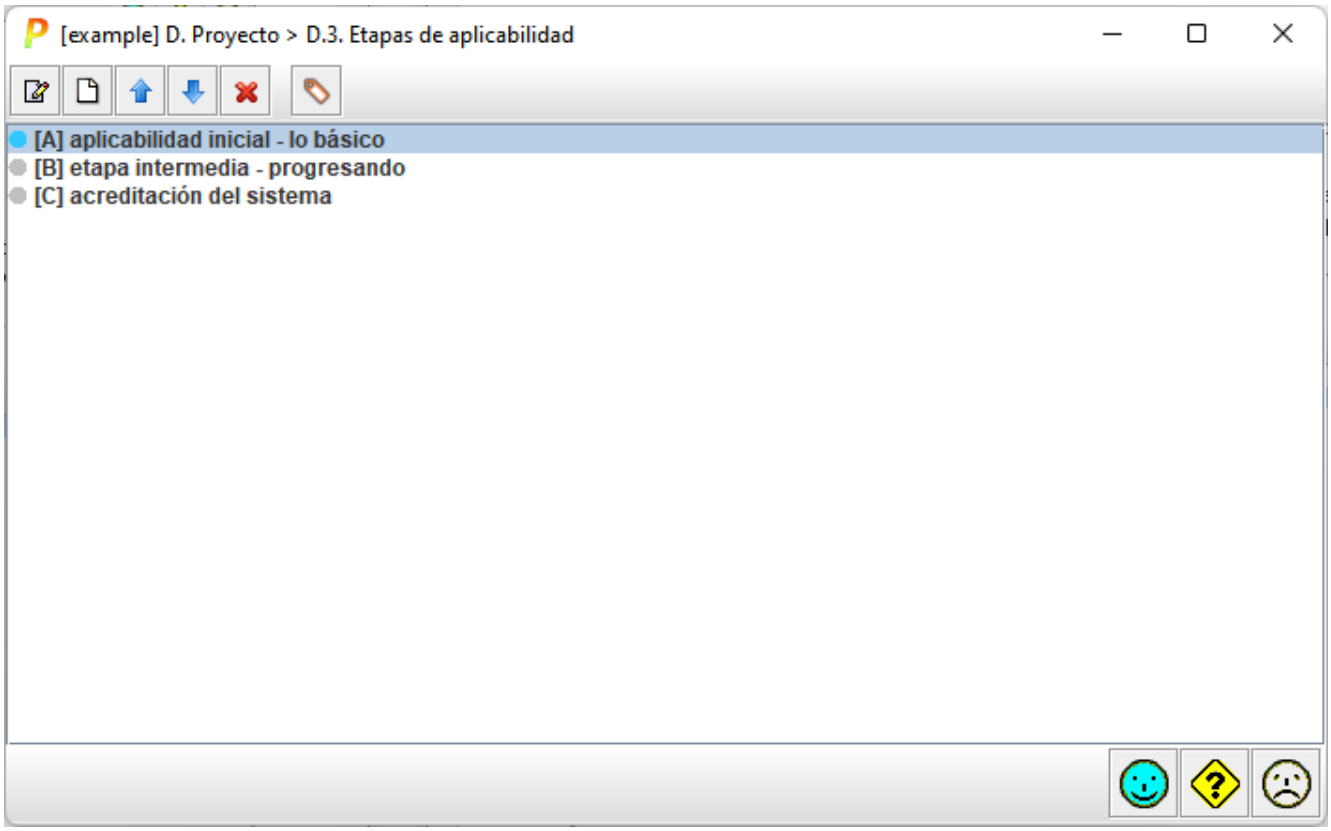
La descripción puede incluir hiperenlaces (URLs). Para ir a la página enlazada, CLIC con el botón derecho, y después 



7.3 Etapas de aplicabilidad

Puede definir varias etapas de aplicabilidad. Esto significa que en diferentes etapas se aplican diferentes salvaguardas y controles.

Esta funcionalidad es útil cuando se quiere establecer un plan gradual de implementación de medidas de seguridad. O cuando diferentes autoridades u organismos de certificación aprueban diferentes declaraciones de aplicabilidad.



La pequeña marca a la izquierda del nombre muestra qué etapa es la que se utiliza actualmente. Una marca gris para todas las etapas, y una marca azul para la etapa actual.

	seleccione una etapa y haga clic para editarla
	seleccione una etapa y haga clic para añadir una etapa nueva a continuación
	seleccione una etapa y haga click para desplazarla hacia arriba también: SHIFT + UP_ARROW
	seleccione una etapa y haga click para desplazarla hacia abajo también: SHIFT + DOWN_ARROW
	seleccione una etapa y haga click para desplazarla hacia arriba también: DELETE
	añade etapas estándar; se pueden definir en el fichero INFO de configuración

En el panel, haga doble-clic sobre una etapa para editarla.

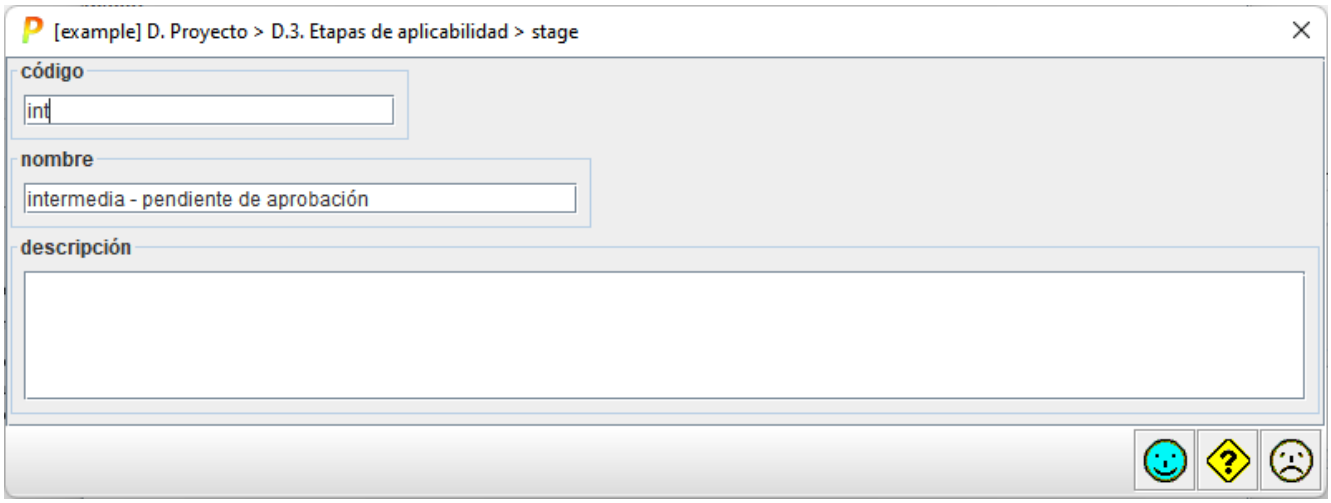
Haga clic con el botón derecho para seleccionar una etapa como la actual.

7.3.1 Edición

Cuando se edita una etapa, puede especificar:

- el código, que debe ser único
- el nombre de la etapa
- una descripción más extensa

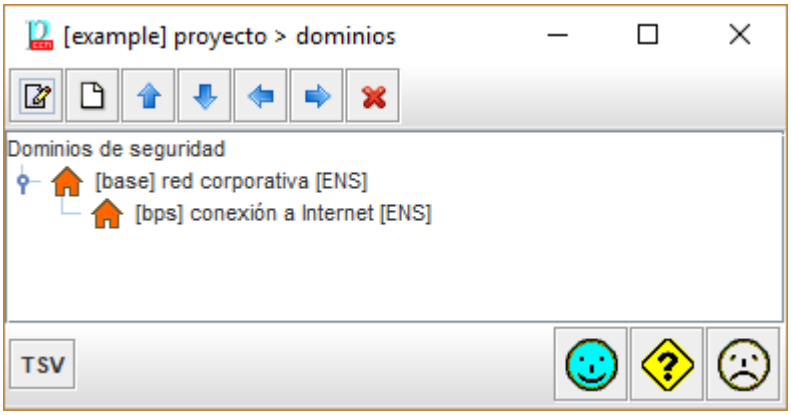
La descripción puede incluir hiperenlaces (URL). Para ir a la página referenciada, haga clic en el botón derecho y luego 



7.4 Dominios de seguridad

Puede organizar los activos en dominios de seguridad. Cada dominio tiene su propia valoración de salvaguardas. Cuando en un sistema, diferentes activos están sujetos a diferentes salvaguardas o a salvaguardas con diferente nivel, los dominios permiten agrupar los activos sometidos a una misma política.

Esta pantalla permite establecer y gestionar la jerarquía de dominios. Siempre existe un dominio BASE, que no se puede eliminar. Los activos que no están adscritos a ningún dominio específico, caen en la BASE.



Barra superior de herramientas

	seleccione un dominio y haga clic para editarlo
	seleccione un dominio y haga clic para añadir otro dominio dentro de él
	seleccione un dominio y haga clic para moverlo hacia arriba también: MAYÚSCULAS + FLECHA_ARRIBA
	seleccione un dominio y haga clic para moverlo hacia abajo también: MAYÚSCULAS + FLECHA_ABAJO
	seleccione un dominio y haga clic para moverlo a la izquierda también: MAYÚSCULAS + FLECHA_IZQUIERDA
	seleccione un dominio y haga clic para moverlo hacia la derecha también: MAYÚSCULAS + FLECHA_DERECHA
	seleccione un dominio y haga clic para eliminarlo también: DELETE

En el panel con la jerarquía de dominios

- seleccione y haga clic-clic para editar un dominio
- haga clic en la manivela para expandir o colapsar el árbol

Haga clic en el botón TSV para cargar perfiles de amenazas.

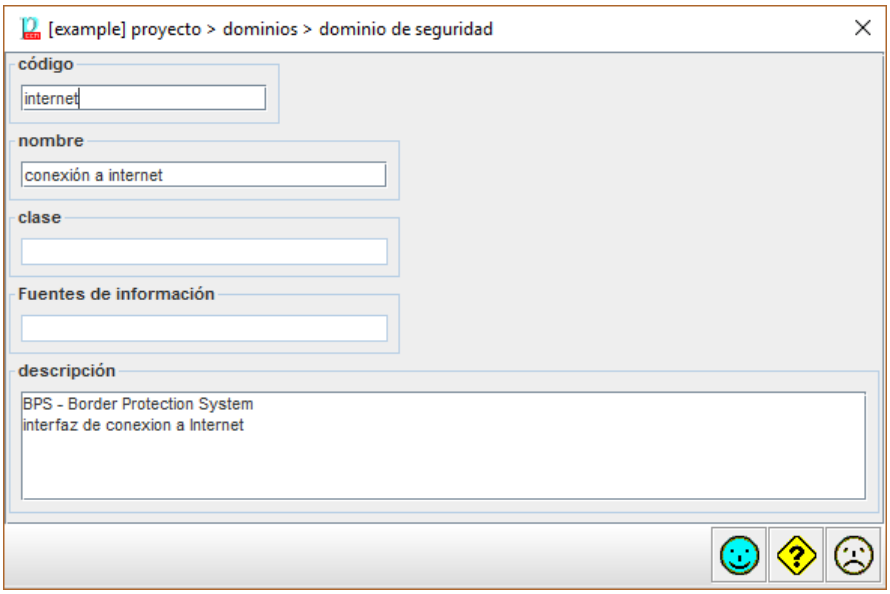
- Ver "*Threat Standard Values*

7.4.1 Edición

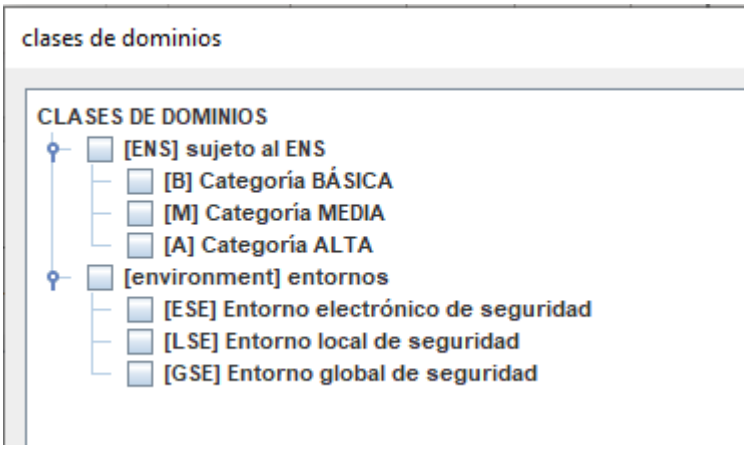
Cuando se edita un dominio de seguridad, se pueden especificar varias cosas

- el código, que debe ser único
- el nombre del dominio
- la clase del dominio; se puede marcar un dominio con una o más clases; las clases disponibles dependen de la configuración
- una o más fuentes de información
- una descripción más extensa

La descripción puede incluir hiperenlaces (URLs). Para ir a la página enlazada, haga clic con el botón derecho y después 



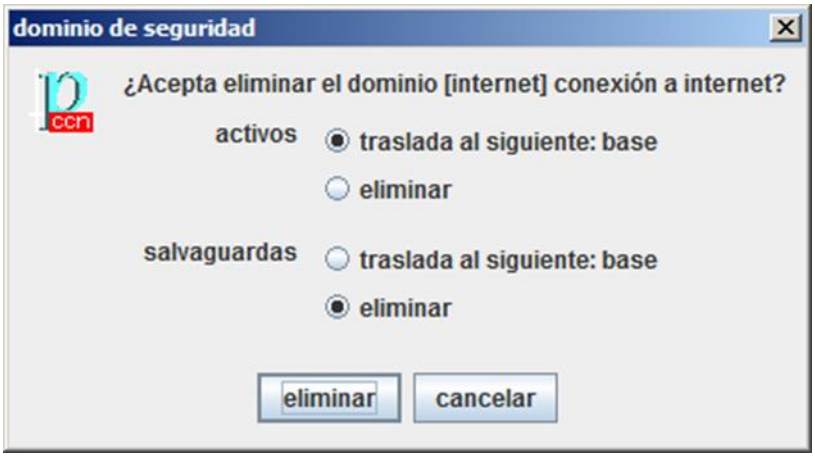
Un dominio puede marcarse como de una o más clases. El conjunto de clases disponibles es parte de la configuración de PILAR. La mayor parte de las clases carecen de semántica y sirven simplemente para seleccionar dominios de una cierta clase.



En el caso del ENS, seleccionar un dominio como ENS.B implica que PILAR no calcula la categoría del dominio en base al nivel de seguridad de sus activos esenciales, sino que lo categoriza como de categoría B directamente. Similar para ENS.M y ENS.A.

7.4.2 Eliminación

Cuando vaya a eliminar un dominio, PILAR le preguntará qué desea hacer con los datos asociados a ese dominio. Concretamente, el usuario debe indicar qué hacer con los activos en ese dominio y qué hacer con las salvaguardas evaluadas en ese dominio. Si el dominio no es subdominio de otro, hay poco que hacer: eliminar los datos. Pero si el dominio está anidado, es posible pasar la información al dominio que lo envuelve:

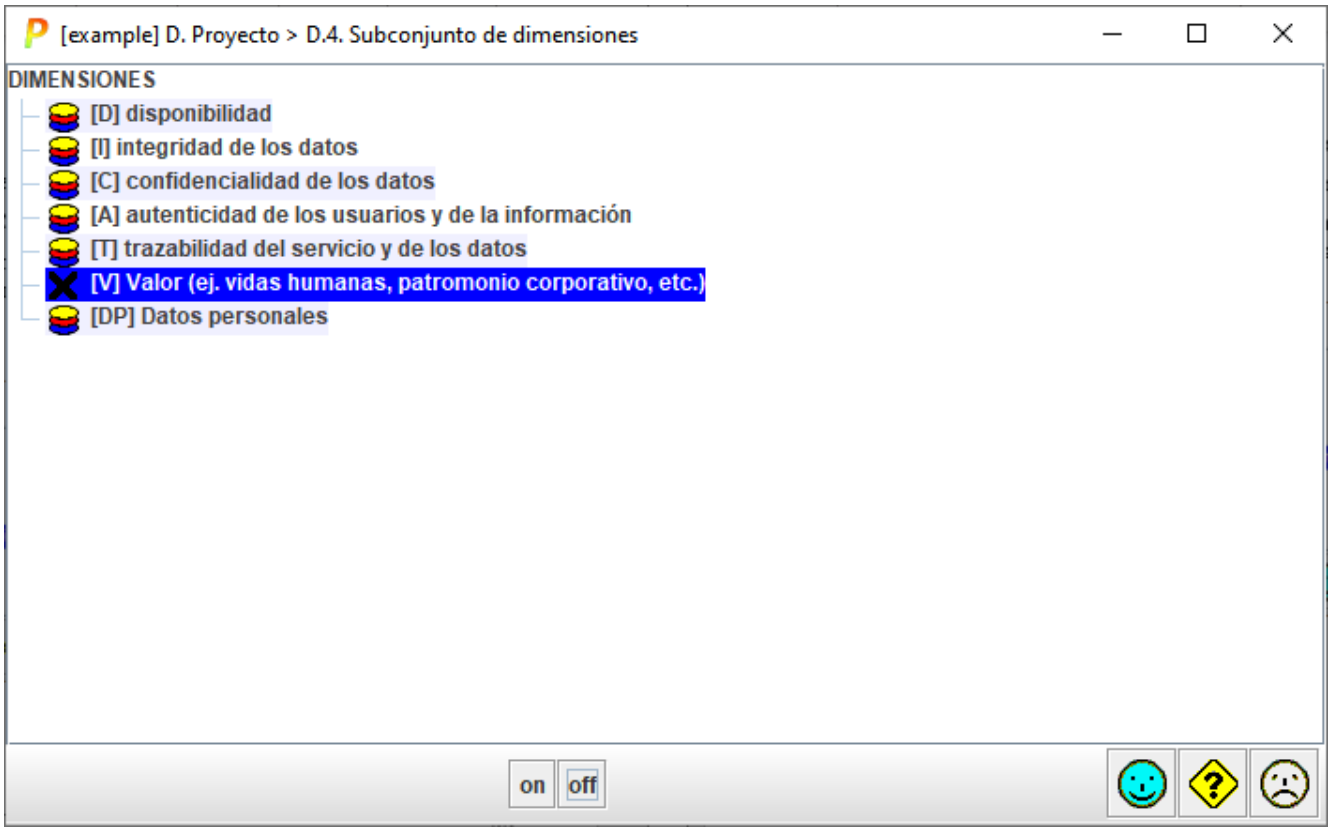


7.5 Subconjunto de dimensiones

La biblioteca estándar establece las dimensiones disponibles.

Sin embargo, se puede renunciar a algunas dimensiones. Marque on/off en la caja de selección..

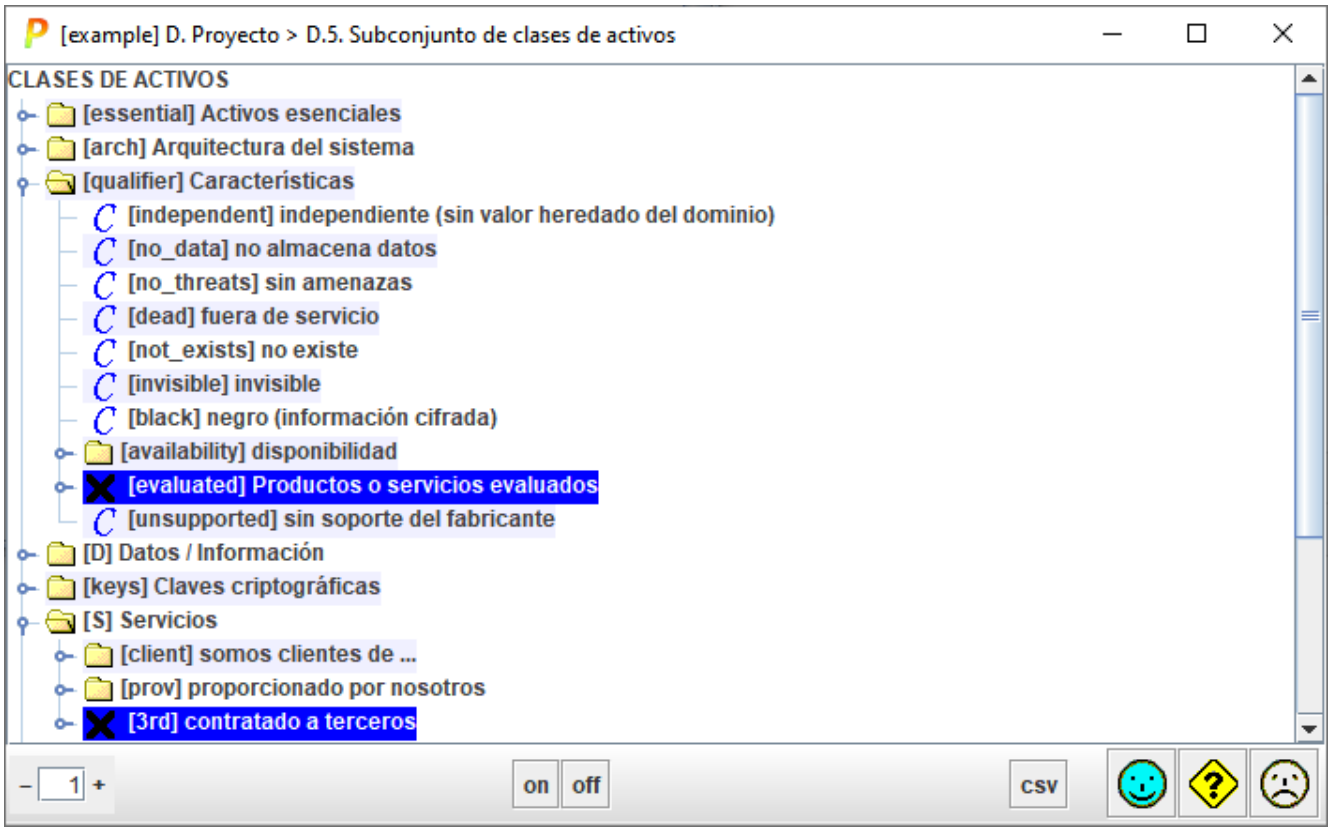
Las dimensiones no seleccionadas no se quitan del modelo. El único efecto es retirarlas de las presentaciones, así el usuario puede centrarse en el “asunto del día” eliminando información innecesaria de las pantallas.



7.6 Subconjunto de clases de activos

Las clases de activos se emplean para calificar activos. Las clases disponibles se cargan de la biblioteca. El usuario puede añadir nuevas clases por medio de los ficheros de personalización. Además, proyecto por proyecto, puede restringir la visibilidad de algunas clases para enfocarse en las que son relevantes.

Selecciones las clases que desea hacer visibles / invisibles y use para los botones ON / OFF para cambiar su estado.

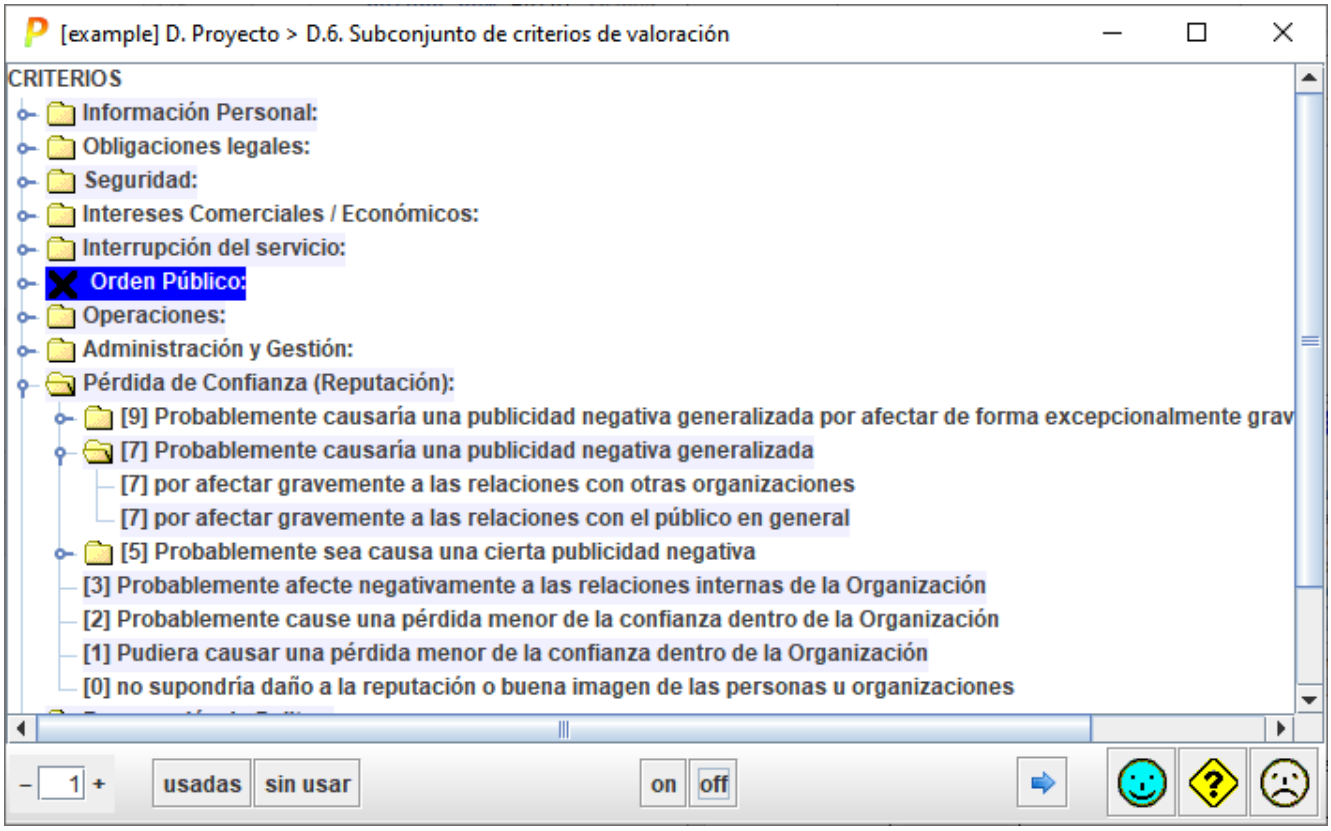


7.7 Subconjunto de criterios de valoración

La biblioteca estándar establece los criterios para asignar niveles de valoración cualitativos a los activos..

Sin embargo, se puede renunciar a algunos criterios, si no los considera apropiados para su Organización. Seleccione el criterio o grupo de criterios, y use los botones ON / OFF al pie.

Los criterios no seleccionados no se quitan del modelo. El único efecto es retirarlos de las presentaciones, eliminando información innecesaria de las pantallas.



Uso básico: seleccione uno o más criterios en el panel central y haga clic en O / OFF para seleccionarlo o deseleccionarlos.

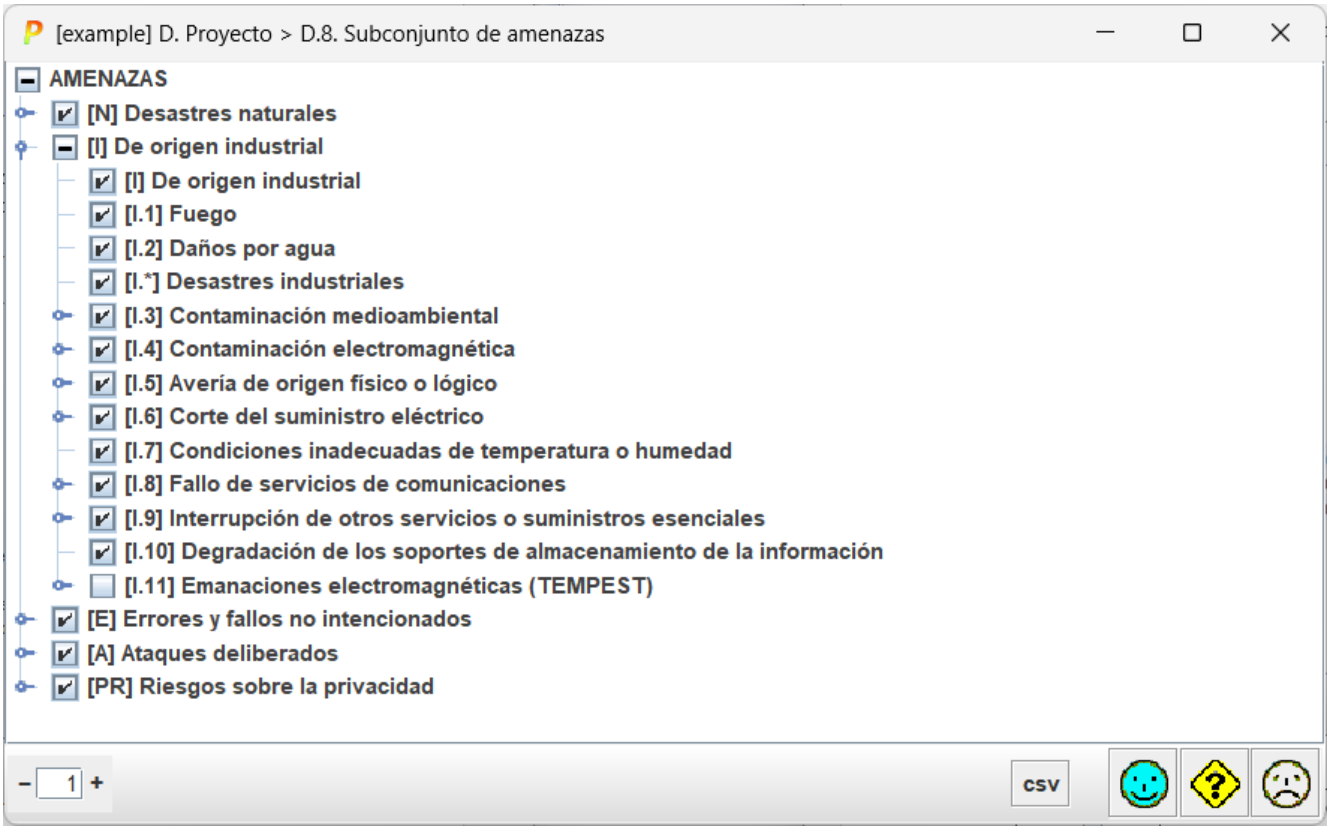
- 1 +	Seleccione el nivel de despliegue del árbol.
usadas	Selecciona aquellos criterios que se utilizan actualmente en el proyecto de análisis de riesgos.
sin usar	Selecciona aquellos criterios que no se utilizan actualmente en el proyecto de análisis de riesgos.
on	habilita los criterios seleccionados
off	inhabilita (oculta) los criterios seleccionados
csv	exporta los criterios seleccionados a un fichero CSV

7.8 Subconjunto de amenazas

La biblioteca estándar establece las amenazas disponibles.

Sin embargo, se puede renunciar a algunas amenazas. Seleccione la amenaza o el grupo de amenazas, y use los botones ON / OFF al pie.

Las amenazas no seleccionadas no se quitan del modelo. El único efecto es retirarlas de las presentaciones, así el usuario puede centrarse en el "asunto del día" eliminando información innecesaria de las pantallas.



	Haga clic para seleccionar / deseleccionar una amenaza o un grupo de amenazas.
	Para seleccionar el nivel de despliegue del árbol.
csv	exporta las amenazas a un fichero CSV

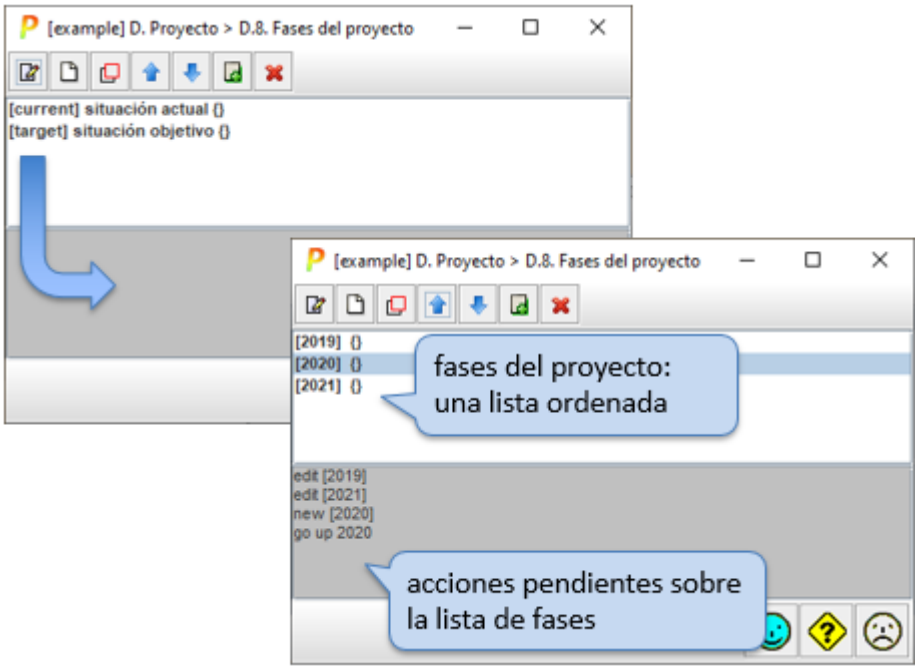
7.9 Fases del proyecto

Para empezar rápidamente
¡No haga nada! El estándar debe ser suficiente: • [current] el sistema a fecha de hoy • [target] el sistema deseable **OK** para continuar.

Identificaremos las fases del proyecto, para mostrar la evolución del riesgo. En cada fase se pueden evaluar las salvaguardas y el equipamiento de respaldo.

Hay varias formas de usar las fases:

- como diferentes etapas de un proyecto de mejora de la seguridad, para ir analizando el progreso del riesgo según se van ejecutando programas de mejora
- como histórico, por ejemplo por años, para presentar el progreso de la seguridad del sistema



	Haga clic para editar la fase seleccionada. Ver "*Editar una fase*".
	Haga clic para crear una nueva fase. Ver "*Editar una fase*".
	Haga clic para clonar la fase seleccionada. Se crea una nueva fase que hereda todos los valores asociados a la original. Luego, usted puede editarla para realizar los ajustes necesarios.
	Haga clic para mover hacia arriba la fase seleccionada (encima de la anterior). también: MAYÚSCULAS + FLECHA_ARRIBA (una o más fases)

	Haga clic para mover hacia abajo la fase seleccionada (debajo de la siguiente). también: MAYÚSCULAS + FLECHA_ABAJO (una o más fases)
	Haga clic para combinar dos fases en una. Combina la fase seleccionada con la siguiente. esto se suele hacer antes de eliminar una fase a fin de retener los valores de la fase que se elimina. Ver "[Combinación y eliminación de fases]]"
	Haga clic para eliminar la fase seleccionada

7.9.1 Combinación y eliminación de fases

Suponga que tenemos 4 fases: F1, F2, F3 y F4

y la siguiente valoración de un grupo de salvaguardas

	F1	F2	F3	F4
grupo	L1	L1-L2	L1-L3	L1-L3
S1	L1			
S2	L1	L2		
S3	L1	L2	L3	

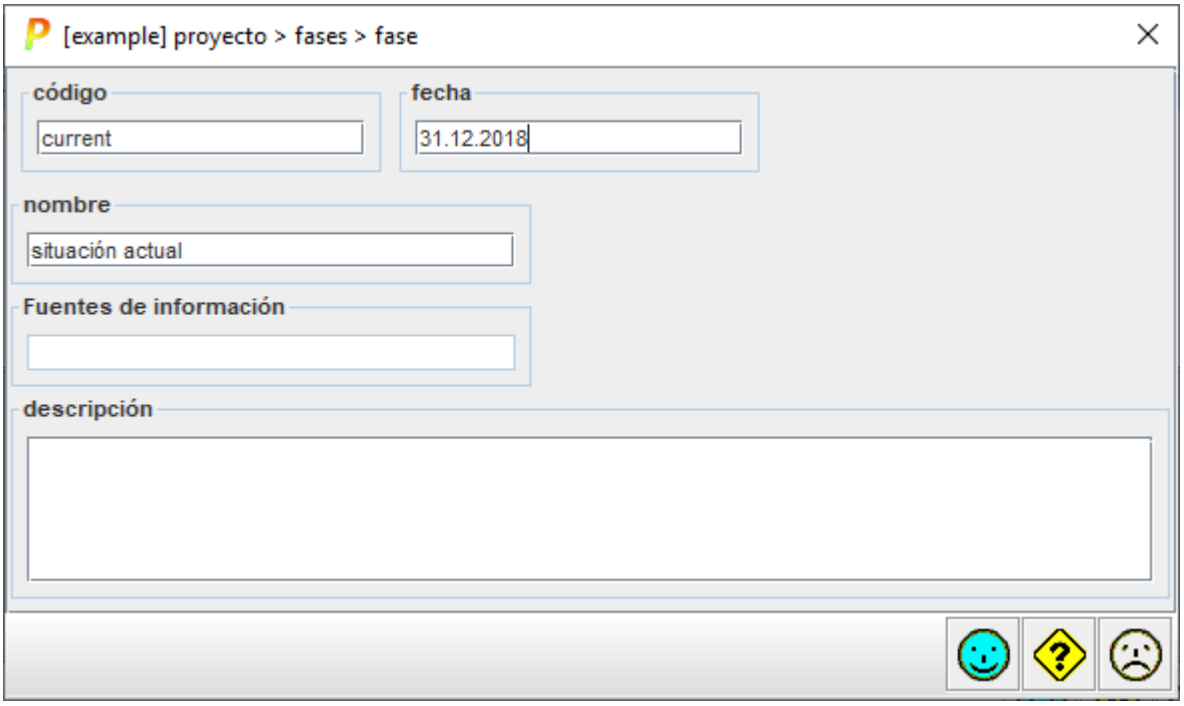
Si combinamos las fases F2 + F3, los valores de la fase F2 no modificados en la fase F3 se copian en la fase F3:

	F1	F2	F3	F4
grupo	L1	L1-L2	L1-L3	L1-L3
S1	L1			
S2	L1	L2	L2	
S3	L1	L2	L3	

De forma que ahora podemos eliminar la fase F2 sin temor a perder información:

	F1	F3	F4
grupo	L1	L1-L3	L1-L3
S1	L1		
S2	L1	L2	
S3	L1	L3	

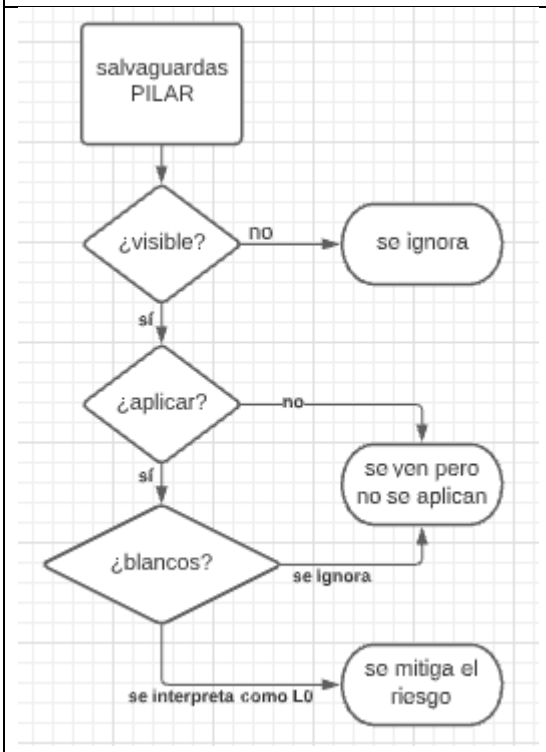
7.9.2 Editar una fase

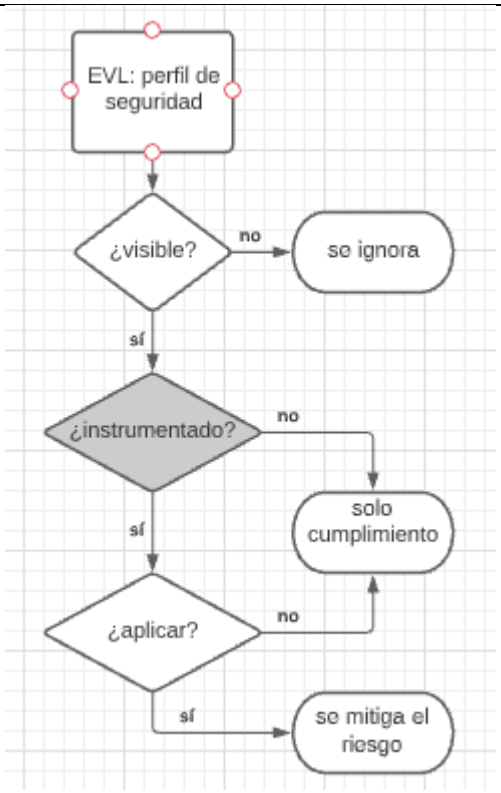


código	debe ser único
fecha	(opcional) una fecha, de forma que se asocia un concepto abstracto como es una fase del proyecto a un calendario real. El formato es día . mes . año
nombre	una descripción sucinta
fuentes	Fuentes de información asociadas a la fase. Las fuentes controlan el acceso a la valoración de la madurez de salvaguardas y controles para esa fase.
descripción	Una descripción más larga de la fase. La descripción puede incluir hiperenlaces (URLs). Para ir a la página enlazada, haga clic con el botón derecho y después

7.10 Tratamiento del riesgo

RESUMEN	
salvaguardas (PILAR and NIST)	perfiles de seguridad (EVL)

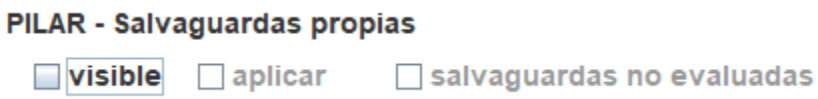




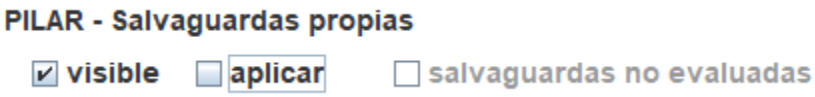
Se puede controlar cómo se usan las diferentes medidas de seguridad (salvaguardas y controles en perfiles EVL).

Para las salvaguardas de PILAR, pueden verse o no:

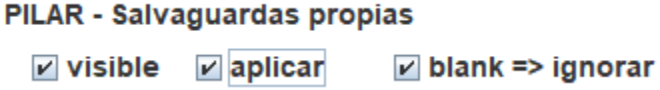
- Si no se ven, se ignoran a todos los efectos: en las pantallas y en la mitigación del riesgo

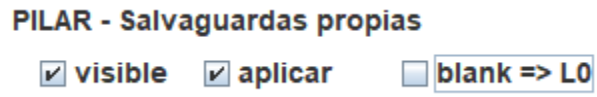


- Si se ven, se pueden aplicar para mitigar el riesgo, o no.

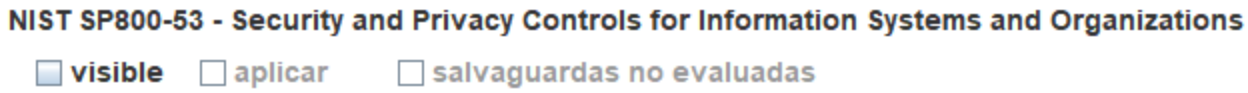


- Si se ven y se aplican, puede elegir qué hacer con las salvaguardas en blanco (sin valoración de madurez). Puede ignorarlas o interpretar que su madurez es L0



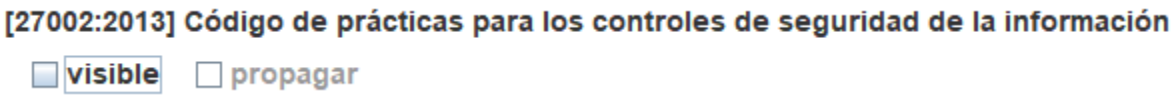


Las mismas opciones están disponibles para las salvaguardas del NIST 800-53 rev.5.

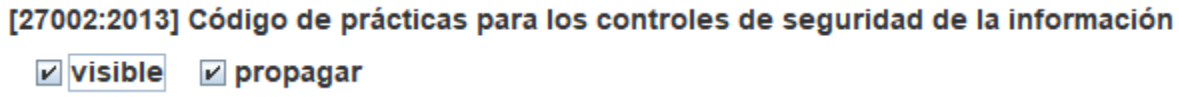


Para los perfiles de seguridad, EVL, puede decidir si son visibles o no

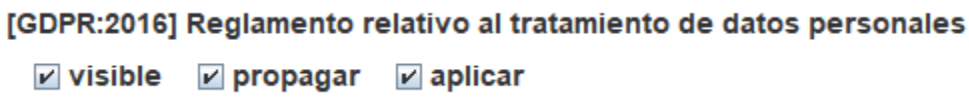
- Si no son visibles, se ignoran a todos los efectos..



- Si son visibles, puede elegir si los valores de madurez se trasladan automáticamente a las salvaguardas asociadas



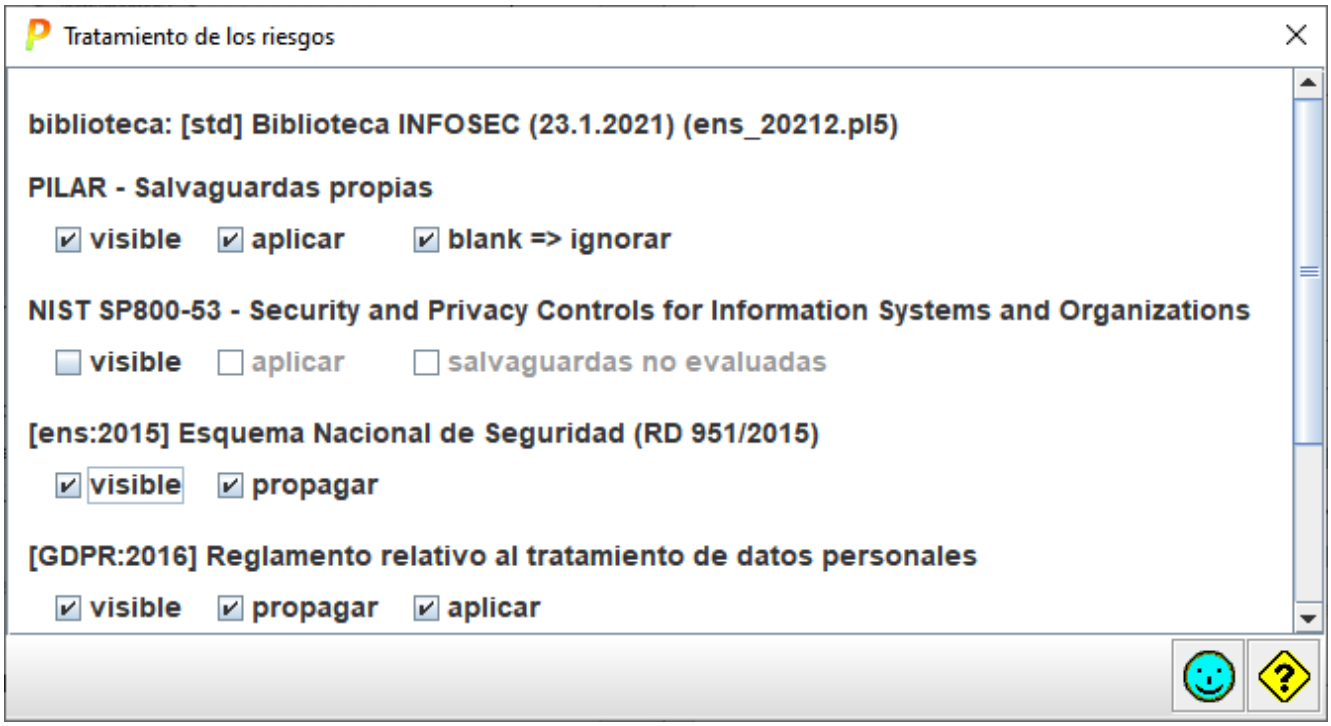
- Algunos perfiles están instrumentados para mitigar el riesgo directamente. Puede usarlos directamente para mitigar el riesgo



Muchos perfiles EVL asocian los controles a salvaguardas. Puede valorar unos y otros en paralelo.

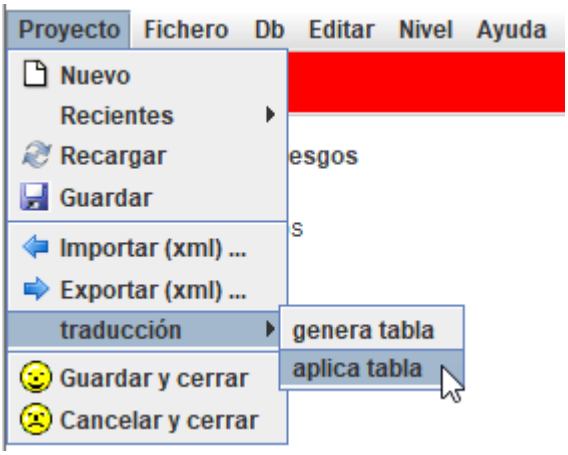
Versiones anteriores de PILAR usaban exclusivamente las salvaguardas de PILAR para mitigar el riesgo, y los perfiles EVL para cumplimiento. Puede regresar a este comportamiento seleccionando

- PILAR: visible y aplicar
- NIST 800-53: invisible
- evl*: visible + propagar



7.11 Traducción del proyecto

Puede traducir el idioma utilizado para los elementos del proyecto. PILAR puede traducir el código y el nombre del elemento.



PILAR puede generar una tabla con las reglas de traducción para el proyecto, las fuentes de información, los dominios de seguridad, las capas, los activos y las fases del proyecto.

En la aplicación, las reglas de traducción se aplican secuencialmente.

Una tabla de traducción es un fichero de texto. Cada línea es una regla de traducción.

Se usa el carácter '#' para marcar comentarios, que se ignoran.

Las reglas de traducción tienen el siguiente formato:

```
element : [src_code] src_name -> [target_code] target_name
```

'element' es uno de los siguientes: 'project', 'source', 'domain', 'layer', 'asset', o 'phase'.

El src_code se usa para seleccionar un elemento. El src_name se ignora. El código del elemento seleccionado se reemplaza por target_code, si se indica; si no, permanece inalterado. El nombre del elemento seleccionado se reemplaza por target_name, si se indica; si no, permanece inalterado.

Ejemplo

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

PILAR busca un activo de código ‘mission’. El código no cambia, pero el nombre se traduce a español.

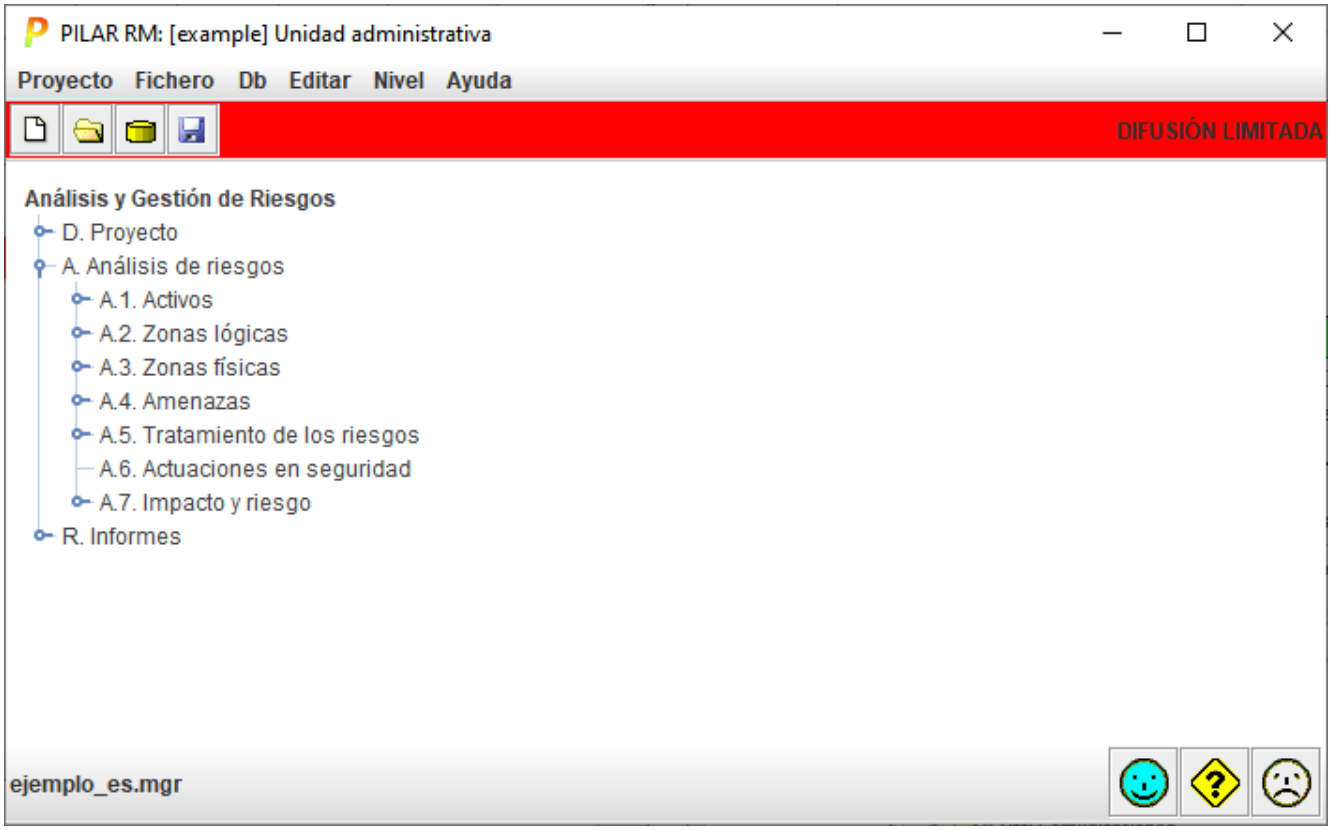
7.11.1 Formato alternativo: CSV

Como alternativa al formato textual, PILAR puede trabajar en formato CSV (Excel). Para ello, indique “.csv” como extensión del fichero de reglas.

Las reglas de traducción se disponen de la siguiente manera:

A	B	C	D	E
element	src_code	src_name	trgt_code	trgt_name
asset	mission	System mission		Misión del sistema

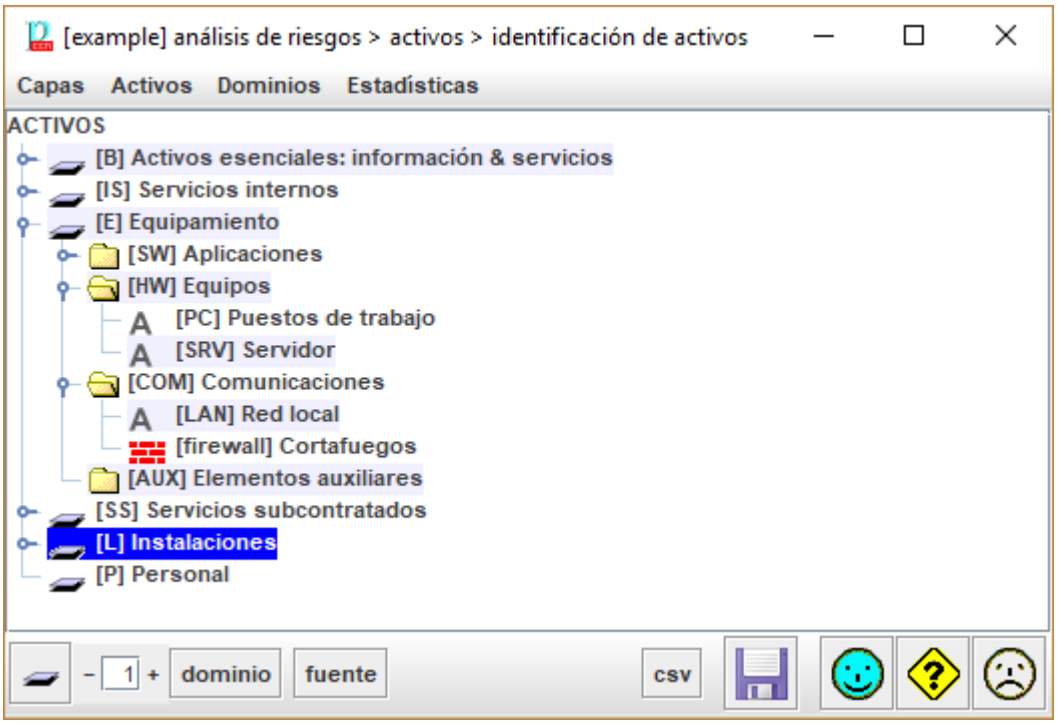
8 Análisis de riesgos



8.1 Activos / Identificación

Para empezar rápidamente
Vaya al menú de **capas** (arriba) y seleccione **ESTÁNDAR**. Seleccione una capa o un grupo y, con el botón derecho, **ACTIVO NUEVO**. **OK** para acabar la identificación del activo.

Esta pantalla se utiliza para capturar los activos y sus características singulares.



Hay varias clases de información a entrar:

capas

Los activos se organizan en capas.

Las capas no tienen ningún impacto en análisis de riesgos: es solamente una manera de organizar los activos para una mejor comprensión y comunicación.

grupos de activos

Es una manera conveniente de estructurar los activos dentro de una capa.

Puede pensar en los grupos como la organización de archivos en directorios.

Los grupos no tienen ningún impacto en el análisis de riesgos.

activos

Estos son esenciales para el análisis de riesgos: los activos de verdad.

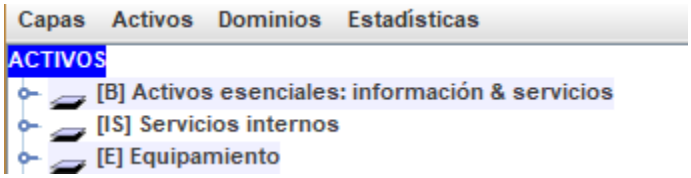
Para mover un grupo o activo

seleccione con el ratón y arrastre a la posición deseada

Para mover uno o más activos, puede seleccionarlos juntos y usar las flechas:

- MAYÚSCULAS + FLECHA ARRIBA: sube los activos a la fila anterior
- MAYÚSCULAS + FLECHA ABAJO: baja los activos a la fila siguiente
- MAYÚSCULAS + FLECHA IZQUIERDA: mueve los activos a la izquierda: hermanos de su padre actual
- MAYÚSCULAS + FLECHA DERECHA: mueve los activos a la derecha: hijos de su hermano mayor actual

Menús superiores



- *Menú capas*
- *Menú activos*
- Para editar los dominios de seguridad. Ver "*Dominios de seguridad*".
- *Menú estadísticas*

Barra inferior de herramientas

	Haga clic para colapsar el árbol al primer nivel.
	Para seleccionar el nivel de expansión del árbol.
dominio	Haga clic y seleccione un dominio. PILAR selecciona los activos en dicho dominio.
fuente	Haga clic y seleccione una fuente de información. PILAR selecciona los activos asociados a dicha fuente.
csv	Exporta los datos a un fichero CSV (comma-separated values).
	Guarda el proyecto en su fichero o en su base de datos.

8.1.1 Menú Capas

capas estándar	Incorpora las capas definidas en la biblioteca. Fichero INFO.
nueva capa	Crea una nueva capa
editar la capa	Edita la capa seleccionada
eliminar la capa	Elimina la capa seleccionada

Para incorporar las capas estándar (fichero INFO)

- capas / capas estándar

Para incorporar una nueva capa

- menú capas / nueva capa

o

- seleccionar una capa
- botón derecho / nueva capa

Para editar una capa

- menú capas / editar la capa

o

- seleccionar una capa
- botón derecho / editar la capa

Para eliminar una capa

- menú capas / eliminar la capa

o

- seleccionar una capa
- botón derecho / eliminar la capa

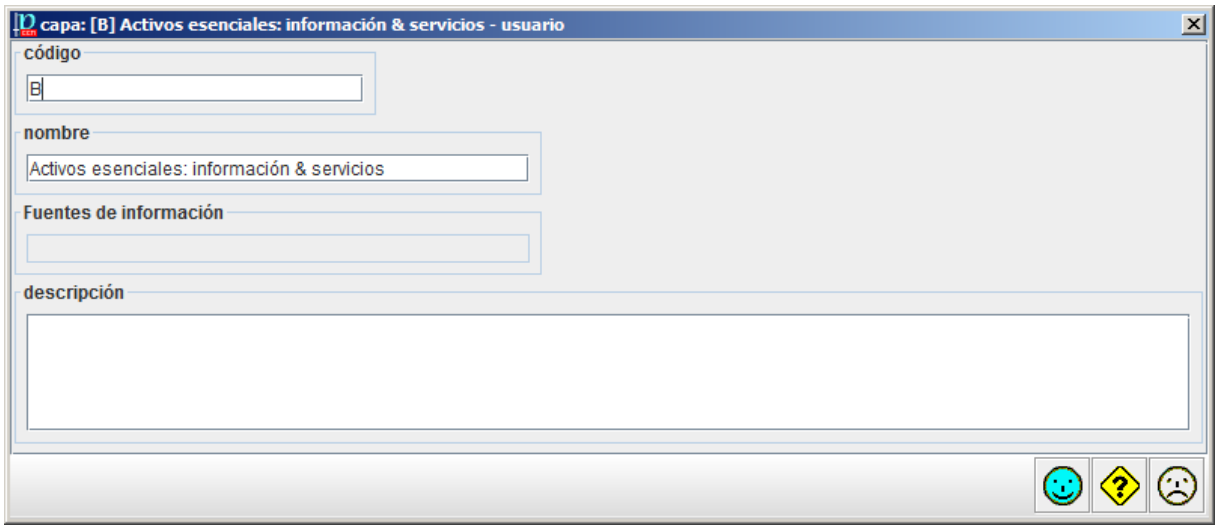
o

- seleccionar una capa
- tecla SUPRIMIR

Para cambiar una capa de orden

- arrastrar con el ratón

Por último, puede editar una capa:



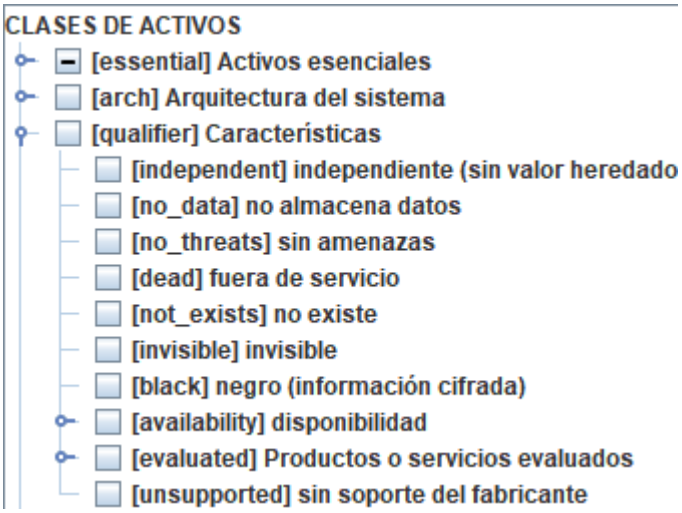
- El código debe ser único.
- El nombre es una descripción sucinta.
- Puede asociar una o más fuentes de información a la capa.

- La descripción puede ser más extensa e incluir hiperenlaces (URLs). Para ir a la página enlazada, haga clic con el botón derecho y después 

8.1.2 Menú Activos

nuevo activo / nuevo	Crea un nuevo activo. Ver "*Editar un activo*".
nuevo activo / nuevo grupo	Crea un nuevo grupo (un directorio). Ver "*Editar un activo*".
nuevo activo / duplicar	Se crea un nuevo activo, usando los datos de otro activo como punto de partida. Debe editar el nuevo activo y por lo menos cambiar el código, ya que debe ser único. Ver "*Editar un activo*".
copiar	Selecciona uno o más activos para ser duplicados en otro sitio.
cortar	Extrae uno o más activos del árbol, para que se puedan pegar en otro sitio.
pegar	Pega los activos cortados en otro sitio.
editar	Ver "*Editar un activo*".
combinar activos	Seleccione dos o más activos. Esta función los combina, arrejuntando las clases de unos y otros. Debe editar el nuevo activo y por lo menos cambiar el código, ya que debe ser único. Ver "*Editar un activo*".
descripción	Salta a la descripción larga del activo seleccionado.
dominio de seguridad	Mueve los activos seleccionados a un dominio de seguridad.
fuentes de información	Asocia una o más fuentes de información a los activos seleccionados.
ordenar / [a..z] …	Los activos seleccionados se ordenan alfabéticamente, por código.
ordenar / … [A..Z]	Los activos seleccionados se ordenan alfabéticamente, por nombre.
ordenar / retrocede	Se invierte la última ordenación, regresando al orden original.
activo / grupo / que sea grupo	Cambia los activos seleccionados, de activos normales a grupos.
activo / grupo / que no sea grupo	Cambia los activos seleccionados, de grupos a activos normales.
eliminar / los hijos	Elimina los hijos de los activos seleccionados.
eliminar / el activo	Elimina los activos seleccionados.

Versiones anteriores permitían marcar algunas características especiales. Estas características se han trasladado a las clases que califican un activo:



independent	el activo no hereda valores de los activos esenciales de su dominio
no_data	el activo no almacena datos (algunas amenazas no aplican)
no_threats	El activo puede marcarse como que está libre de amenazas, o que puede tenerlas.
dead	el activo existe pero está fuera de servicio
not_exists	Puede activar o inhibir un activo. Si no existe, se ignora a efectos del análisis de riesgos te
invisible	Puede ocultar el activo: no aparecerá en las ventanas.
black	los datos están cifrados en este activo
availability	.ajusta el impacto en caso de indisponibilidad
evaluated	el producto o servicio disfruta de una acreditación de seguridad
unsupported	el fabricante ha dejado de proporcionar parches de seguridad

Para incorporar un nuevo activo

- seleccionar una capa | un activo
- menú activos / nuevo activo / nuevo activo

o

- seleccionar una capa
- botón derecho / nuevo activo

o

- seleccionar un activo
- botón derecho / nuevo activo / nuevo activo

Para incorporar un nuevo grupo de activos

- seleccionar una capa | un activo
- menú activos / nuevo activo / nuevo grupo de activos

o

- seleccionar una capa
- botón derecho / nuevo grupo de activos

o

- seleccionar un activo
- botón derecho / nuevo activo / nuevo grupo de activos

Para incorporar un activo que es duplicado de otro

- seleccionar un activo
- menú activos / nuevo activo / duplicar el activo

o

- seleccionar un activo
- botón derecho / nuevo activo / duplicar el activo

Para editar un activo

- seleccionar un activo
- menú activos / editar

o

- seleccionar un activo
- botón derecho / editar

Para añadir una descripción larga a un activo

- seleccionar un activo
- menú activos / descripción

o

- seleccionar un activo
- botón derecho / descripción

o editar el activo

Para establecer a qué dominio de seguridad pertenece un activo

- seleccionar un activo
- menú activos / dominio de seguridad / seleccionar / OK

o

- seleccionar un activo
- botón derecho / dominio de seguridad / seleccionar / OK

o editar el activo

Para asociar fuentes de información a un activo

- seleccionar un activo
- menú activos / fuentes de información / seleccionar / OK

o

- seleccionar un activo
- botón derecho / fuentes de información / seleccionar / OK

o editar el activo

Para convertir un activo normal en grupo

- seleccionar un activo
- menú activos / activo-grupo / que sea grupo

o

- seleccionar un activo
- botón derecho / activo-grupo / que sea grupo

Para convertir un grupo de activos en un activo normal

- seleccionar un activo
- menú activos / activo-grupo / que no sea grupo

o

- seleccionar un activo
- botón derecho / activo-grupo / que no sea grupo

Para eliminar un activo (y los miembros del grupo si los hubiera)

- seleccionar un activo
- menú activos / eliminar / eliminar el activo

o

- seleccionar un activo
- botón derecho / eliminar / eliminar el activo

o

- seleccionar un activo
- tecla SUPRIMIR

Para eliminar los miembros de un grupo de activos

- seleccionar un activo
- menú activos / eliminar / eliminar los hijos

o

- seleccionar un activo
- botón derecho / eliminar / eliminar los hijos

Para cambiar una activo de orden, de grupo o de capa

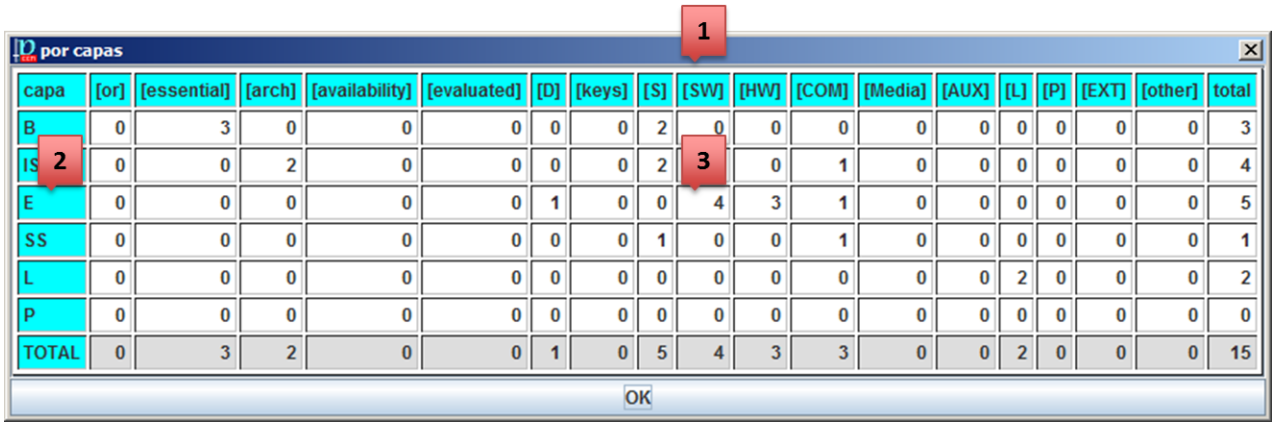
- arrastrar con el ratón
- cortar y pegar

o

- MAYÚSCULAS + FLECHA ARRIBA:
  sube los activos a la fila anterior
- MAYÚSCULAS + FLECHA ABAJO:
  baja los activos a la fila siguiente
- MAYÚSCULAS + FLECHA IZQUIERDA:
  mueve los activos a la izquierda: hermanos de su padre actual
- MAYÚSCULAS + FLECHA DERECHA:
  mueve los activos a la derecha: hijos de su hermano mayor actual

8.1.3 Menú Estadísticas

Agrupados por capas, dominios de seguridad o fuentes de información, informa de cuántos activos hay en cada clase de activos.



capa	[or]	[essential]	[arch]	[availability]	[evaluated]	[D]	[keys]	[S]	[SW]	[HW]	[COM]	[Media]	[AUX]	[L]	[P]	[EXT]	[other]	total
B	0	3	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	3
IS	0	0	2	0	0	0	0	2	0	1	0	0	0	0	0	0	0	4
E	0	0	0	0	0	1	0	0	4	3	1	0	0	0	0	0	0	5
SS	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1
L	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	2
P	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TOTAL	0	3	2	0	0	1	0	5	4	3	3	0	0	2	0	0	0	15

Cada columna cubre una de las clases de activos. Por ejemplo, [1] cubre la clase [SW]. En la columna [1] hay 3 [3] activos con clases bajo [SW], todos ellos en la capa E [2].

Tenga en cuenta que un mismo activo puede estar calificado con varias clases, de forma que los totales de la tabla a veces no son la suma de las otras celdas.

La tabla estadística se puede imprimir haciendo clic en el botón derecho.

8.1.4 Operaciones sobre un activo

En el árbol:

— clic-clic abre el activo para edición. Ver "*Editar un activo*".
— clic con el botón derecho, abre un menú con operaciones similares a las que se presentan en la barra superior de herramientas, solo que ahora se aplican sobre el activo bajo el ratón.

Para mover un activo de un sitio a otro

— marcar y dejar caer (drag & drop)

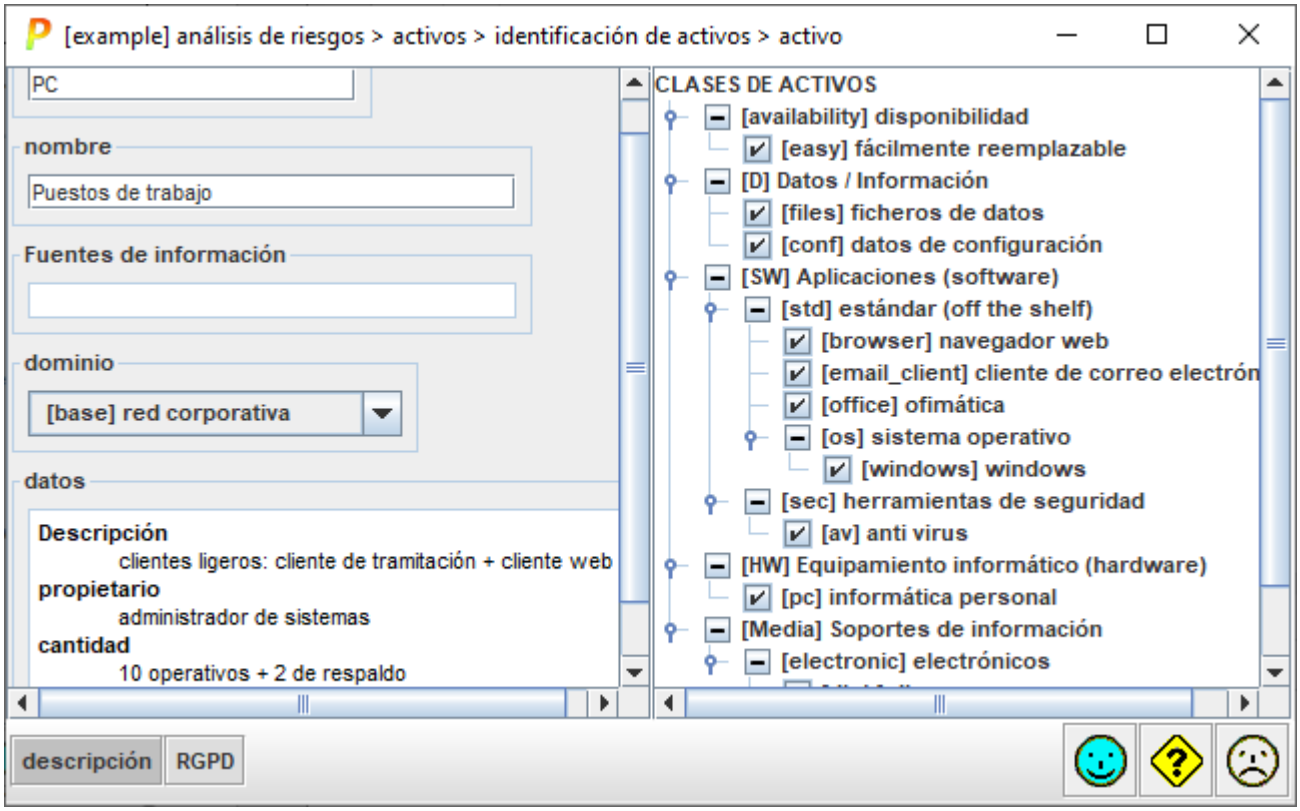
o puede usar las flechas para mover los activos seleccionados

- MAYÚSCULAS + FLECHA_ARRIBA: mueve hacia arriba; antes que el activo previo
- MAYÚSCULAS + FLECHA_ABAJO: mueve hacia abajo; después que el activo siguiente

- MAYÚSCULAS + FLECHA_IZQUIERDA: mueve a la izquierda (pasa a ser hermano de su padre)
- MAYÚSCULAS + FLECHA_DERECHA: mueve a la derecha (pasa a ser hijo de su hermano mayor

8.2 Activos / Editar un activo

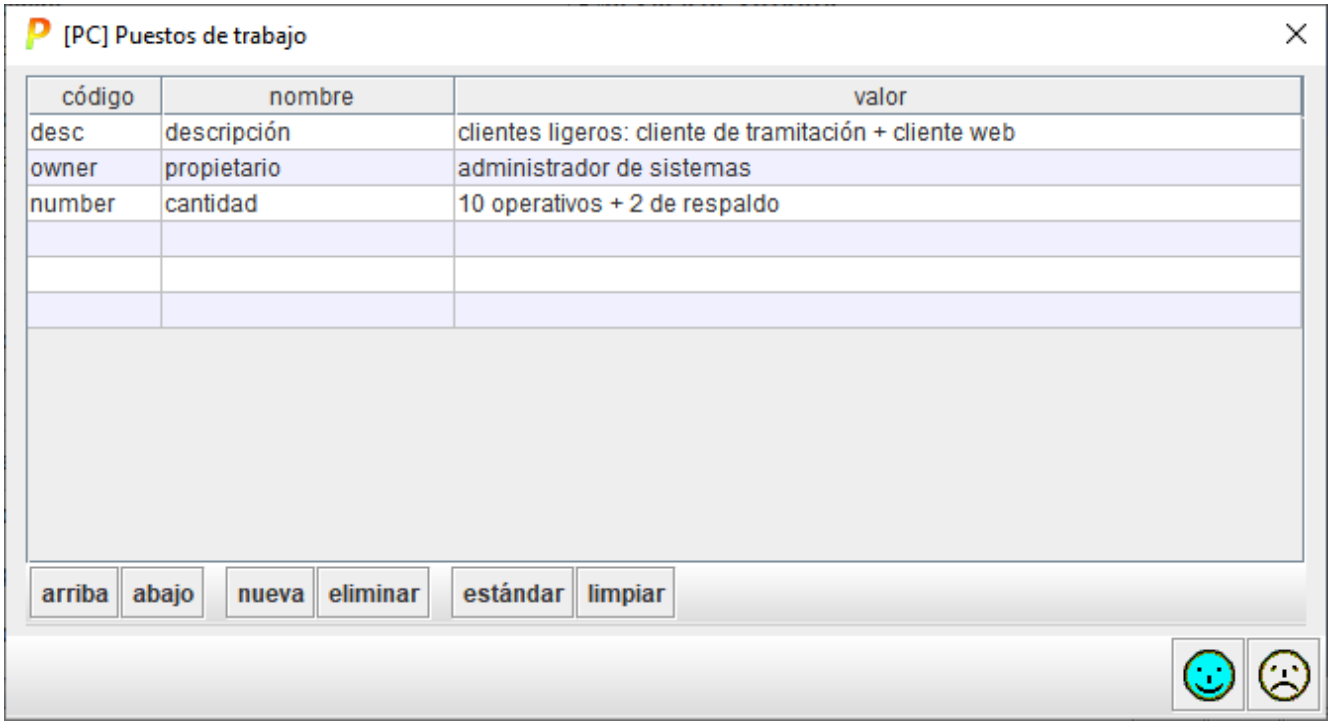
Para empezar rápidamente
Seleccione un **código único** y un nombre descriptivo. Marque una o más clases en el panel derecho. **ESTÁNDAR** y agregue una cierta información descriptiva. **OK** para continuar.



código	que debe ser único
nombre	Una descripción sucinta: en una línea
fuentes	Haga clic para asociar un activo a una o más fuentes de información.
dominio	Selecciona el dominio de seguridad al que pertenece el activo.
descripción	Una descripción más extensa. La descripción puede contener hiperenlaces (URLs). Para ir a la página enlazada, haga clic con el botón derecho y después

Datos: Pares código-valor

Pares clave-valor para describir el activo. Solo es a efectos informativos.
Haga clic-clic para editarlos



- Haga clic en el código para editarlo. Útil para traducciones.
- Haga clic en el dato para editarlo.
- Haga clic en el valor para editarlo.

Operaciones sobre los pares clave-valor:

- arriba – mueve la fila hacia arriba
- abajo – mueve la fila hacia abajo
- nueva – nueva fila
- eliminar – elimina la fila
- estándar – añade las finas estándar que falten teniendo en cuanta las clases marcadas. Fichero INFO.
- limpiar – elimina las líneas sin valor

8.2.1 Clases de activos

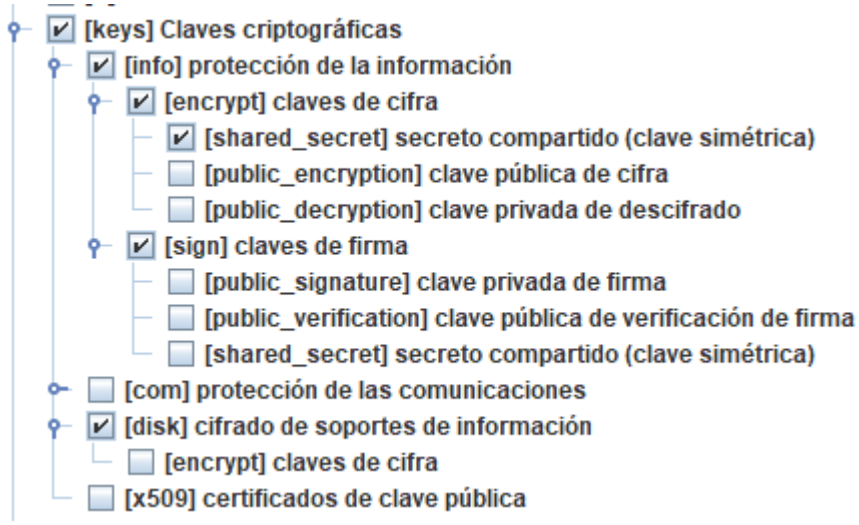
Un activo puede ser calificado con cero o más clases. Las clases se usan para sugerir amenazas y salvaguardas.

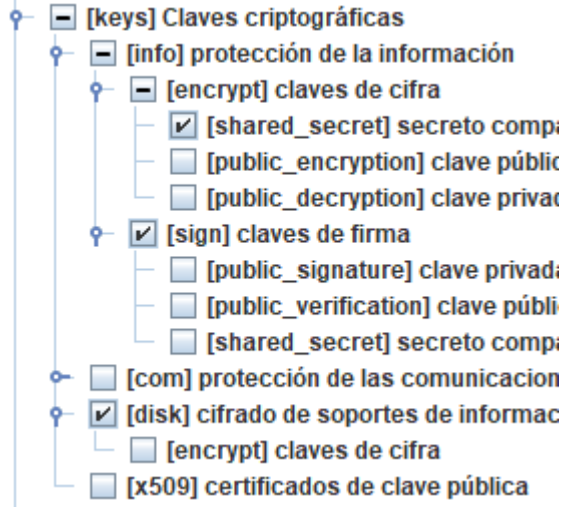
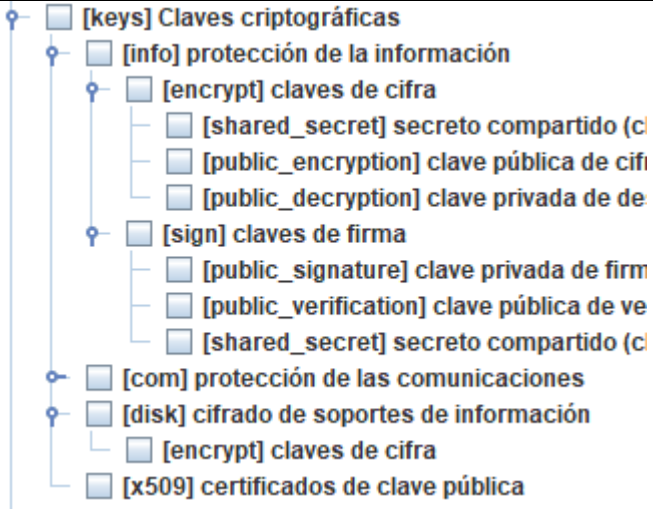
☐ significa que esa clase no está asociada al activo
☑ significa que esa clase sí está asociada al activo
▪ significa que alguna subclase de ésta está asociada al activo

Clases: limpiar / borrar

En el árbol derecho puede hacer clic con el botón derecho para limpiar o eliminar clases. Limpiar significa eliminar las marcas redundantes. Eliminar significa retirar las marcas.

Ejemplo



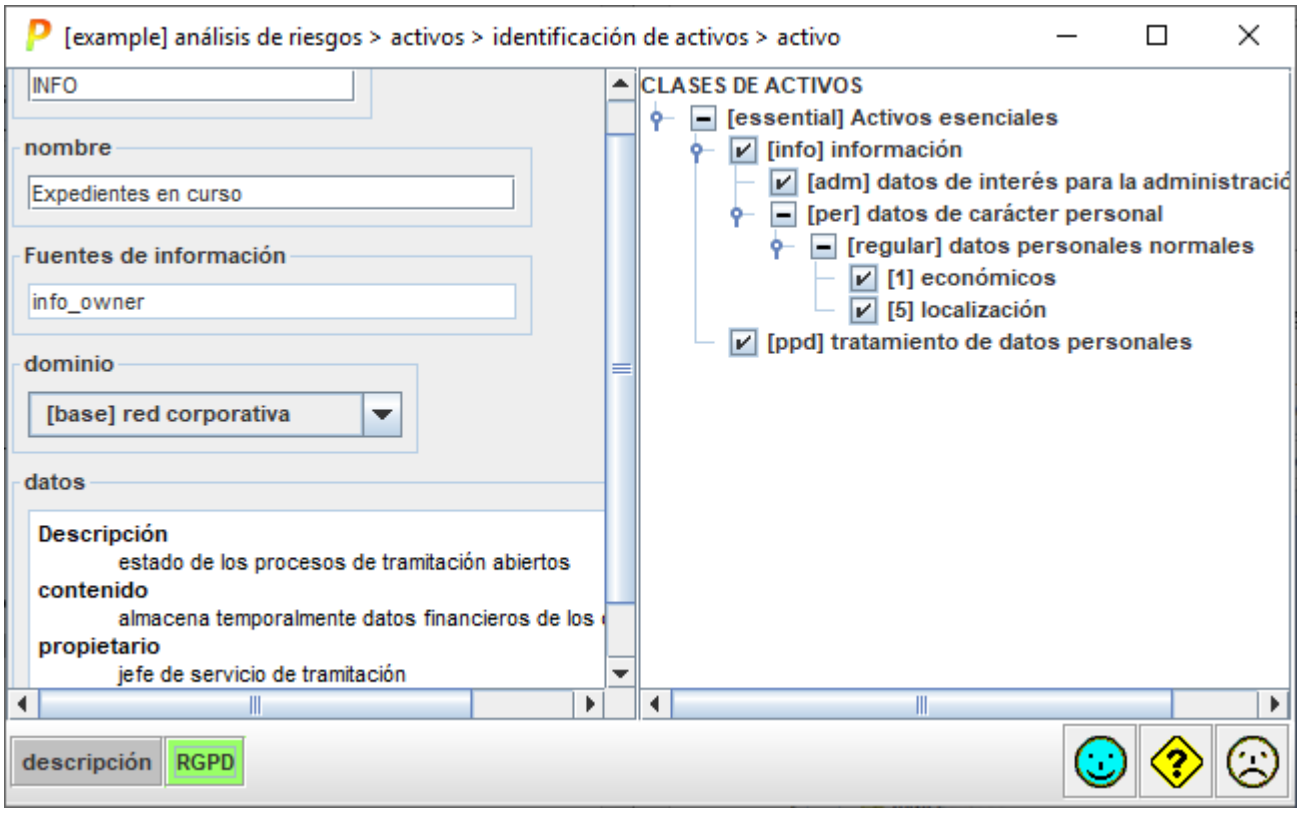
clic derecho + LIMPIAR	clic derecho + ELIMINAR
	

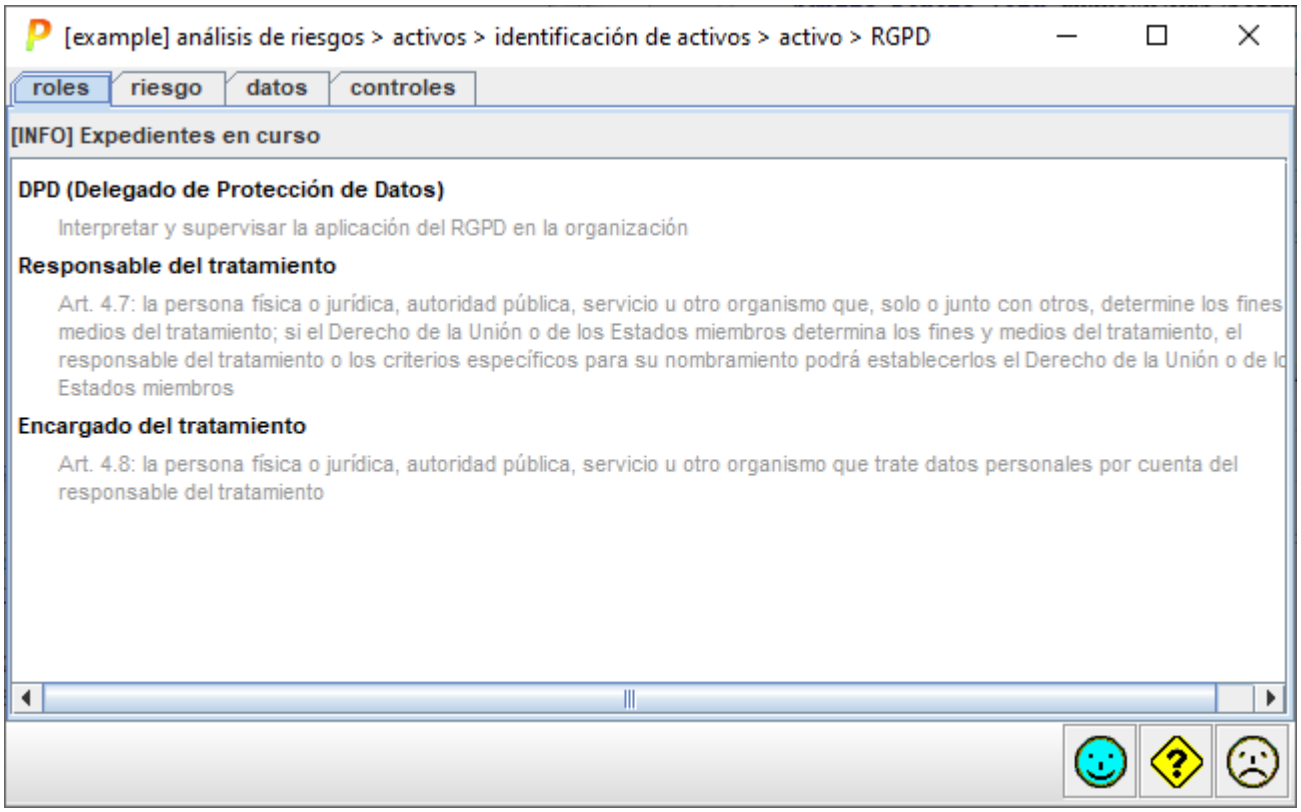
8.2.2 RGPD: privacidad

Para activos que manejan datos de carácter personal, puede especificar información administrativa a fin de cumplir lo requerido en el Reglamento.

Esta información se puede proporcionar de forma general para todo el sistema de información (ver *Datos del proyecto*) O de forma específica para un cierto activo.

La información debe ser auto-explicativa:

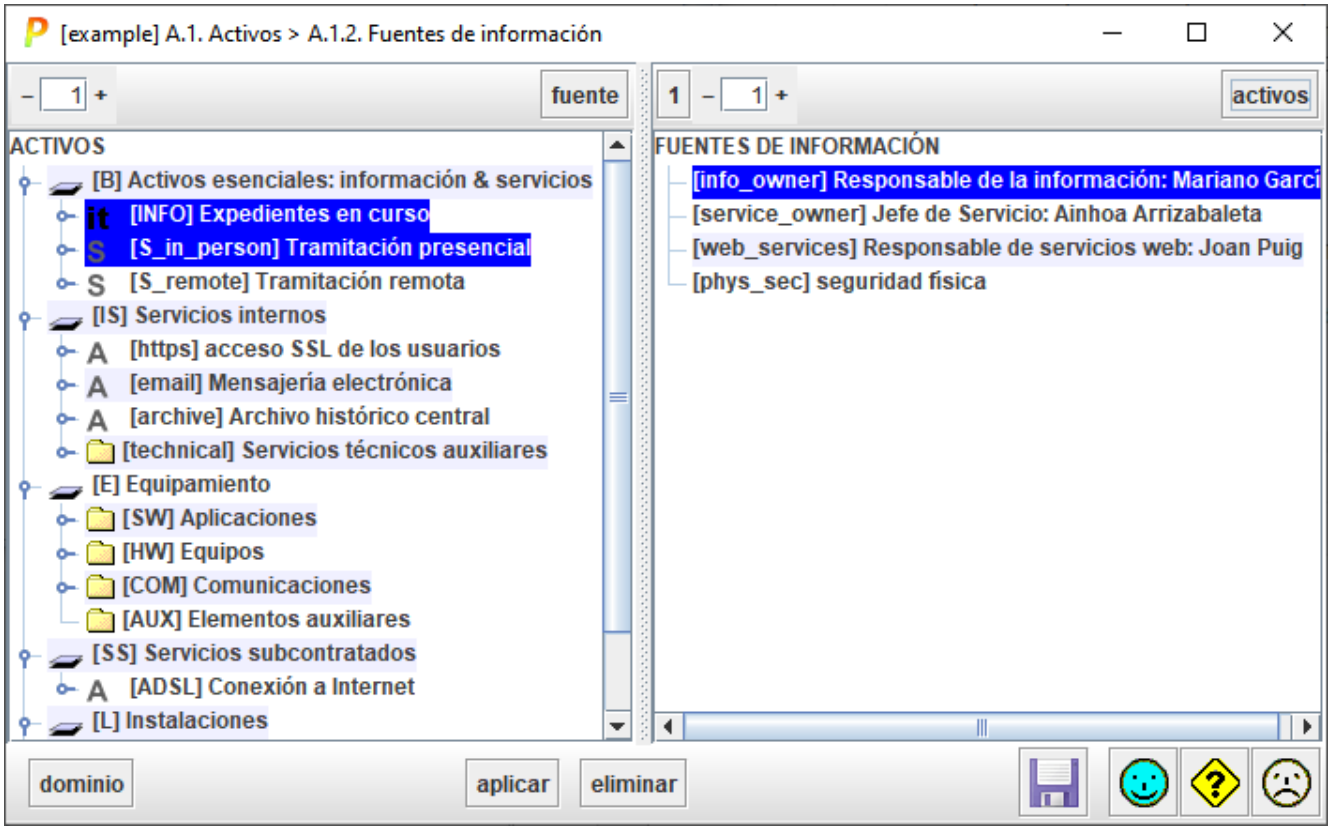

[example] análisis de riesgos > activos > identificación de activos > activo
INFO
nombre
Expedientes en curso
Fuentes de información
info_owner
dominio
[base] red corporativa
datos
Descripción
estado de los procesos de tramitación abiertos
contenido
almacena temporalmente datos financieros de los
propietario
jefe de servicio de tramitación
CLASES DE ACTIVOS
[essential] Activos esenciales
[info] información
[adm] datos de interés para la administració
[per] datos de carácter personal
[regular] datos personales normales
[1] económicos
[5] localización
[ppd] tratamiento de datos personales
descripción
RGPD


[example] análisis de riesgos > activos > identificación de activos > activo > RGPD
roles
riesgo
datos
controles
[INFO] Expedientes en curso
DPD (Delegado de Protección de Datos)
Interpretar y supervisar la aplicación del RGPD en la organización
Responsable del tratamiento
Art. 4.7: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines
medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el
responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de l
Estados miembros
Encargado del tratamiento
Art. 4.8: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del
responsable del tratamiento

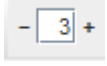
8.3 Activos / Fuentes de información

Para gestionar la asociación de activos a fuentes de información.

El panel izquierdo presenta el árbol de activos. El panel derecho, las fuentes de información.



Barra superior izquierda

	Controla el nivel de despliegue del árbol de activos (izquierda).
FUENTE	— Seleccione uno o más activos a la izquierda — Haga clic en FUENTE PILAR seleccionará las fuentes asociadas a la derecha

Barra superior derecha

	Controla el nivel de despliegue del árbol de fuentes de información (derecha).
ACTIVOS	— Seleccione una o más fuentes a la derecha — Haga clic en ACTIVOS. PILAR seleccionará los activos asociados a la izquierda

Barra inferior

dominio	— Selecciona los activos que pertenecen a un cierto dominio

aplicar	— Seleccione uno o más activos — Seleccione una o más fuentes — Haga clic en APLICAR y quedarán asociados.
eliminar	— Seleccione uno o más activos — Seleccione una o más fuentes — Haga clic en ELIMINAR y quedarán disociados.

Para asociar una fuente a un activo

- seleccione uno o más activos a la izquierda
- seleccione una o más fuentes a la derecha
- clic APLICAR

Para eliminar una asociación

- seleccione uno o más activos a la izquierda
- seleccione una o más fuentes a la derecha
- clic ELIMINAR

Para seleccionar las clases asociadas a un activo

- seleccione uno o más activos a la izquierda
- clic CLASES DE ACTIVOS

Para seleccionar los activos asociados a una clase

- seleccione una o más clases a la derecha
- clic ACTIVOS

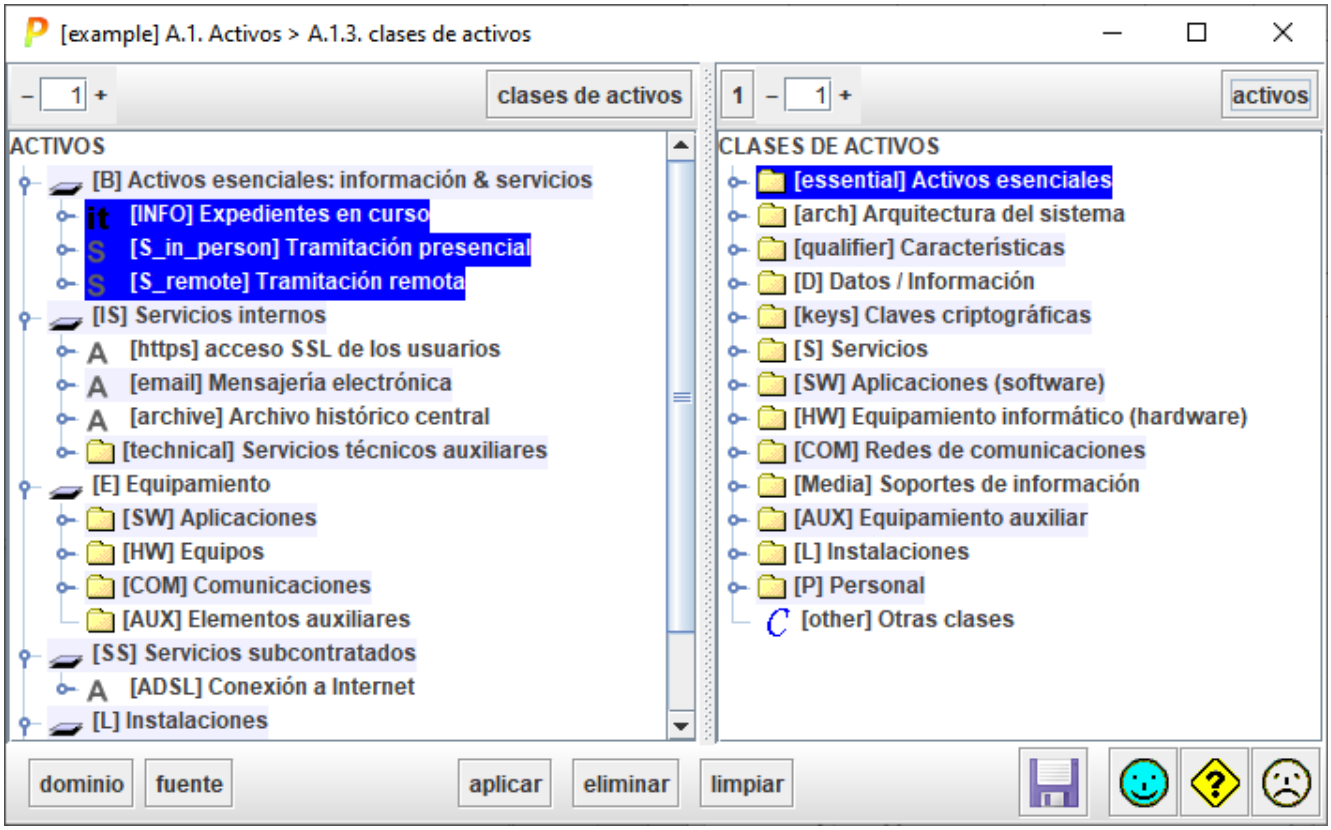
Para copiar y pegar una asociación

- seleccione uno o más activos a la izquierda
- clic CLASES DE ACTIVOS
- seleccione uno o más activos a la izquierda
- clic APLICAR

8.4 Activos / Clases de activos

Esta pantalla permite ver, asignar, eliminar y validar las clases que afectan a un activo y los activos que se ven calificados por una cierta clase.

El árbol izquierdo muestra los activos y los códigos de las clases asociadas a cada activo.



Barra superior izquierda

− 3 +	Controla el nivel de despliegue del árbol de activos (izquierda).
CLASES DE ACTIVOS	— Seleccione uno o más activos a la izquierda — Haga clic en CLASES DE ACTIVOS. PILAR seleccionará las clases asociadas a la derecha

Barra superior derecha

− 3 +	Controla el nivel de despliegue del árbol de clases (derecha).
ACTIVOS	— Seleccione una o más clases a la derecha — Haga clic en ACTIVOS. PILAR seleccionará los activos asociados a la izquierda

Barra inferior

dominio	— Selecciona los activos que pertenecen a un cierto dominio
fuente	— Selecciona los activos asociados a una cierta fuente
aplicar	— Seleccione uno o más activos — Seleccione una o más clases — Haga clic en APLICAR y quedarán asociados.
eliminar	— Seleccione uno o más activos — Seleccione una o más clases — Haga clic en ELIMINAR y quedarán disociados.
limpiar	— Seleccione uno o más activos — Haga clic en LIMPIAR y quedarán simplificadas.

Para asociar una clase a un activo

- seleccione uno o más activos a la izquierda
- seleccione una o más clases a la derecha
- clic APLICAR

Para eliminar una asociación

- seleccione uno o más activos a la izquierda
- seleccione una o más clases a la derecha
- clic ELIMINAR

Para simplificar una asociación (o sea, si están marcadas a la derecha una cierta clase y su padre, para quedarnos solo con la clase más detallada)

- seleccione uno o más activos a la izquierda
- clic LIMPIAR

Para seleccionar las clases asociadas a un activo

- seleccione uno o más activos a la izquierda
- clic CLASES DE ACTIVOS

Para seleccionar los activos asociados a una clase

- seleccione una o más clases a la derecha
- clic ACTIVOS

Para copiar y pegar una asociación

- seleccione uno o más activos a la izquierda
- clic CLASES DE ACTIVOS
- seleccione uno o más activos a la izquierda
- clic APLICAR

8.5 Activos / Nombres CPE

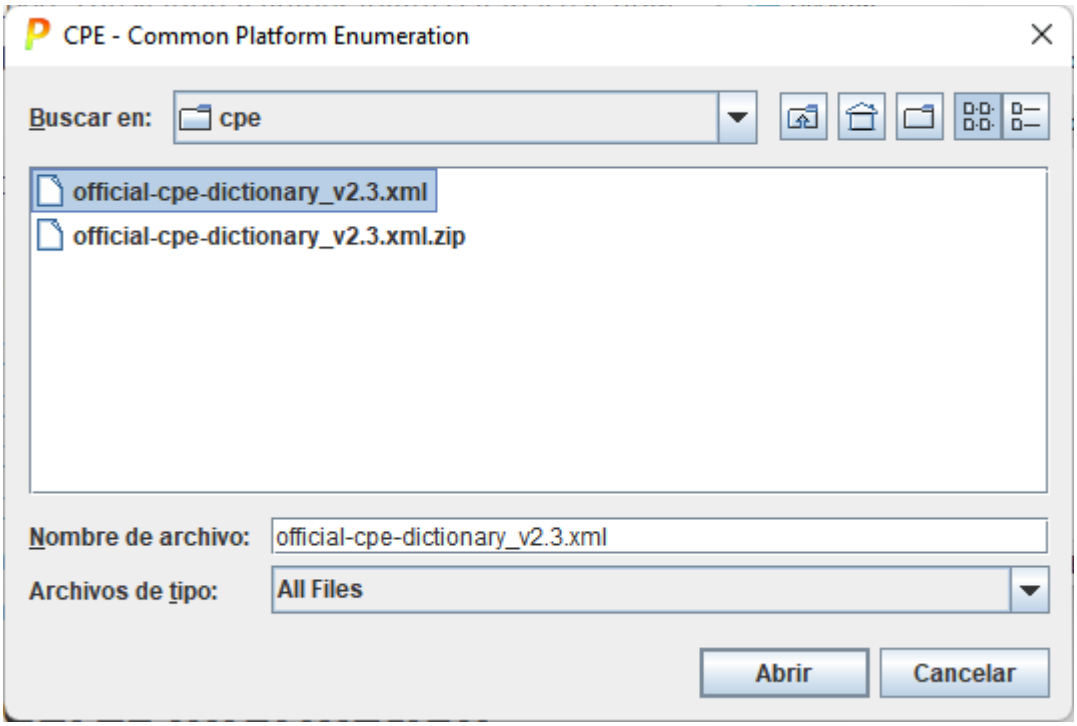
A los activos se les pueden asociar uno o más nombres CPE que se pueden usar posteriormente para asociarles vulnerabilidades CVE.

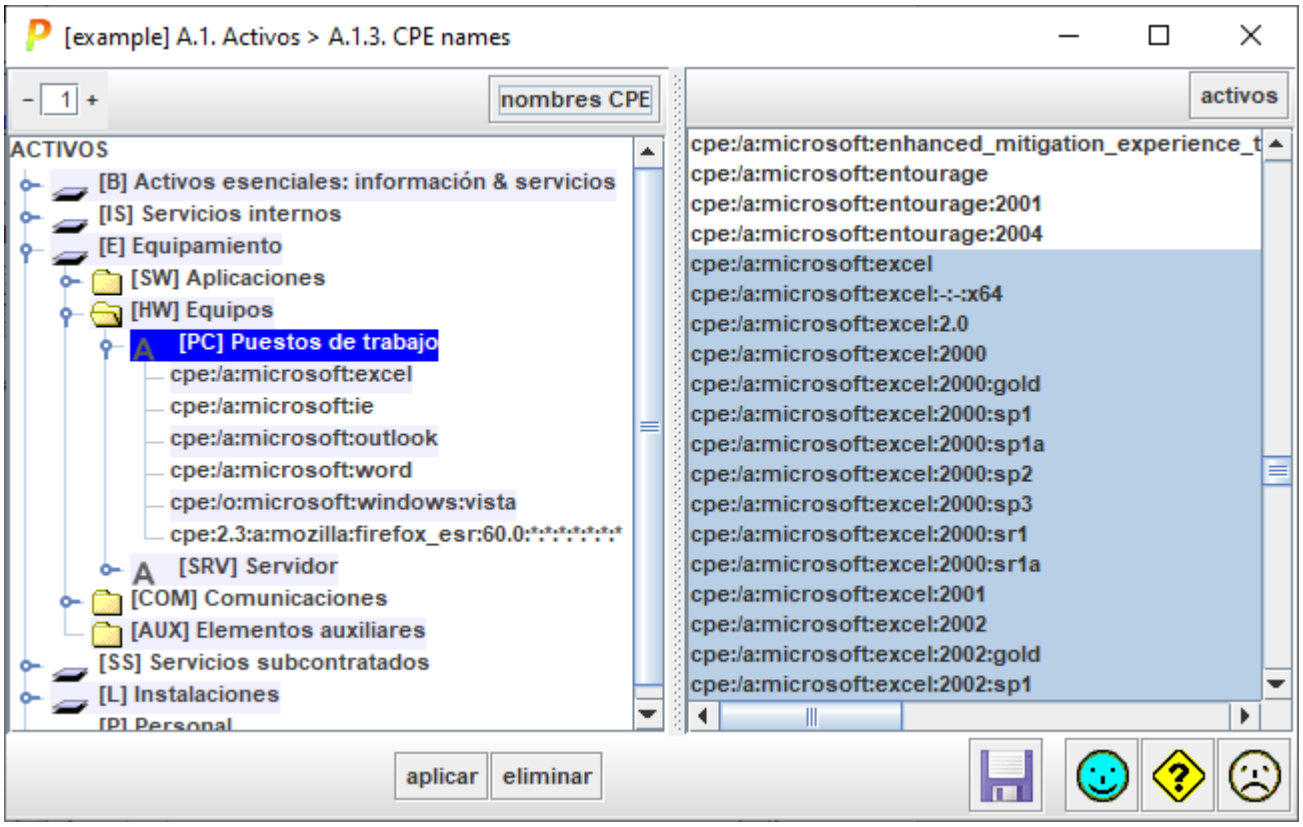
Ver https://www.ar-tools.com/doc/

El diccionario de nombres CPE evoluciona continuamente. Descargue una versión actualizada de

[http://nvd.nist.gov/download.cfm]

NIST distribuye el diccionario en versión 2.2 y 2.3. PILAR lee ambas, pero prefiere 2.3.





Barra superior izquierda

3	Controla el nivel de despliegue del árbol de activos
NOMBRES CPE	Seleccione uno o más activos a la izquierda. Haga clic en NOMBRES CPE y PILAR seleccionará a la derecha los nombres asociados.

Barra superior derecha

3	Controla el nivel de despliegue del árbol de nombres CPE
ACTIVOS	Seleccione uno o más nombres a la derecha. Haga clic en ACTIVOS y PILAR seleccionará a la izquierda los activos asociados.

Barra inferior

APLICAR	Seleccione uno o más activos a la izquierda. Seleccione uno o más activos a la derecha. Haga clic en APLICAR para asociarlos.
ELIMINAR	Seleccione uno o más activos a la izquierda. Seleccione uno o más activos a la derecha. Haga clic en ELIMINAR para disociarlos.
FILTRAR	Reduce los elementos en el panel derecho filtrando por fabricante.

Para asociar un nombre a un activo

- seleccione uno más activos a la izquierda
- seleccione uno o más nombres a la derecha
- clic APLICAR

Para disociar un activo de un nombre

- seleccione el nombre que quiere disociar
- clic ELIMINAR

Para seleccionar los nombres asociados a un activo

- seleccione uno o más activos a la izquierda
- clic NOMBRE CPE

Para seleccionar los activos asociados a un nombre

- seleccione uno o más nombres a la derecha
- clic ACTIVOS

Para buscar un activo o un nombre

- control-F en el panel correspondiente

8.6 Activos / Dependencias

Se pueden establecer dependencias entre activos. Las dependencias se usan para propagar el valor (es decir, los requisitos de seguridad) desde los activos valiosos (arriba) a los activos que soportan el valor por delegación (abajo).

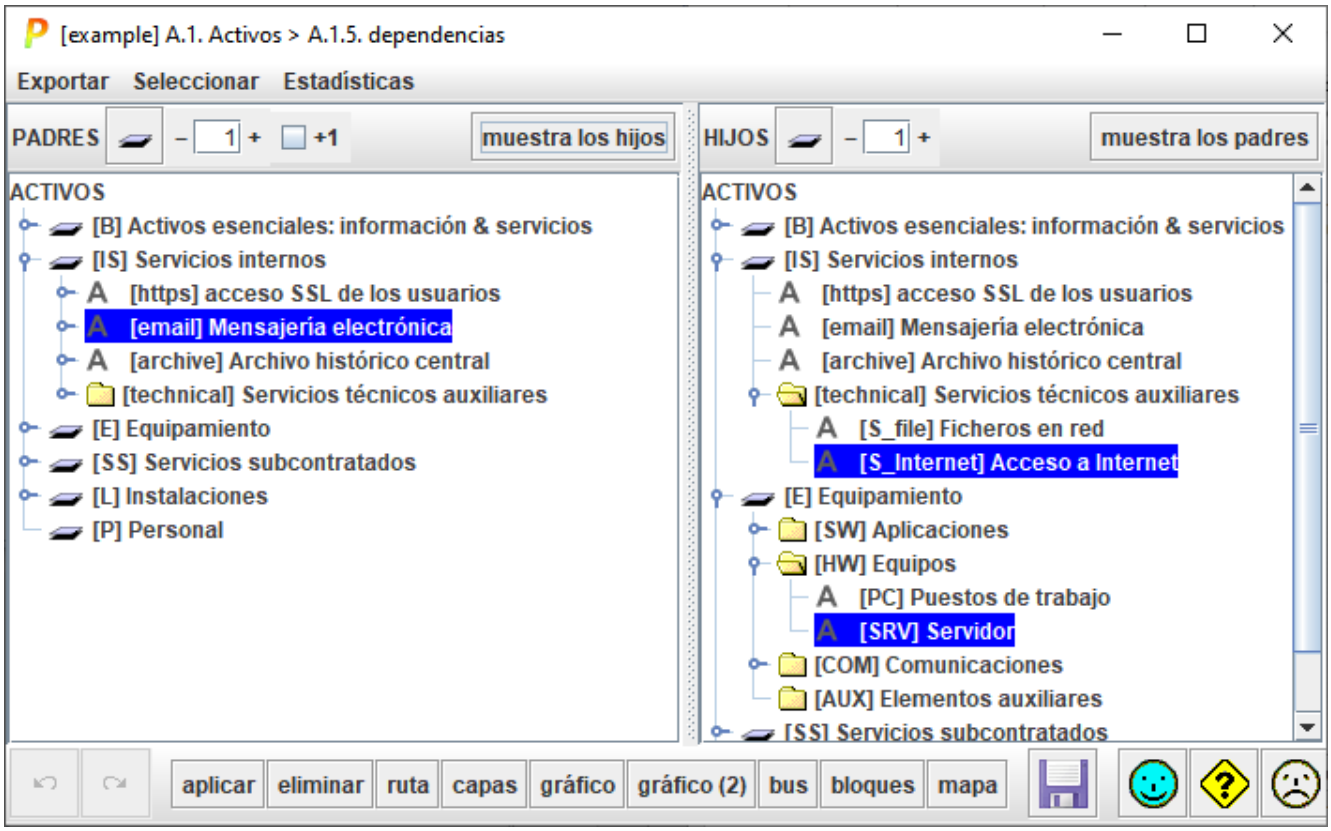
El sistema de información puede valorarse por dominios o activo por activo. Se elige en *Opciones / Valoración*

Si el usuario está valorando por dominios, puede prescindir de dependencias y pasar directamente a *Valoración por dominios*

Si el usuario está valorando activo por activo, entonces debe establecer las dependencias y luego pasar a *Valoración por activos*

Para empezar rápidamente
Si ha identificado las instalaciones … • asocie cada equipo a la instalación donde se encuentra Si ha identificado servicios y equipos … • asocie cada servicio al equipamiento que utiliza: software, hardware, comunicaciones, medios,… Si ha identificado personal … • asocie cada persona a los servicios o al equipo sobre los que puede causar daño voluntaria o accidentalmente Repita hasta que cada activo por debajo de la capa de negocio se utiliza para algo.

Esta pantalla se utiliza para establecer las dependencias entre activos. El panel izquierdo muestra los activos “padre” (el activo superior en el grafo de dependencias), mientras que el panel derecho muestra los activos “hijo” (los activos inferiores en el grafo de dependencias).



Menú superior EXPORTAR

XML	eXtensible Markup Language
GraphML	formato GraphML
CSV	Comma Separated Values; para excel

Menú superior SELECCIONAR

sin padres	selecciona los activos sin dependencias superiores
sin hijos	selecciona los activos sin dependencias inferiores
bucles	selecciona grupos de activos atrapados en un bucle de dependencias

Menú superior ESTADÍSTICAS

dependencias	tabla resumen

Barra superior izquierda (PADRES)

	Haga clic para colapsar el árbol izquierdo.
	Controla el nivel de expansión del árbol izquierdo. Si está seleccionado [+1], se muestran también los activos de los que depende.
+1	Controla si el árbol de activos (izquierdo) incluye las dependencias.

mostrar los hijos	Seleccione un activo en el árbol izquierdo. Haga clic en MOSTRAR LOS HIJOS. PILAR seleccionará a la derecha los activos de los que depende directa e indirectamente.

Barra superior derecha (HIJOS)

	Haga clic para colapsar el árbol derecho.
	Control the level of expansion of the right tree.
mostrar los padres	Seleccione un activo en el árbol derecho. Haga clic en MOSTRAR LOS PADRES. PILAR seleccionará a la izquierda los activos que dependen de él directa e indirectamente.

Barra inferior

	Deshace el último APILAR o ELIMINAR.
	Rehace el último APLICAR o ELIMINAR deshecho.
aplicar	Seleccione uno o más activos a la izquierda. Seleccione uno o más activos a la derecha. Haga clic en APLICAR. PILAR hace depender cada activo seleccionado a la izquierda de todos y cada uno de los activos seleccionados a la derecha.
eliminar	Seleccione uno o más activos a la izquierda. Seleccione uno o más activos a la derecha. Haga clic en ELIMINAR. PILAR elimina toda dependencia directa entre los activos seleccionados a la izquierda y los activos seleccionados a la derecha. o seleccione una o más dependencias a la izquierda y haga clic en ELIMINAR para eliminarla.
ruta	Seleccione un activo a la izquierda y un activo a la derecha. Haga clic en RUTA. PILAR abre una ventana auxiliar mostrando el grafo de dependencias desde el activo izquierdo (VERDE) al activo derecho (ROJO).
capas	Abre una ventana con tantas cajitas como capas, mostrando las dependencias entre activos de cada capa. Ver "*Activos / Dependencias / Capas*".
gráfico (1)	Abre una ventana con tantas cajitas como activos, mostrando las dependencias entre ellos. Ver "*Activos / Dependencias / Grafo*".
gráfico (2)	Como GRÁFICO; pero usando un algoritmo alternativo para colocar los nodos. Ver "*Activos / Dependencias / Grafo*".

buses	Abre una ventana con tantas cajitas como activos, mostrando las dependencias entre ellos. Ver "*Activos / Dependencias / Buses*".
bloques	Abre una ventana con tantas cajitas como activos, mostrando las dependencias entre activos de cada capa. Ver "*Activos / Dependencias / Bloques*".
mapa	Abre una ventana con tantas cajitas como activos, mostrando las dependencias entre ellos. Ver "*Activos / Dependencias / Mapa*".
	Guarda el proyecto en su fichero o en su base de datos.

Varias pantallas presentan un botón LIVE. Si se selecciona, el diagrama sigue la selección de activos en la pantalla principal. Si no, hay que actualizarlo manualmente..

Para establecer una dependencia

- seleccione P en el panel izquierdo (unos o más activos)
- seleccione H en el panel derecho (unos o más activos)
- clic APLICAR

Si P o H, o ambos, son grupos, la dependencia será establecida entre los miembros correspondientes de cada grupo. Así pues, cuando un grupo depende de otro grupo, cada activo del grupo del padre depende de cada activo del grupo del hijo.

Para quitar una dependencia

- seleccione P en el panel izquierdo (unos o más activos)
- seleccione H en el panel derecho (unos o más activos)
- ELIMINAR

o

- seleccione H en el panel izquierdo (unos o más activos)
- ELIMINAR

Para descubrir a los hijos de P

- seleccione P en el panel izquierdo (unos o más activos)
- clic HIJOS

Para descubrir a los padres de H

- seleccione H en el panel derecho (unos o más activos)
- clic PADRES

Para fijar un grado de dependencia

Por defecto, las dependencias son al 100%.

Para fijar un grado entre el 0% y el 100%:

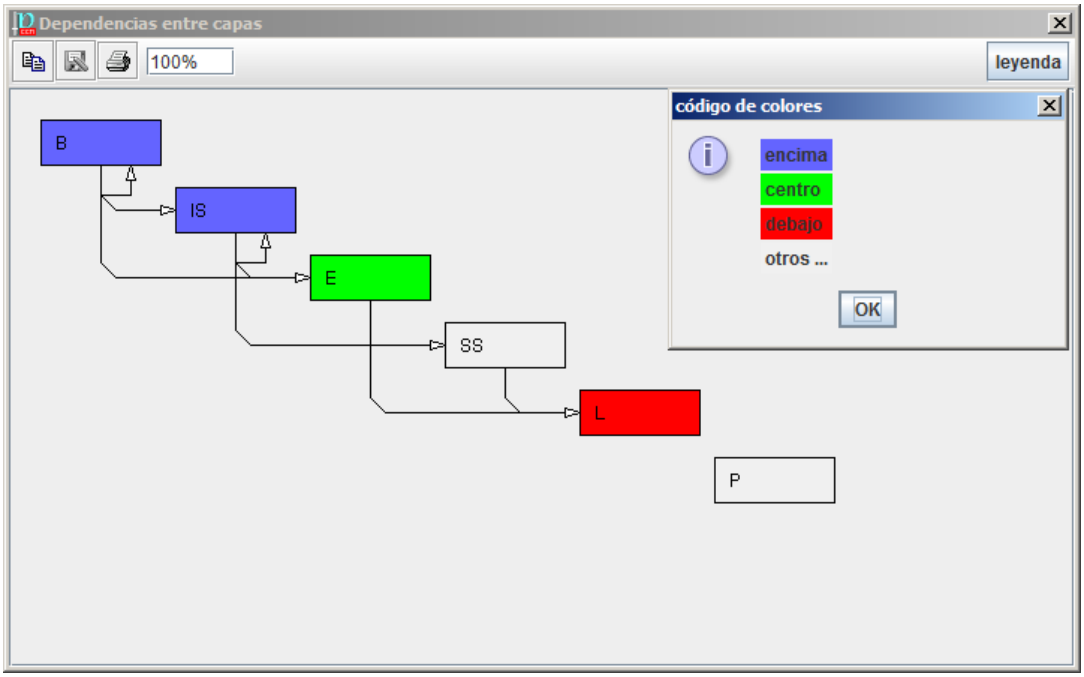
- amplíe las dependencias debajo de un activo

- seleccione el activo del hijo (marcado con el icono “d”)
- clic en el botón derecho del ratón para establecer un valor
- vea "*Dependencias por dimensión de seguridad*"

Para descubrir cómo se relaciona un activo con otro:

- seleccione el padre en el panel izquierdo
- seleccione el hijo en el panel derecho
- clic en RUTA

8.6.1 Mapa de dependencias entre capas



El gráfico muestra las relaciones entre las capas. Una capa L1 depende de una capa L2 si hay algún activo en L1 que dependa de algún activo en L2.

Si es un modelo “limpio”

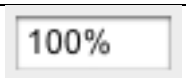
- las capas superiores dependen solamente de capas inferiores
- las capas inferiores dependen solamente de capas superiores
- puede haber dependencias internas en las capas

Lo anterior no es obligatorio; pero los proyectos que no se adhieren a la regla son más difíciles de entender y explicar.

Cuando haga clic en una capa, el gráfico se colorea:

azul profundo	capas superiores directamente relacionadas
verde	la capa de la referencia

rojo brillante	capas inferiores directamente relacionadas
gris	no relacionadas

	**copiar**	copia la imagen al portapapeles para pegarlo en algún otro sitio
	**guardar**	almacena el dibujo en un fichero gráfico. Los formatos de imagen disponibles dependen de su ordenador; algunos formatos son casi universales jpg, JPEG, png
	**imprimir**	para enviar el gráfico a una impresora
	**escala**	para cambiar el tamaño de la imagen
	leyenda	muestra el código de colores

Estas gráficas presentan un botón MEMORIA que permite memorizar diagramas bajo un nombre

nueva etiqueta	define una nueva etiqueta con un nombre
renombrar	permite cambiarle el nombre a una etiqueta
eliminar	permite eliminar una etiqueta
cargar	el diagrama actual se guarda bajo el nombre de la etiqueta
seleccionar	se recupera el diagrama referenciado

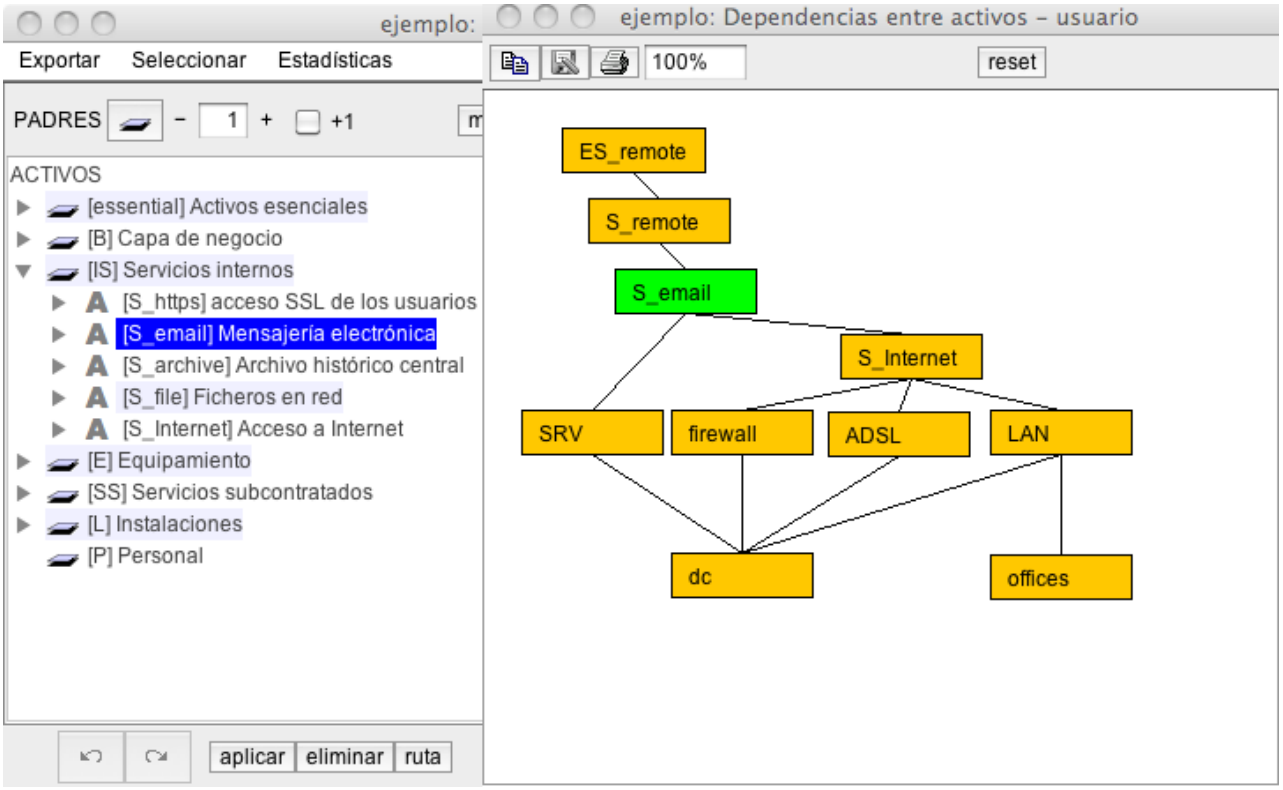
8.6.2 Grafo de dependencias entre activos

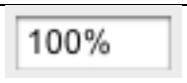
El gráfico muestra las relaciones de dependencia entre activos. Solo presenta aquellos activos seleccionados en el panel principal y los relacionados con los seleccionados. Si no se selecciona nada, se presentan todos los activos.

PILAR aplica una serie de heurísticos para ubicar los activos de forma que se respete lo más posible la estructura de capas, pero que en ningún momento un activo "superior" esté por debajo de un activo "inferior". De esta forma todas las dependencias van de arriba a abajo. Sin embargo, si el gráfico no es agradable, el usuario puede recolocar los activos según desee (use el ratón para seleccionar y llevar a otra posición.).

Actualmente PILAR incluye 2 algoritmos de posicionamiento automático de nodos (sabiamente denominados (1) y (2)). La única diferencia reside en el posicionado automático.

El gráfico sigue la selección en la pantalla principal de dependencias. Así pues, si selecciona un activo, un grupo o una capa, solo los activos en el grupo y aquellos otros activos alcanzables directa o indirectamente, aparecerán en el gráfico.



	**copiar**	copia la imagen al portapapeles para pegarlo en algún otro sitio
	**guardar**	almacena el dibujo en un fichero gráfico. Los formatos de imagen disponibles dependen de su ordenador; algunos formatos son casi universales jpg, JPEG, png
	**imprimir**	para enviar el gráfico a una impresora
	**escala**	para cambiar el tamaño de la imagen
	reset	reposiciona las cajas heurísticamente

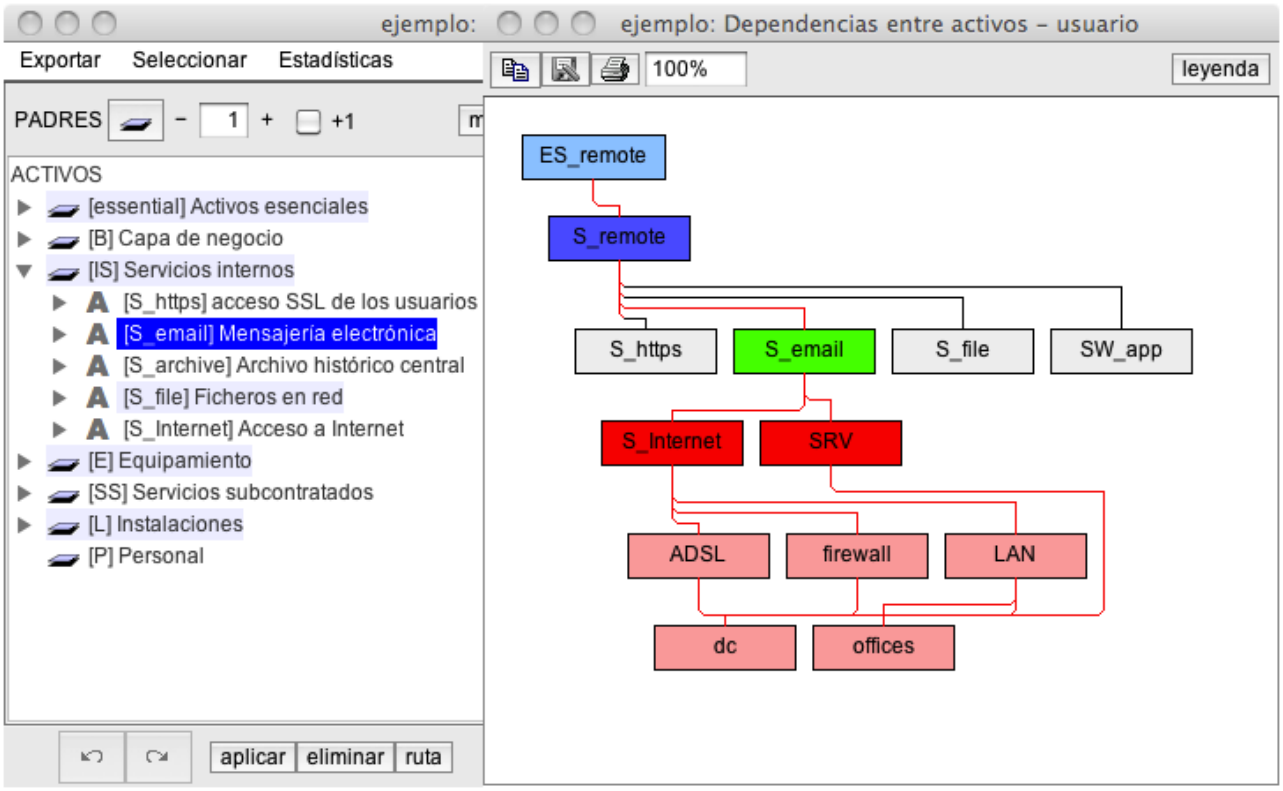
8.6.3 Buses: dependencias entre activos

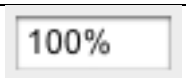
El gráfico muestra las relaciones de dependencia entre activos. Solo presenta aquellos activos seleccionados en el panel principal y los relacionados con los seleccionados. Si no se selecciona nada, se presentan todos los activos.

Los activos se posicionan en la pantalla de forma heurística de tal forma que todas las relaciones de dependencia van hacia 'abajo'. PILAR crea unos *buses* o pistas de conexión entre activos, evitando que los enlaces pasen por encima de los activos.

La gráfica sigue lo que se va seleccionando en la pantalla principal.

Por último, dentro del gráfico, si se selecciona un activo (haciendo clic en él), se marcan en color aquellos que están por encima (rojo) o por debajo (azul), directa o indirectamente.



	**copiar**	copia la imagen al portapapeles para pegarlo en algún otro sitio
	**guardar**	almacena el dibujo en un fichero gráfico. Los formatos de imagen disponibles dependen de su ordenador; algunos formatos son casi universales jpg, JPEG, png
	**imprimir**	para enviar el gráfico a una impresora
	**escala**	para cambiar el tamaño de la imagen
	leyenda	muestra el código de colores

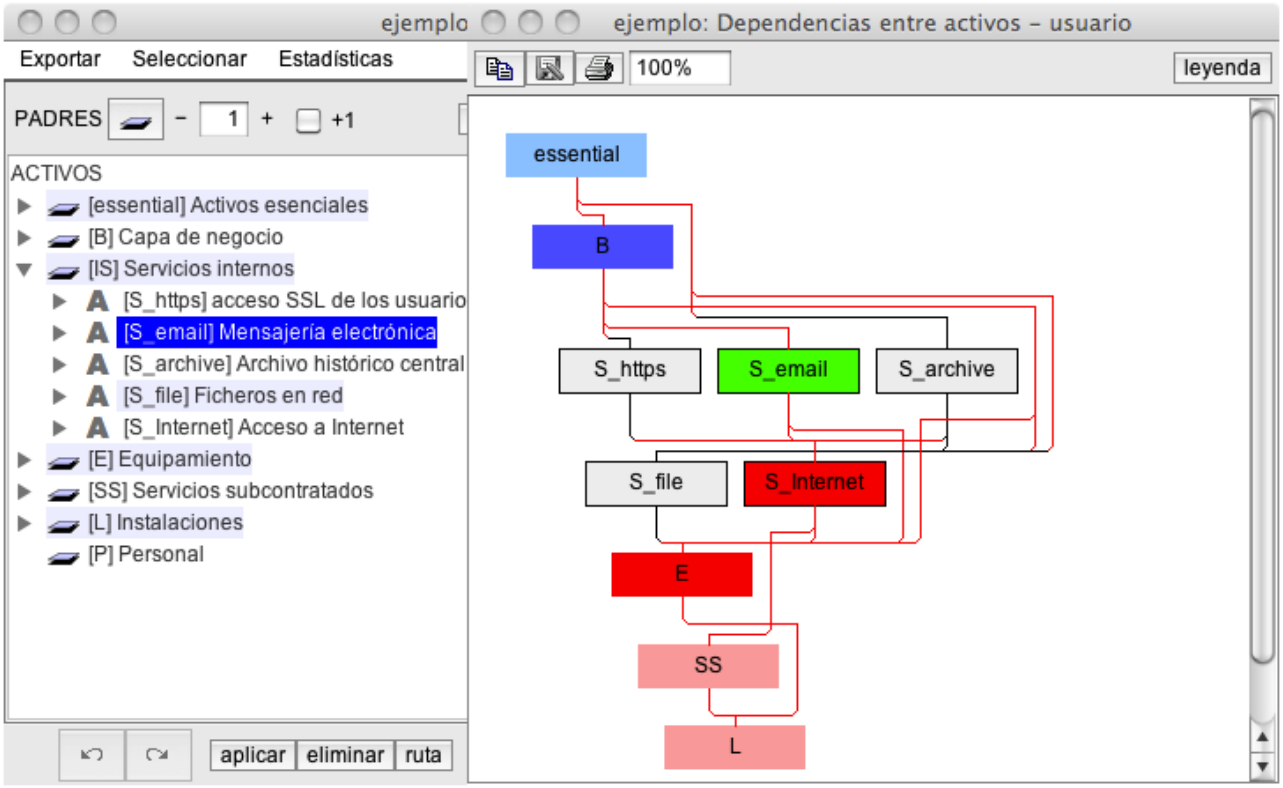
8.6.4 Bloques: dependencias entre activos

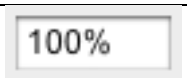
El gráfico muestra las relaciones de dependencia entre activos. Solo se presentan los activos que se pueden ver en la pantalla principal, respetando lo que está expandido o colapsado en dicha pantalla.

Los activos se posicionan en la pantalla de forma heurística de tal forma que todas las relaciones de dependencia van hacia ‘abajo’. PILAR crea unos *buses* o pistas de conexión entre activos, evitando que los enlaces pasen por encima de los activos.

La gráfica sigue lo que se va seleccionando en la pantalla principal.

Por último, dentro del gráfico, si se selecciona un activo (haciendo clic en él), se marcan en color aquellos que están por encima (rojo) o por debajo (azul), directa o indirectamente.



	**copiar**	copia la imagen al portapapeles para pegarlo en algún otro sitio
	**guardar**	almacena el dibujo en un fichero gráfico. Los formatos de imagen disponibles dependen de su ordenador; algunos formatos son casi universales jpg, JPEG, png
	**imprimir**	para enviar el gráfico a una impresora
	**escala**	para cambiar el tamaño de la imagen
	leyenda	muestra el código de colores

8.6.5 Mapa de dependencias entre activos

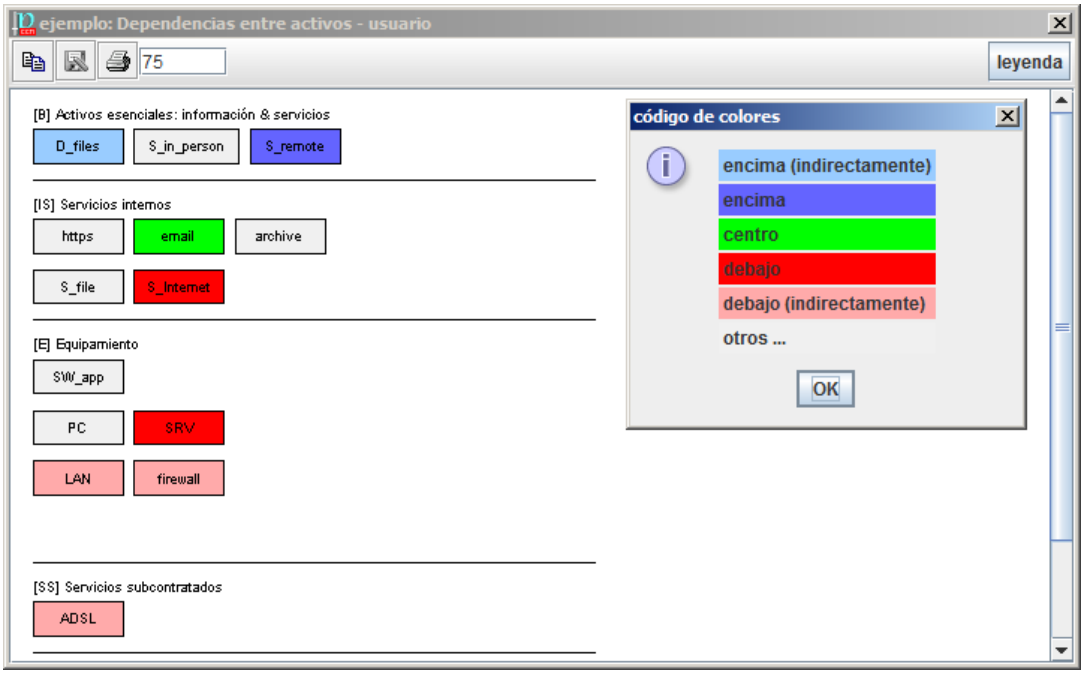
Este mapa sirve para estudiar gráficamente las dependencias entre activos.

Los activos se presentan en capas. La ubicación es fija: para reubicarlos habría que reposicionarlos en el árbol de activos.

Cuando se selecciona un activo, el mapa se colorea:

azul claro	activos superiores relacionados indirectamente
azul fuerte	activos superiores relacionados directamente
verde	el activo seleccionado
rojo fuerte	activos inferiores relacionados directamente

rojo claro	activos inferiores relacionados indirectamente
gris	sin relación



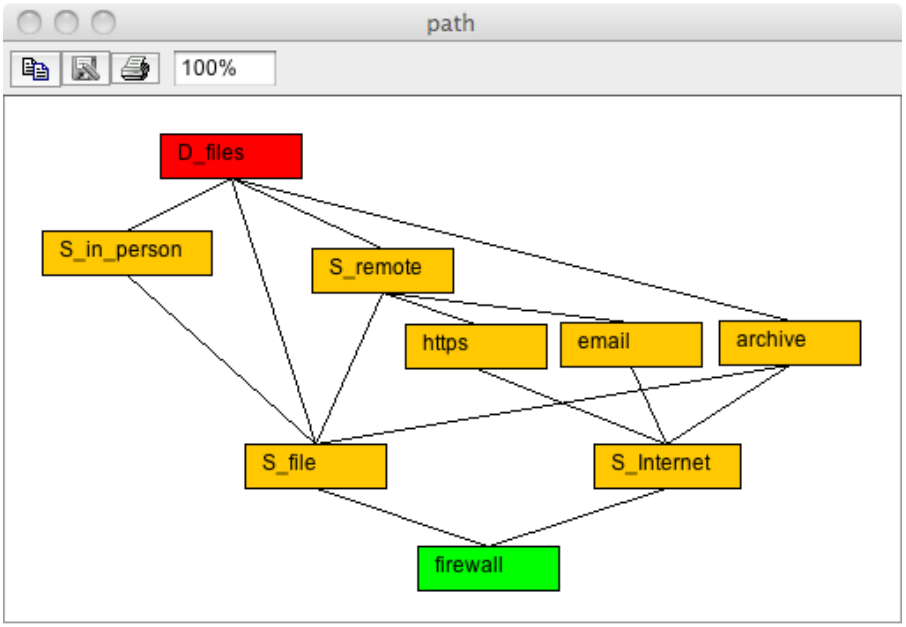
Para modificar las dependencias

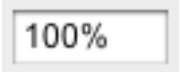
Mientras que tiene seleccionado un activo (verde) se puede ir a otro activo y hacer clic en el botón derecho del ratón:

- para agregar este activo como superior del seleccionado
- para agregar este activo como inferior del seleccionado
- para eliminar la dependencia entre este activo y el seleccionado

Para describir la vía de dependencia entre un activo y otro

- seleccione el padre (verde)
- seleccione el hijo (botón derecho del ratón)
- clic en RUTA



	**copiar**	copia la imagen al portapapeles para pegarlo en algún otro sitio
	**guardar**	almacena el dibujo en un fichero gráfico. Los formatos de imagen disponibles dependen de su ordenador; algunos formatos son casi universales jpg, JPEG, png
	**imprimir**	para enviar el gráfico a una impresora
	**escala**	para cambiar el tamaño de la imagen
	leyenda	muestra el código de colores

8.6.6 Dependencias por dimensión de seguridad

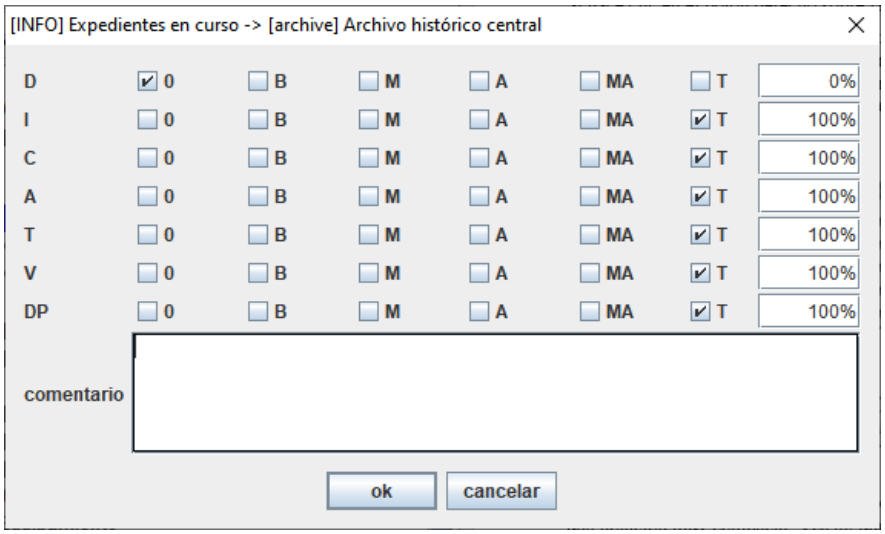
Se puede especificar un grado de dependencia diferente en cada dimensión. Para ello haga clic con el botón derecho sobre la dependencia y aparecerá una pantalla donde puede marcar el grado de dependencia preciso en cada dimensión.

Los valores típicos son como sigue:

N	ninguno	0%	no depende
L	bajo	1%	académico – prácticamente despreciable
M	medio	10%	significativo; pero no mucho
H	alto	50%	no se exactamente ...
VH	muy alto	90%	prácticamente, completamente dependiente
T	total	100%	depende completamente

Si hace clic en el botón derecho sobre la dependencia que desea modificar, tendrá varias opciones:

— marca todas el mismo porcentaje se aplica a cada dimensión
— marca solo 100% para la dimensión seleccionada, 0% para las demás
— marca 100% para la dimensión seleccionada, deja las demás como estaban
— elimina 0% para la dimensión seleccionada, deja las demás como estaban
— detalles abre una ventana de edición



Cuando deje la pantalla para establecer dependencias, el valor seleccionado aparece en el árbol usando una notación muy compacta. Vea algunos ejemplos:

expresión	**significado**
D:100%	la dependencia se limita a la dimensión D, disponibilidad; las otras dimensiones no dependen ejemplo: cuando una VPN elimina la necesidad de proteger el canal de trasporte más allá de su disponibilidad
I:100% / C:100%	la dependencia se limita a las dimensiones I, integridad, y C, confidencialidad; las otras dimensiones son independientes ejemplo: cuando la existencia de equipamiento alternativo garantiza la disponibilidad funcional del activo

El formato puede definirse como

expresión ::= { una_dimension }0+

una_dimensión ::= ACRÓNIMO `':'` porcentaje `'/'`

Cuando aparece una expresión, todas las dimensiones toman como grado de dependencia 0%, salvo que se indique explícitamente.

8.7 Activos / Valoración

El sistema de información puede valorarse por dominios o activo por activo. Se elige en *Opciones / Valoración*

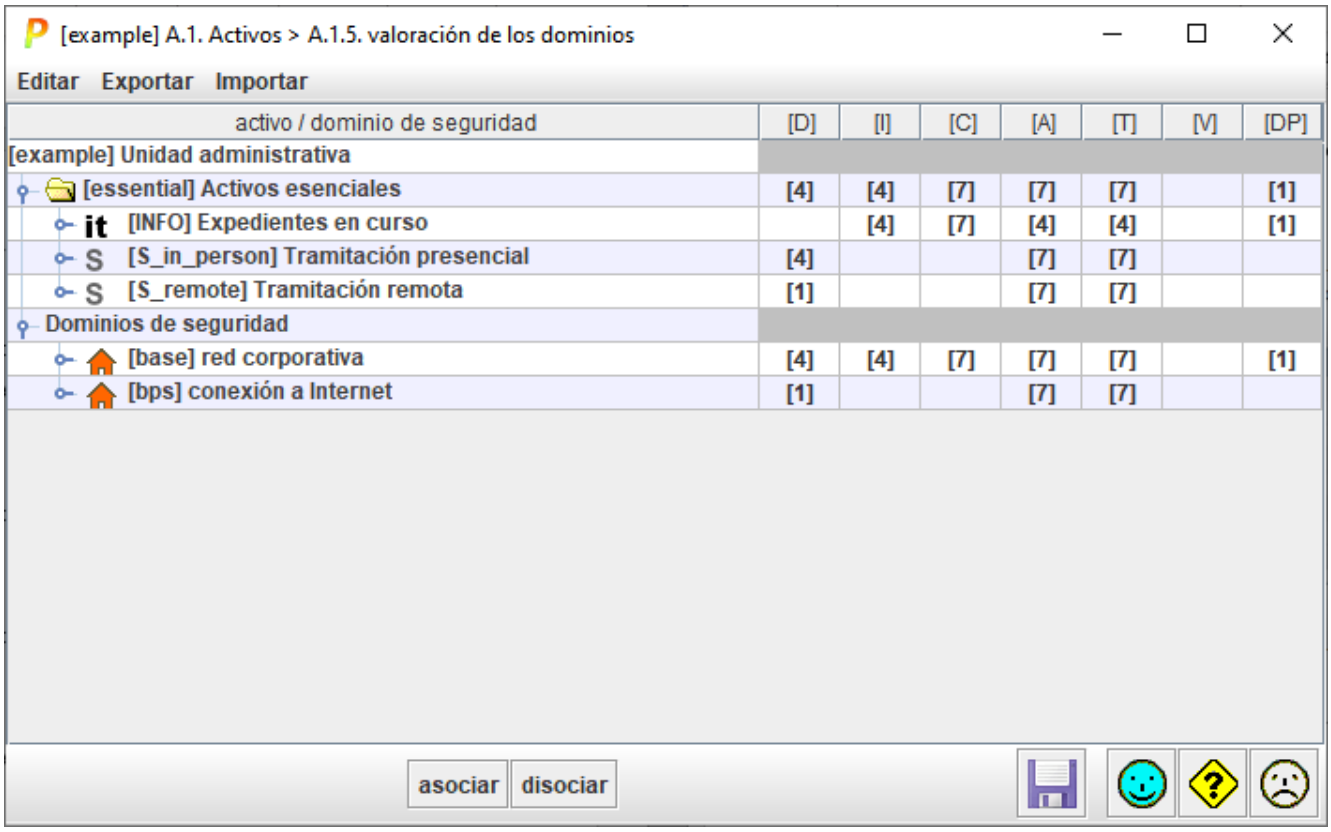
Si el usuario está valorando por dominios, puede prescindir de dependencias y pasar directamente a *Valoración por dominios*

Si el usuario está valorando activo por activo, entonces debe establecer las dependencias y luego pasar a *Valoración por activos*

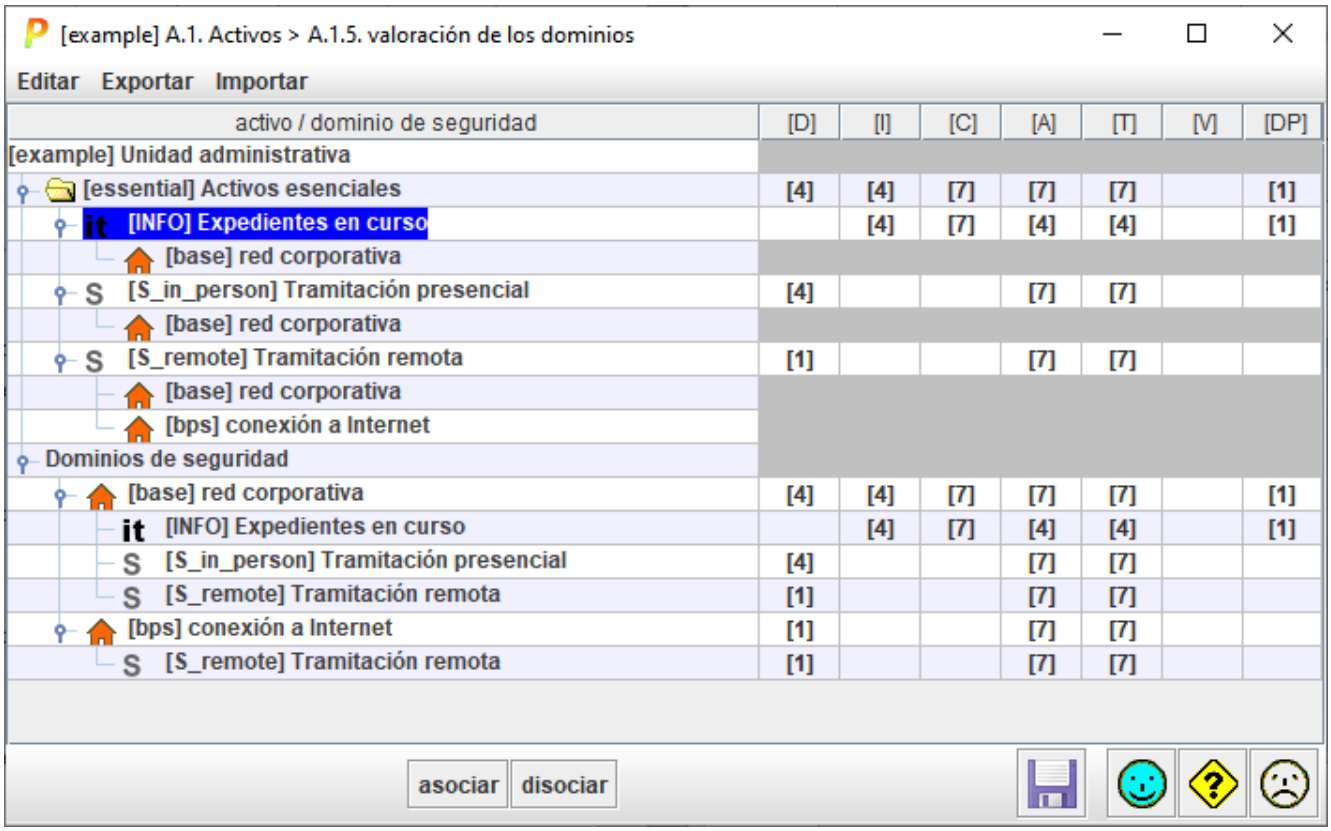
8.7.1 Valoración de los dominios de seguridad

Se hace una valoración "rápida y aproximada" común para todos los activos en el dominio. Es más rápido que la valoración por dependencias. Usando este método, todos los activos en el dominio reciben los mismos valores.

El valor del sistema de información se establece por dominios. La valoración la imponen los activos esenciales (información y servicios) y se la trasladan al dominio que los acoge y a los dominios a los que se asocian.



Se entiende mejor si se despliegan las asociaciones de activos a dominios y viceversa:



Menú superior EDITAR

	Seleccione una o más celdas. Copie lo valores para pegarlos más tarde.
	Seleccione una o más celdas de destino. Pegue los valores que antes copió. Si el original era una celda y el destino son varias, se repite el valor.

Menú superior EXPORTAR

CSV	CSV – comma separated values; para excel
XML	XML – extensible markup language

Menú superior IMPORTAR

XML	XML – extensible markup language

Tabla – Tantas columnas como dimensiones de seguridad.

Para cada activo esencial y cada dimensión de seguridad, el valor

- Ver *Activos / Valoración / cualitativo*
- Ver *Activos / Valoración / cuantitativo*

Para cada dominio de seguridad, el valor heredado de los activos esenciales que tiene asociados

Barra inferior

asociar	Seleccione un activo y un dominio. Haga clic en ASOCIAR para asociar el activo al dominio. Los activos siempre están asociados a su dominio. El usuario solo puede asociarlos a alguno más.
disociar	Seleccione un activo y un dominio. Haga clic en DISOCIAR para disociar el activo del dominio. Un activo nunca puede disociarse de su propio dominio.
	Guarda el proyecto en su fichero o en su base de datos.

Típicamente, la información requiere proteger confidencialidad, integridad, autenticidad y trazabilidad, mientras que los servicios añaden requisitos en términos de disponibilidad.

La valoración del sistema es el mayor valor de los establecidos para alguna información o servicio.

Cada dominio hereda la valoración de los activos esenciales que contiene y de los asociados a él.

Para asociar un activo a un dominio

- seleccione el activo
- seleccione el dominio
- clic ASOCIAR

Para disociar un activo de un dominio

- seleccione el activo
- seleccione el dominio
- clic DISOCIAR

8.7.2 Valoración activo por activo

El valor de cada activo puede ser

propio

porque explícitamente se lo adjudicamos (en esta pantalla)

por dominios (ver "*Dependencias entre activos*").

heredando bien de los activos esenciales del mismo dominio, o de los activos esenciales de dominios asociados

por dependencias (ver "*Dependencias entre activos*").

heredando de los activos que dependen de él.

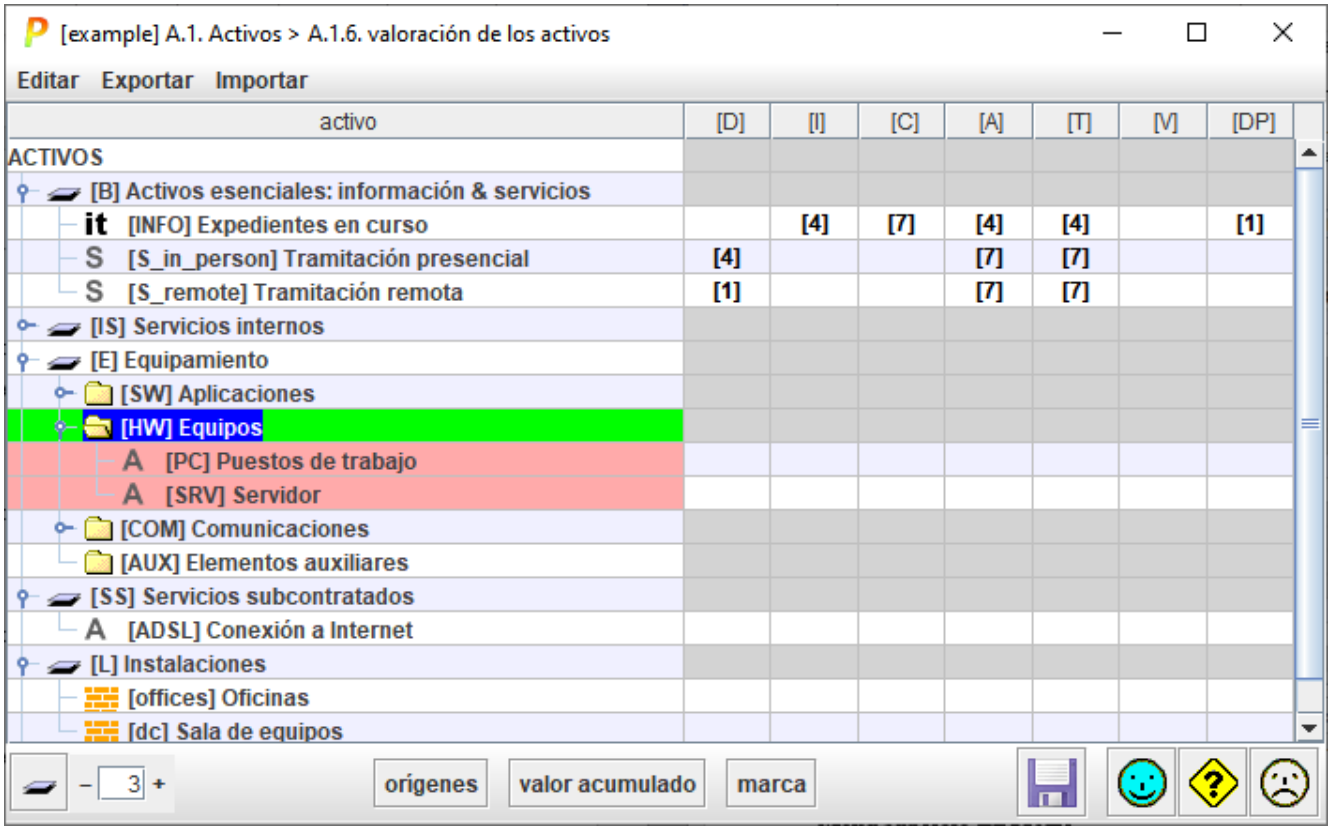
Esta pantalla se emplea para valorar activos individuales y para analizar el valor propagado entre activos.

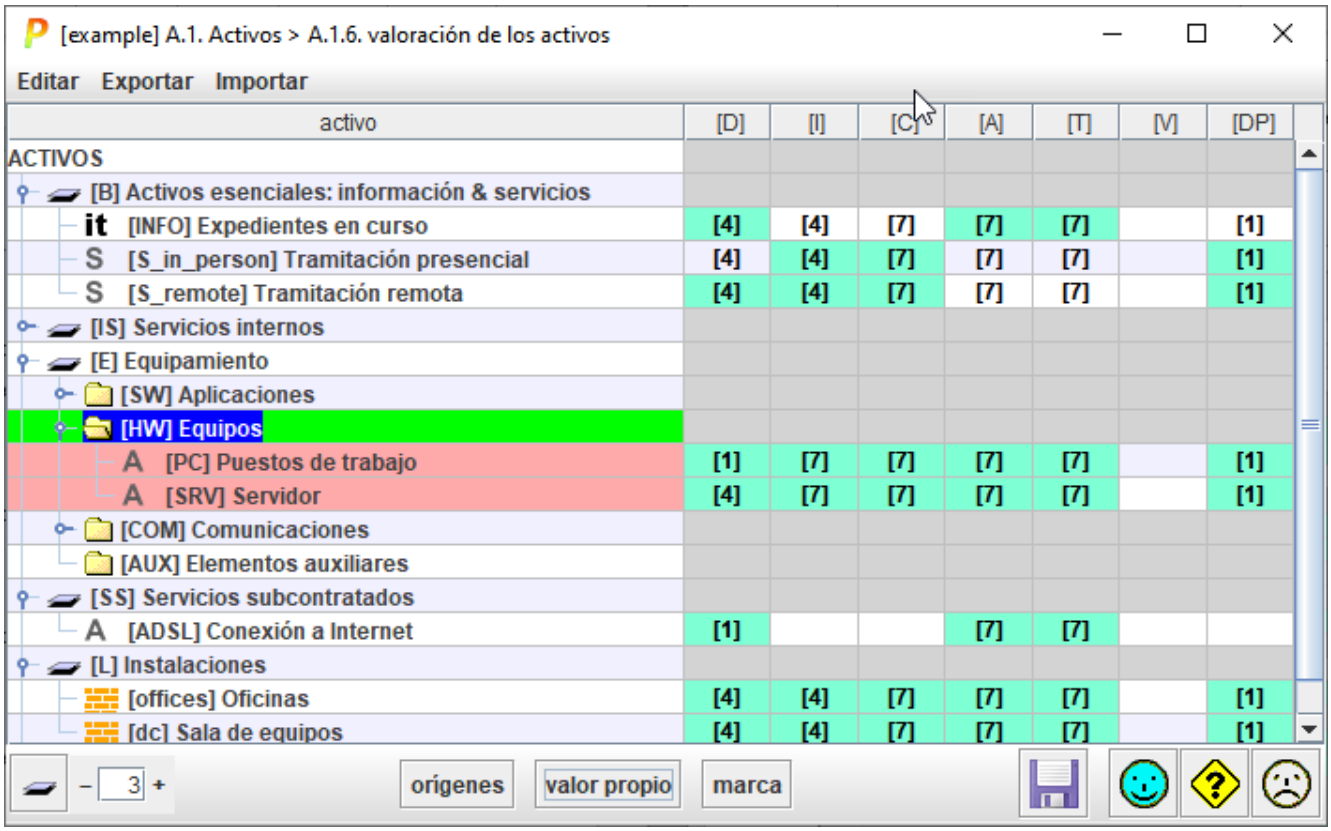
Para empezar rápidamente
¿Cuál es su principal preocupación respecto de este sistema de información? • Seleccione un activo (la fila) • seleccione una dimensión de seguridad (la columna)

- haga doble clic para seleccionar un valor entre 0 (insignificante) y 10 (absolutamente crítico) … o algún valor intermedio.

Repita los pasos anteriores con la demás preocupaciones en orden decreciente hasta que considere que el resto de asuntos no son tan importantes.

Haga clic en **ACUMULADO** para estudiar la propagación del valor de los activos superiores hacia los inferiores. Conviene realizar una comprobación de que cada activo tiene un valor con sentido.





Menú superior EDITAR

	Seleccione una o más celdas. Copie lo valores para pegarlos más tarde.
	Seleccione una o más celdas de destino. Pegue los valores que antes copió. Si el original era una celda y el destino son varias, se repite el valor.

Menú superior EXPORTAR

CSV	CSV – comma separated values; para excel
XML	XML – extensible markup language

Menú superior IMPORTAR

XML	XML – extensible markup language

Tabla – Tantas columnas como dimensiones de seguridad.

Para cada activo esencial y cada dimensión de seguridad, el valor

- Ver *Activos / Valoración / cualitativo*
- Ver *Activos / Valoración / cuantitativo*

Para cada activo y cada dimensión de seguridad.

Cuando se presenta el valor propio, el valor aparece sobre fondo blanco

[D]	[I]	[C]	[A]	[T]
	[4]	[7]	[4]	[4]
[4]			[7]	[7]
[1]			[7]	[7]

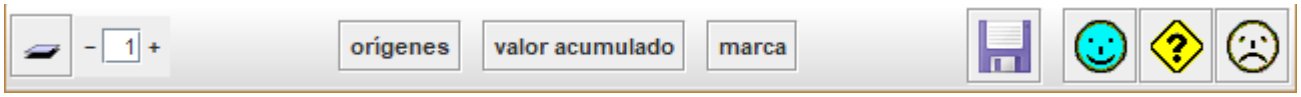
Cuando se presenta en valor acumulado, aparece sobre fondo verdoso

[D]	[I]	[C]	[A]	[T]
[4]	[4]	[7]	[7]	[7]
[4]	[4]	[7]	[7]	[7]
[4]	[4]	[7]	[7]	[7]

Cuando el análisis de riesgos es cuantitativo, los valores son cantidades numéricas:

	47K	100K	47K	47K
47K	47K	100K	260K	147K
10K	47K	100K	260K	147K

Barra inferior



	Haga clic para recoger el árbol de activos
	Controla el nivel de despliegue del árbol de activos
fuentes	Seleccione una fuente. PILAR seleccionará los activos que están asociados a dicha fuente.
valor acumulado / propio	Conmuta entre presentar solo el valor propio, o acompañarlo del valor acumulado.
marcar	Útil para ver cómo se propaga el valor. Seleccione una celda y haga clic en MARCAR. El valor fuente se marca sobre fondo verde. Los destinos de ese valor se marcan sobre fondo negro. Por ejemplo, para ver a dónde se propaga el valor de trazabilidad: 

	Guarda el proyecto en su fichero o en su base de datos.

La columna izquierda cubre los activos (organizados en capas y grupos). Puede ser extendida y recogida.

Las otras columnas cubren dimensiones de seguridad. Solamente los activos pueden recibir valores; las otras filas están muertas.

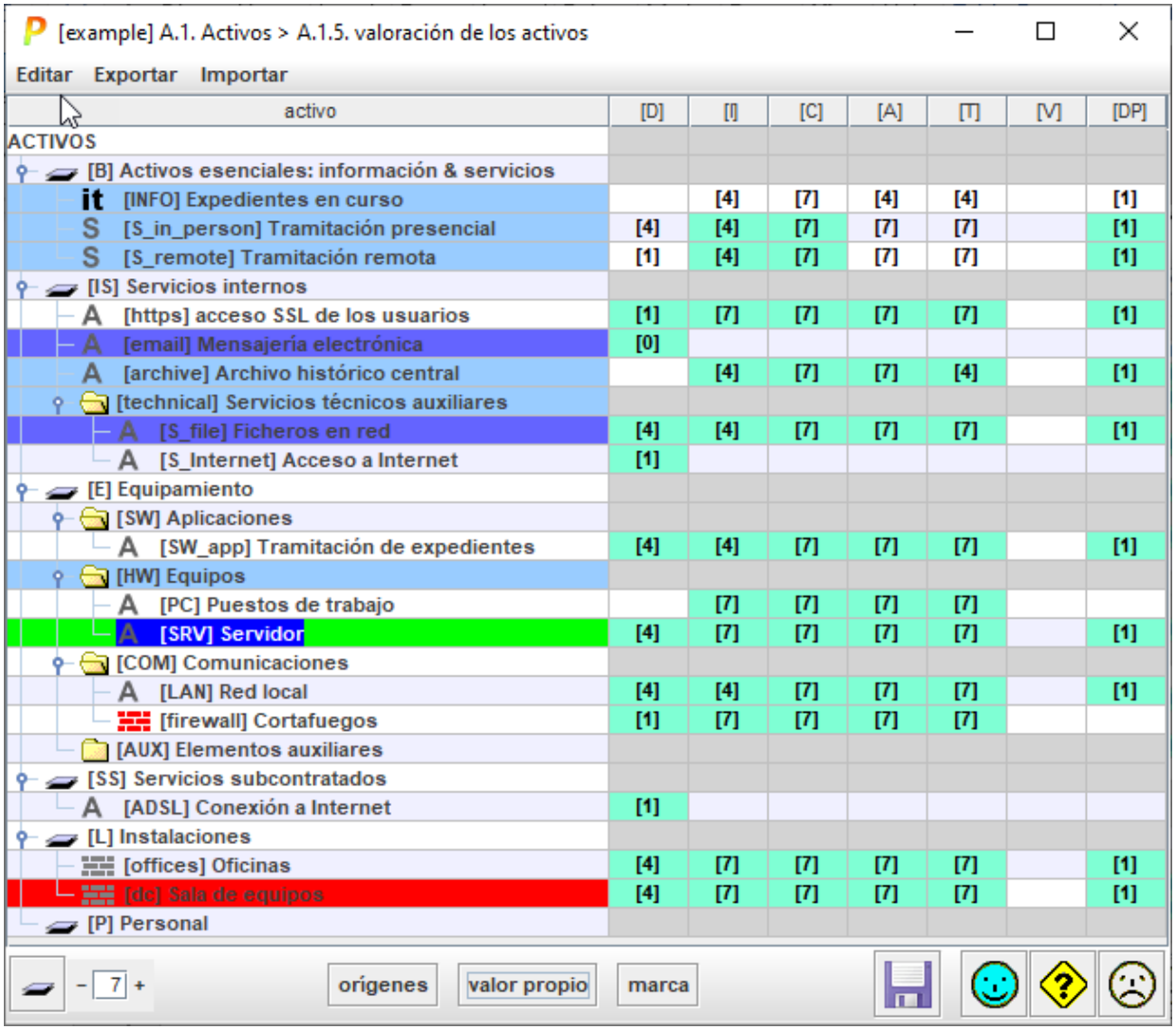
La pantalla permite a

- [para el análisis cuantitativo] introducir un valor numérico
- para introducir un comentario que explica por qué este valor
- para seleccionar los criterios que se aplican de ésos en la biblioteca.
  Es importante intentar utilizar criterios codificados.

Para descubrir de dónde llega el valor que se acumula en un activo:

- seleccione el activo (una fila)
- clic ORÍGENES

También puede seleccionar un activo y automáticamente se muestra qué activos están por encima y cuales por debajo en el árbol de dependencias:



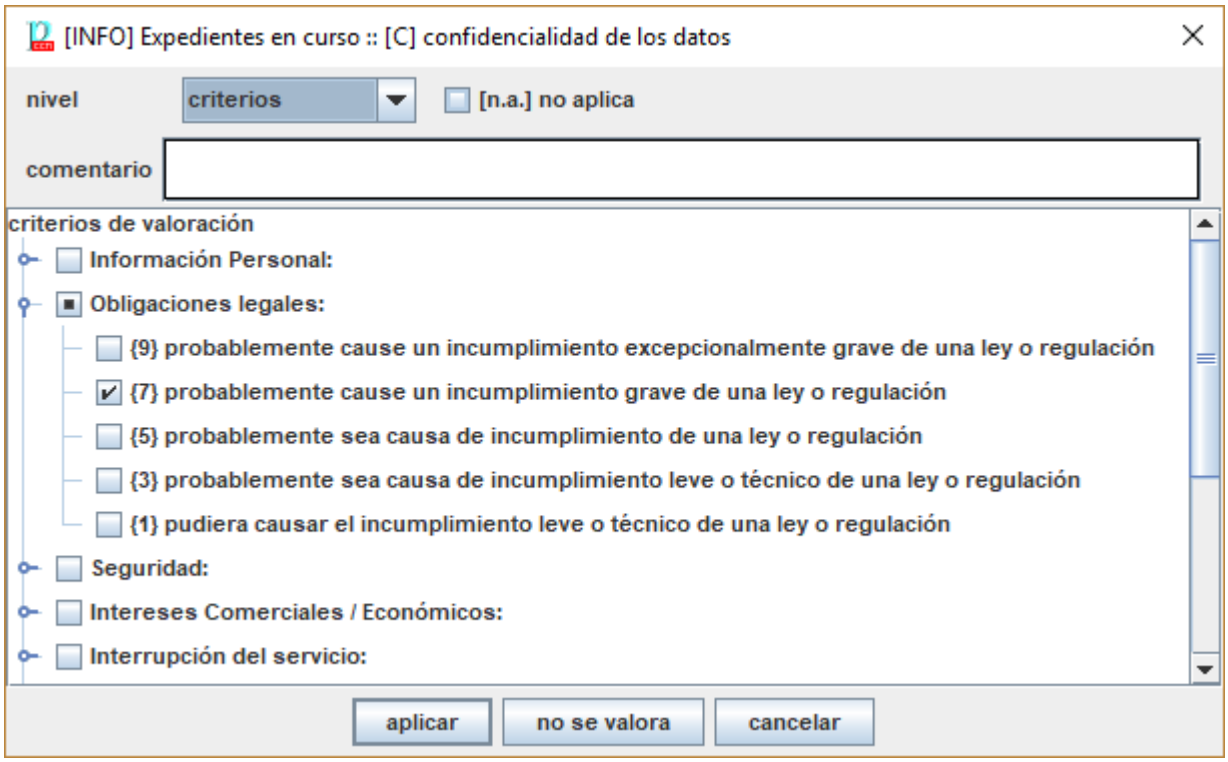
8.7.3 Valoración cualitativa

Una opción rápida (atajo) es usar las combinaciones de teclas CTRL+ o CTRL- para incrementar / decrementar el valor en una cierta dimensión.

Como alternativa, haciendo clic-clic se abre una ventana para incluir valores, comentarios y documentar criterios.

Para asignar un valor a un activo

- seleccione un activo (fila) y dimensión (columna)
- clic-clic



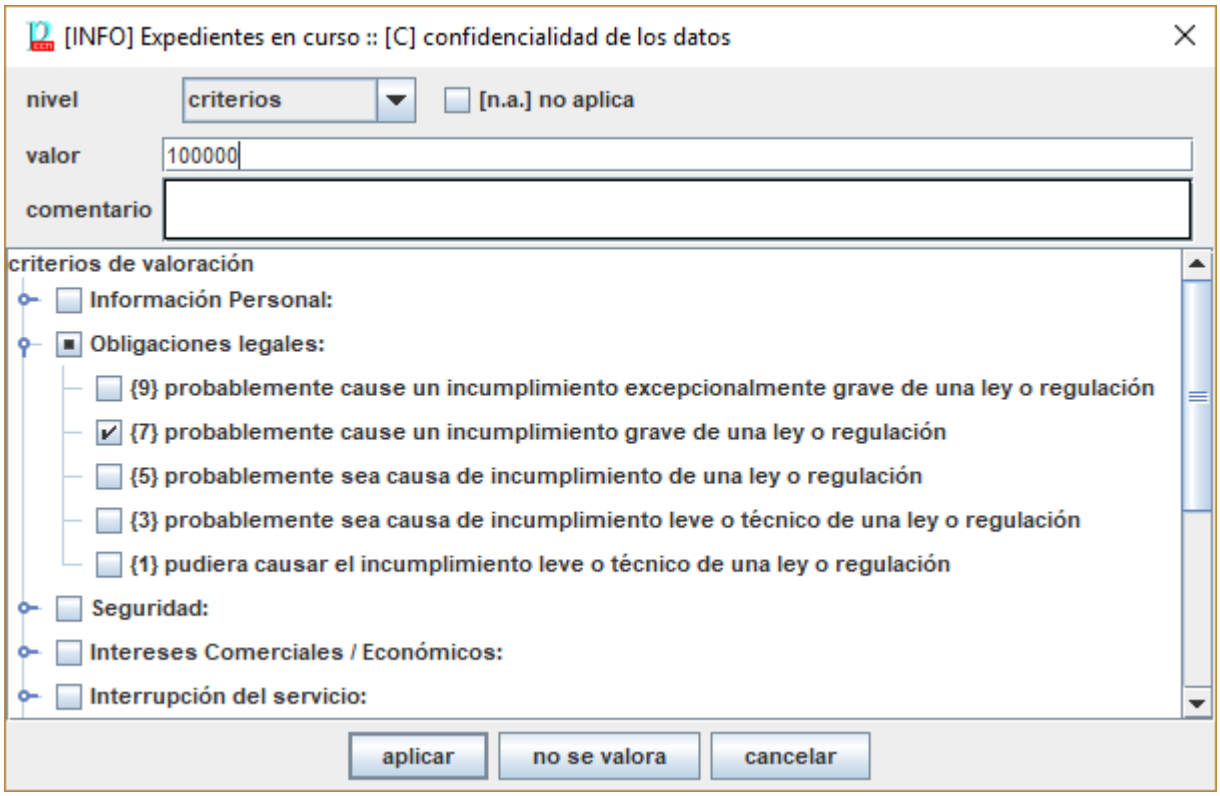
combo nivel	Si selecciona “CRITERIOS”, el valor lo decide la marca de mayor valor de los criterios marcados en el panel. Si selecciona un nivel, este será el asignado al activo, independientemente de los criterios marcados.
[n.a.]	Se marca N.A. cuando esa dimensión no tiene relevancia ni para ese activo ni propaga su valor a los activos de los que depende. Ver “*Anulación de una valoración*”.
comentario	Un comentario para explicar el porqué de la valoración
panel	Criterios para valorar un activo
aplicar	Aplica el valor y cierra la ventana
no se valora	Elimina el valor del activo y cierra la ventana
cancelar	Cierra la ventana sin modificar la valoración del activo

8.7.4 Valoración cuantitativa

Muy similar a la valoración cualitativa pero, además, se puede asignar una cantidad.

Para asignar un valor a un activo

— seleccione un activo (fila) y dimensión (columna)
— clic-clic

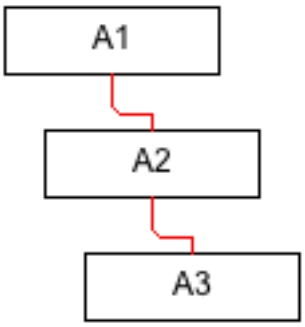


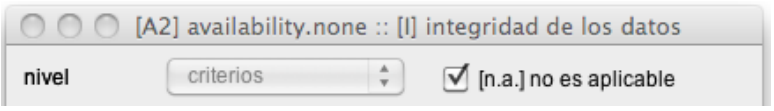
combo nivel	Marca el valor cualitativo. Si selecciona "CRITERIOS", el valor lo decide la marca de mayor valor de los criterios marcados. Si selecciona un nivel, este será el asignado al activo, independientemente de los criterios marcados.
[n.a.]	Se marca N.A. cuando esa dimensión no tiene relevancia ni para ese activo ni propaga su valor a los activos de los que depende. Ver "*Anulación de una valoración*".
valor	Marca el valor cuantitativo.
comentario	Un comentario para explicar el porqué de la valoración
panel	Criterios para valorar un activo
aplicar	Aplica el valor y cierra la ventana
no se valora	Elimina el valor del activo y cierra la ventana
cancelar	Cierra la ventana sin modificar la valoración del activo

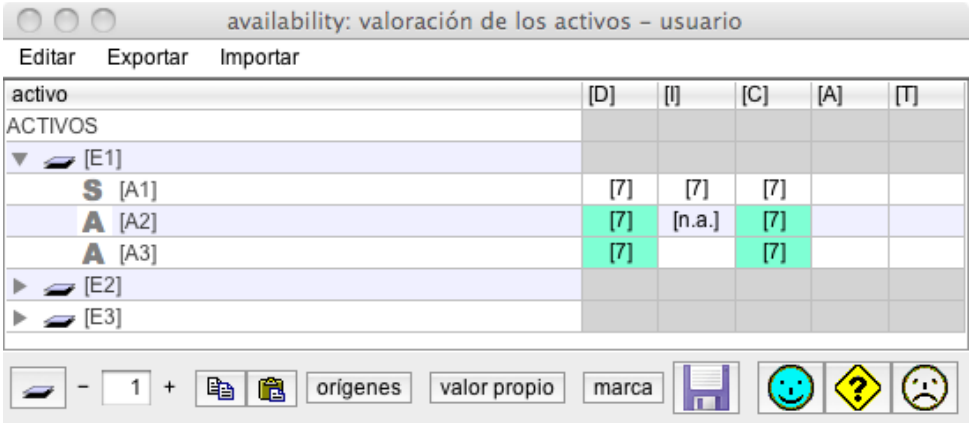
Cuando PILAR conoce solo una valoración cualitativa o solo una valoración cuantitativa, recurre a la tabla de valores-niveles (ver personalización, https://www.ar-tools.com/doc/) para estimar el valor que falta.

8.7.5 Anulación de una valoración

Los activos acumulan la valoración de sus superiores (por dependencias). Si nos interesa anular la valoración en un cierto activo, e impedir que se siga propagando a los activos inferiores (por dependencias), en la pantalla de determinación del nivel de valoración, seleccione N.A.







El efecto es similar a ajustar la matriz de transferencia de valor por dependencias de los activos que contribuyen al valor acumulado que queremos anular.

8.7.6 Valoración de la disponibilidad

La valoración de la disponibilidad se puede ajustar de varias maneras:

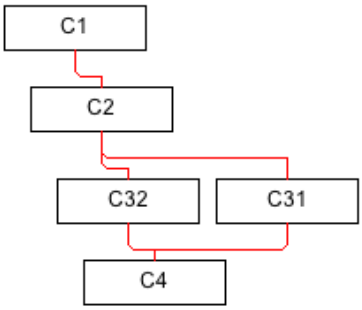
- por *dependencias*,
- por *anulación* del valor,
- ajustando algunos calificativos del activo (ver a continuación).

Si el activo está marcado como "[availability.easy]", entonces la valoración del activo en disponibilidad se reduce en un orden de magnitud (3 niveles en la escala de valoración por niveles). Este ajuste se reflejará en la valoración del impacto de las amenazas. Esta reducción de valor es local, sin afectar al valor que se propaga.

Si el activo está marcado como "[availability.none]", entonces la valoración del activo en disponibilidad se reduce a cero. Este ajuste se reflejará en la valoración del impacto de las amenazas. Esta reducción de valor es local, sin afectar al valor que se propaga.

Si el activo se marca como “[or]”, y depende de más de 1 hijo, la disponibilidad no se propaga a los hijos, ni a los activos siguientes en la cadena de transferencia. No obstante, si al avanzar en la cadena de transferencia las diferentes ramas convergen en un activo común, el valor de disponibilidad surge de nuevo. De esta forma se obvia la valoración en activos alternativos, pero se detectan puntos únicos de fallo.

El siguiente ejemplo muestra cómo los equipos redundantes C31 y C32 no se valoran en disponibilidad, mientras que el activo común, C4, recupera el valor. Nótese que otras dimensiones no se ven afectadas por la calificación como OR.



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[E1]					
[E2]					
[E3]					
S [C1]	[7]		[7]		
A [C2] OR	[7]		[7]		
A [C31]			[7]		
A [C32]			[7]		
A [C4]	[7]		[7]		

8.8 Zonas

Los sistemas de información pueden estar protegidos por fronteras que separan los activos internos de los externos. Ej. un firewall separa el mundo externo de los activos internos. Las fronteras son elementos de defensa importantes donde se puede impedir que atacantes externos lleguen a los activos internos. Necesitamos identificar zonas y conexiones entre zonas (también conocidas como interconexiones)

Zona

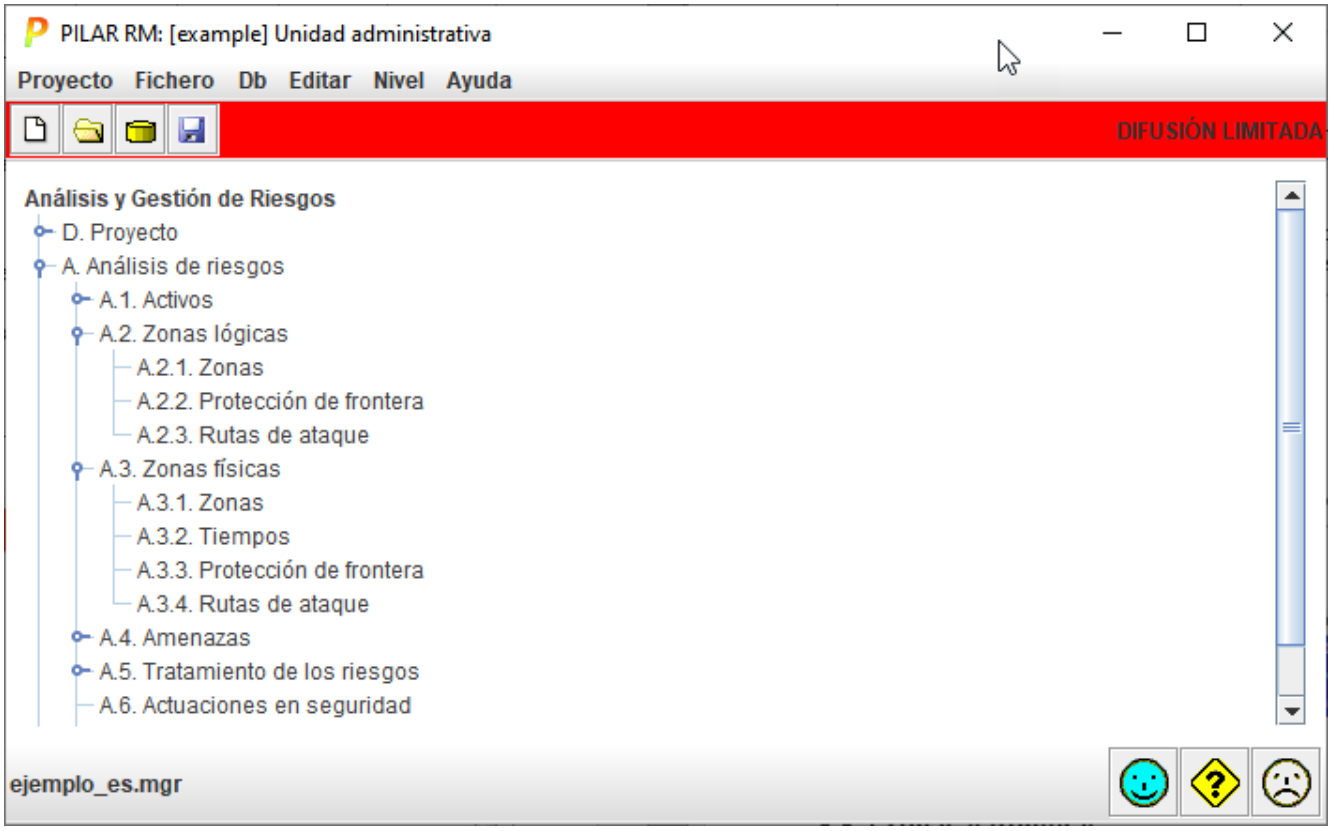
> Una zona se refiere a un conjunto de activos que gestionan cierta información. Es crucial salvaguardar el flujo de información entre zonas para evitar el acceso no autorizado o la transmisión de códigos maliciosos.

Conexión entre zonas

> La interconexión entre zonas se ve facilitada por un conjunto de dispositivos diseñados para proporcionar servicios integrales de protección de los intercambios de información entre las zonas interconectadas. Las fronteras regulan los flujos de información entrantes y salientes.

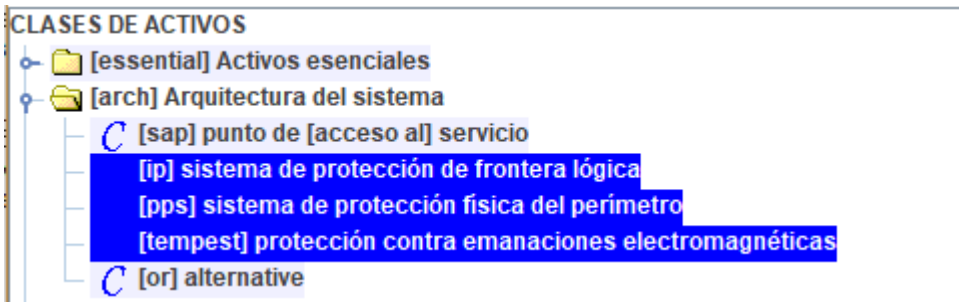
Cuando el sistema TIC incluye activos de interconexión (por ejemplo, un cortafuegos), PILAR valora un conjunto de salvaguardas para proteger la frontera:

La gestión de zonas es parte del análisis de riesgos:



8.8.1 Clases de activos

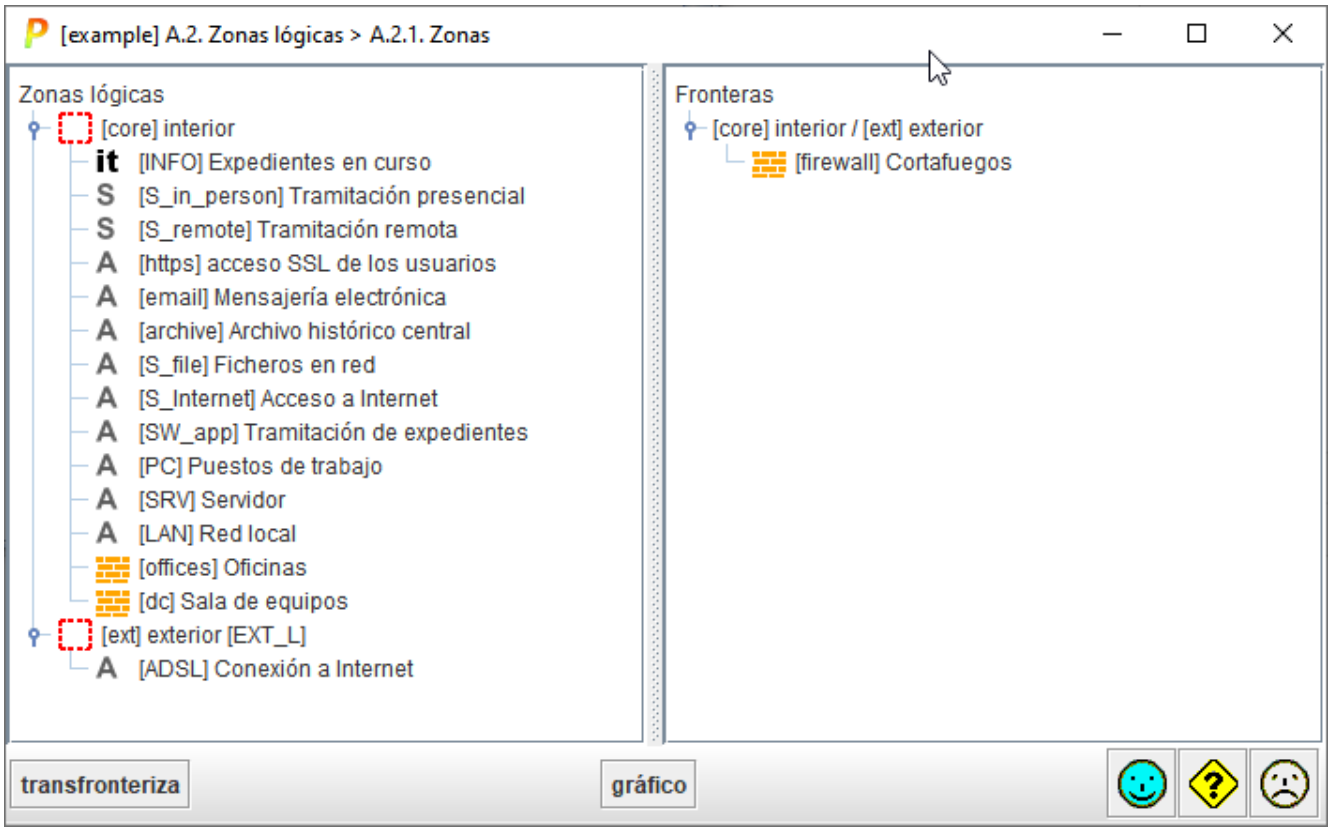
PILAR sabe que hay zonas cuando aparecen activos calificados como de defensa perimetral



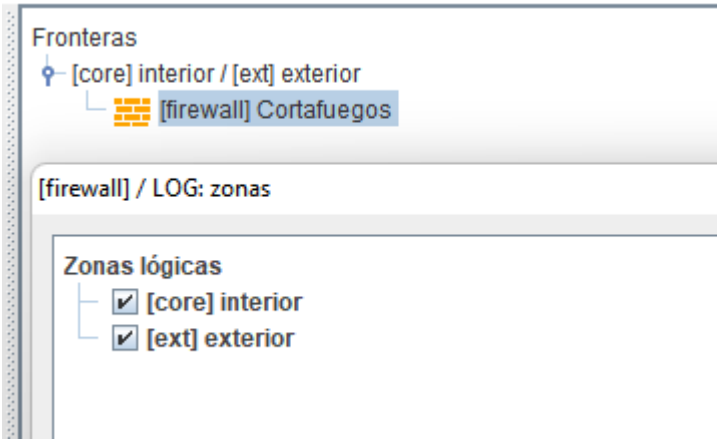
8.8.2 Zonas y fronteras

Se pueden organizar zonas alrededor de las fronteras o perímetros, diferenciando entre lo que está a un lado y lo que está al otro.

Lo más estándar es diferenciar entre lo que está dentro y lo que está fuera, alrededor de los elementos de frontera



y podemos ir arrastrando activos del interior bien a otras zonas o a la frontera.



Tenga en cuenta que un activo que está en una zona A no puede estar simultáneamente en otra zona B, salvo que sea el activo frontera. Un activo de frontera puede estar entre varias zonas.

Con el botón derecho en la raíz “zonas lógicas”, puede crear nuevas zonas y también usar en wizard de PILAR para una disposición estándar de activos alrededor de los marcados como frontera.

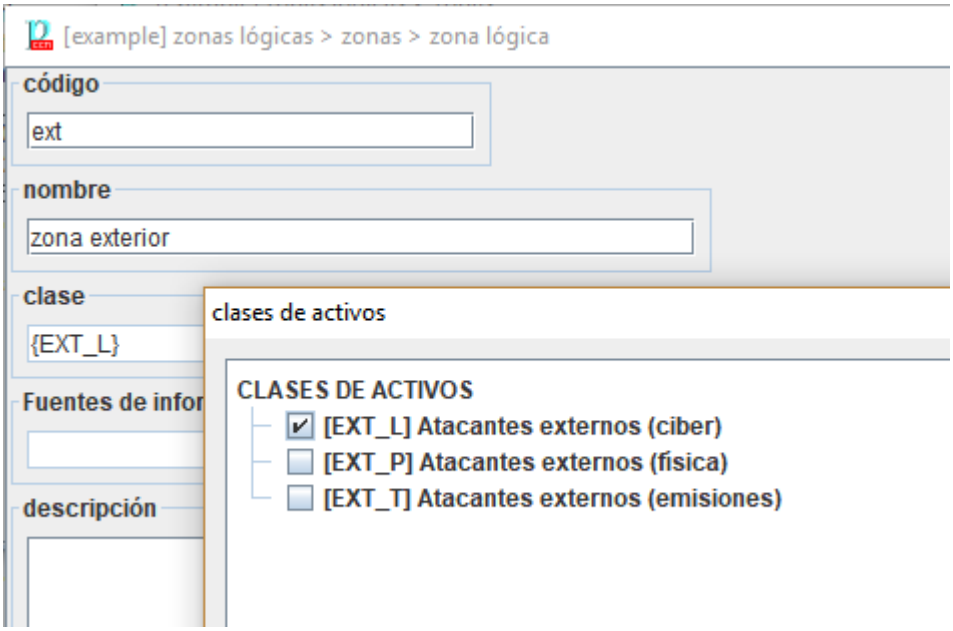
Con el botón derecho en una zona lógica, puede editarla y también crear nuevas zonas.

Con el botón derecho en un activo puede editarlo, que quiere decir marcar en qué zonas está. En este caso, cuando un activo lo queremos en la frontera, debe marcar las zonas (2 o más) que separa esa frontera.

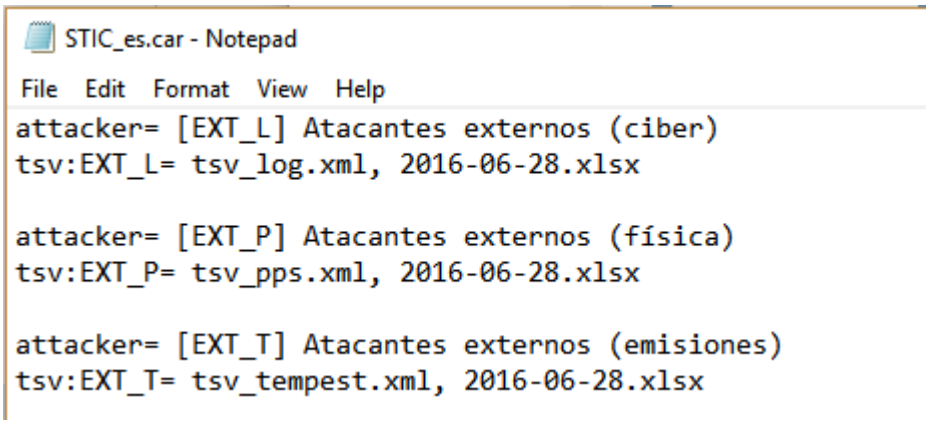
8.8.3 Definición de zonas

Cuando crea o cuando edita una zona puede determinar varios elementos tales como su código (único) un nombre descriptivo, fuentes de información que pueden condicionar su acceso.

Y, en particular, puede indicar la clase de atacantes que pueden iniciar ataques desde esa zona:



Los perfiles de ataque se describen con medio de ficheros TSV que se indican en la configuración .CAR



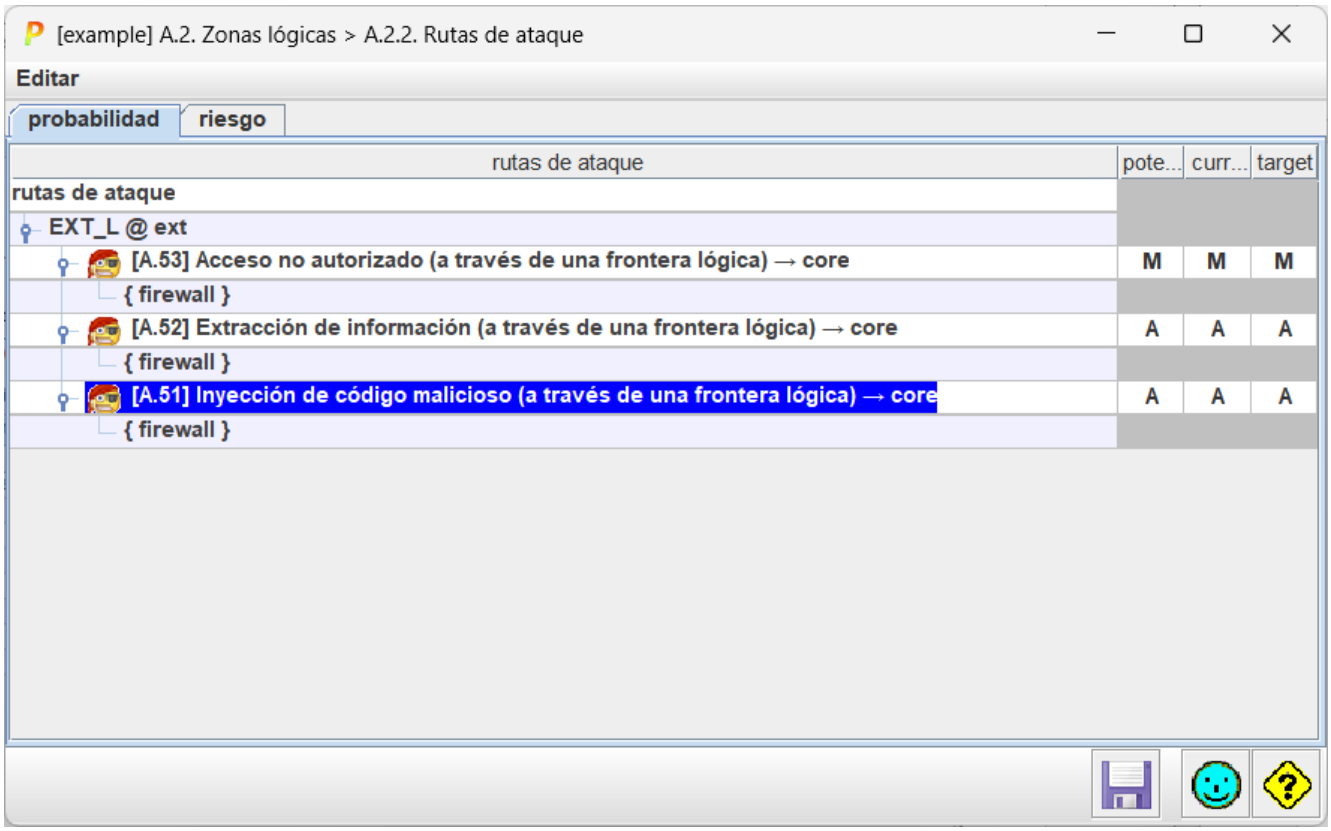
Para un atacante lógico como es EXT_L, su capacidad de ataque sobre los elementos de frontera lógica se definen en el fichero tsv_log.xml. Una vez dentro, su capacidad de ataque es la descrita en 2016-06-28.xlsx.

8.8.4 Rutas de ataque

Actualmente solo para fronteras lógicas.

Se trata de una pantalla de presentación de datos calculados por PILAR: ru.tas que pueden seguir los atacantes desde la zona origen hasta la zona atacada.

Primero, la probabilidad de que el ataque tenga éxito



Que se lee de la siguiente manera:

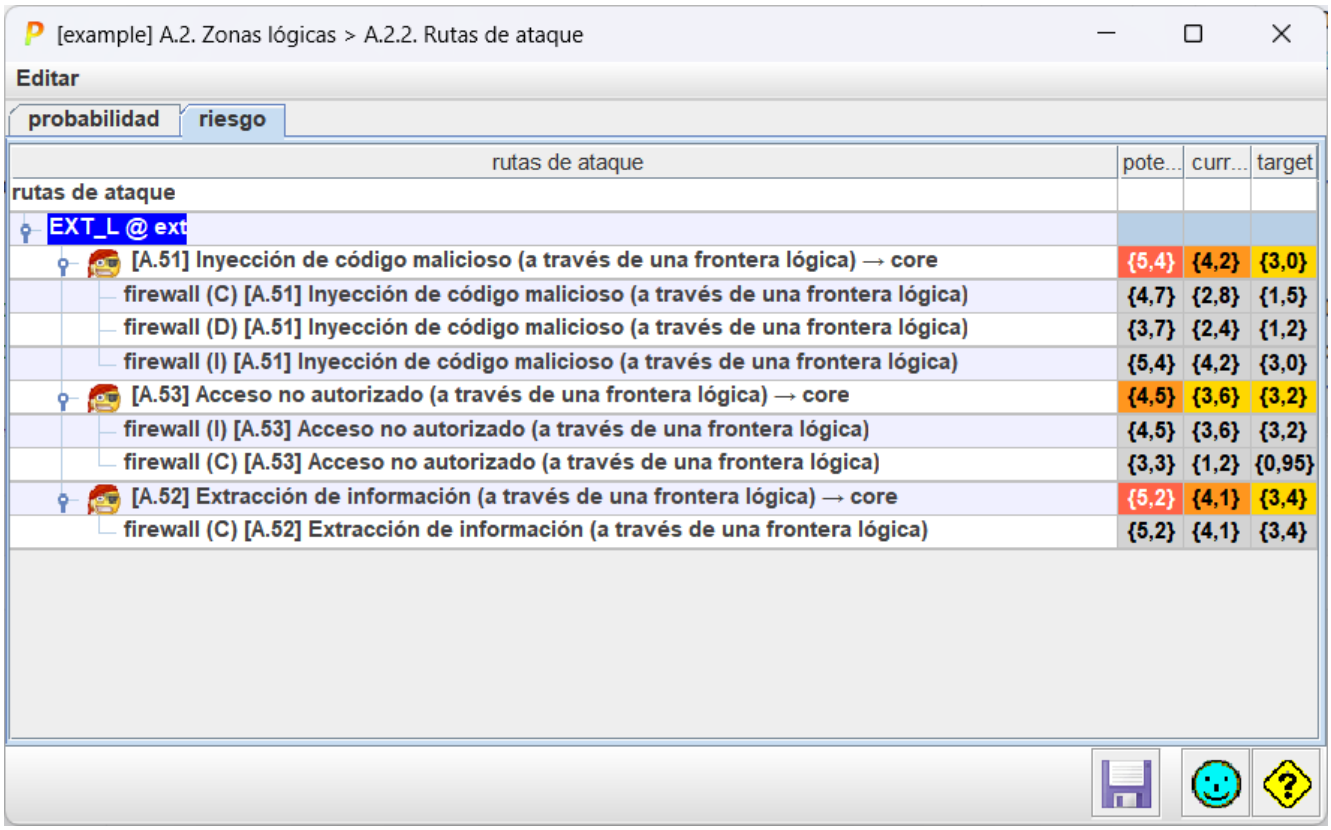
Fila 1

Para atacantes externos de tipo EXT_L en la zona ext

Fila 2 (y 4 y 6)

Por medio de la amenaza A.51, el atacante puede inyectar código dañino a través del dispositivo de frontera “firewall” (fila 3) en la zona core.

y en otra tabla, las consecuencias (riesgo) derivado de estos ataques:



En el ejemplo se muestran las opciones de un atacante externo, EXT_L, situado en la zona [ext]. Tiene tres opciones,

- practicar la amenaza [A.52] y salir de la zona [core] atravesando el activo de frontera, [firewall], lo que tiene consecuencias sobre la confidencialidad de los activos en la zona [core]
- practicar la amenaza [A.53] y entrar a la zona [core] atravesando el activo de frontera [firewall], lo que tiene consecuencias sobre la integridad y confidencialidad de los activos en la zona [core]
- practicar la amenaza [A.51] y entrar de la zona [core] atravesando el activo de frontera, [firewall]], lo que tiene consecuencias sobre la disponibilidad, integridad y confidencialidad de los activos en la zona [core]

Para cada amenaza tiene una probabilidad de éxito, especificada en el TSV asociado en el fichero .CAR para el perfil EXT_L.

Esta probabilidad potencial se ve mitigada por las salvaguardas de protección perimetral que se despliegan en cada fase del proyecto.

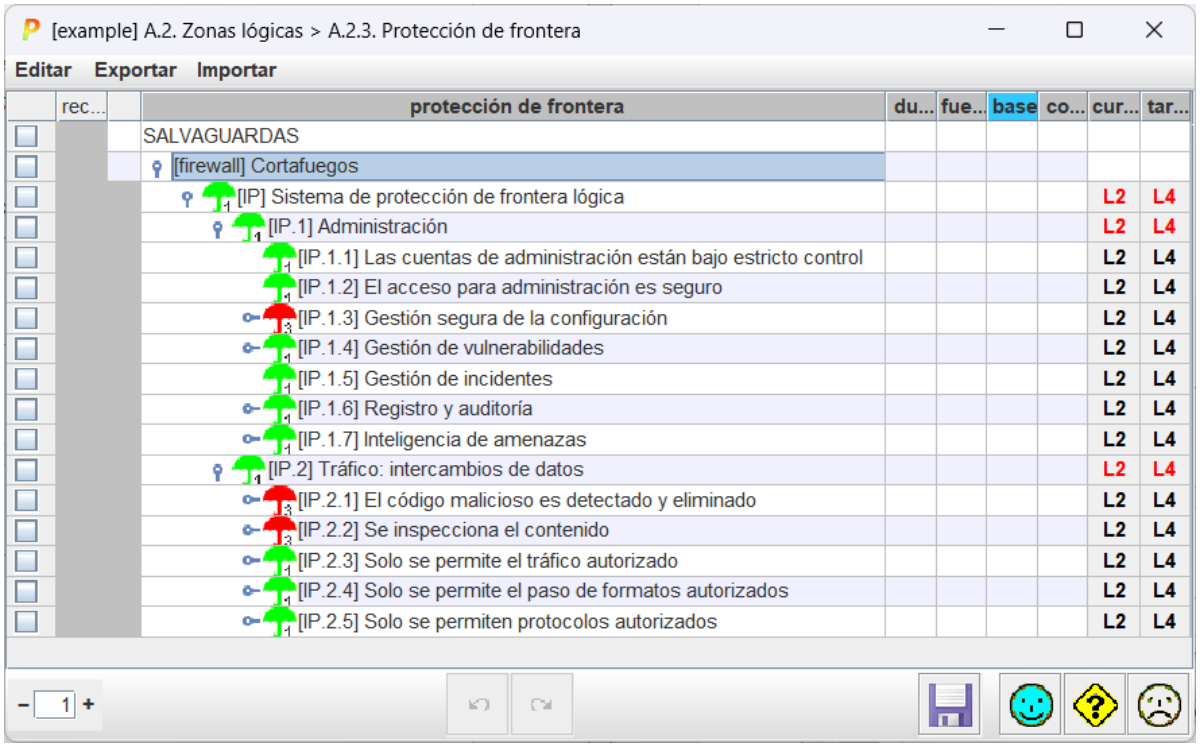
Una vez dentro, el atacante puede practicar otras amenazas sobre los activos del interior, siempre siguiendo lo especificado por los TSV para este perfil de ataque.

8.8.5 Protección de la frontera

Actualmente solo para fronteras lógicas.

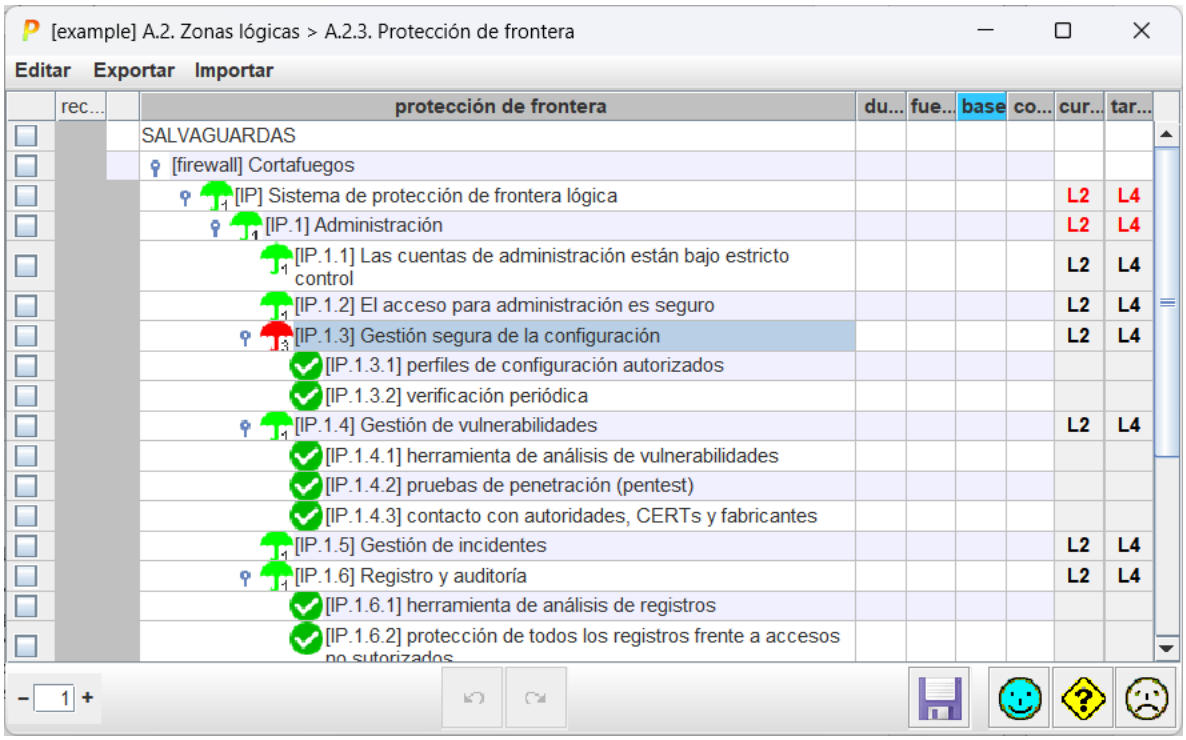
Aquí se especifican medidas de seguridad para proteger la frontera.

La pantalla es similar a la de salvaguardas (ver). Para cada activo de la frontera:



Las medidas de seguridad se organizan en 2 niveles:

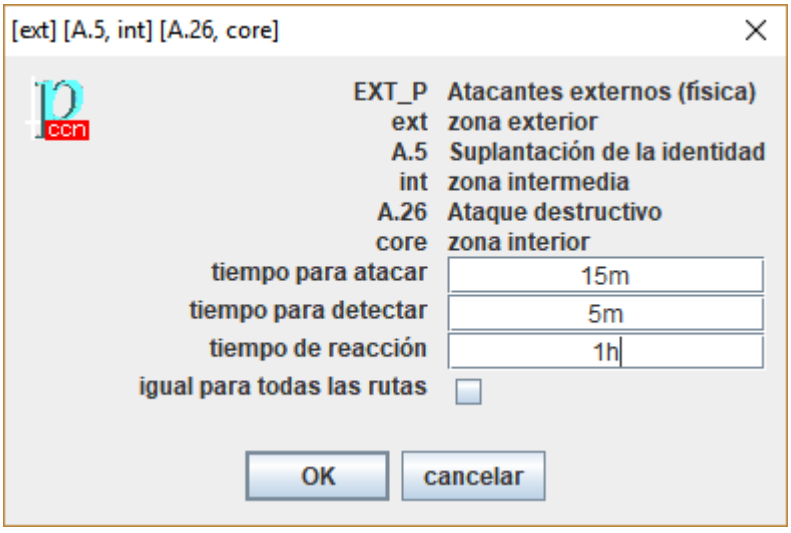
- Nivel de acción (paragüitas), donde se valora la madurez del mecanismo protector, valoración que se usara para mitigar las amenazas
- Nivel de documentación (discos verdes), donde se presentan elementos que se pueden valorar pero cuya valoración NO se emplea para mitigar riesgo, sino simplemente para justificar o explicar la valoración de los elementos de acción correspondientes.



8.8.6 Análisis de tiempos

Este análisis solamente se realiza para ataques físicos. Se trata de comparar el tiempo que tarda el atacante en atravesar el perímetro frente a los tiempos que tarda el defensor en detectarlo y reaccionar.

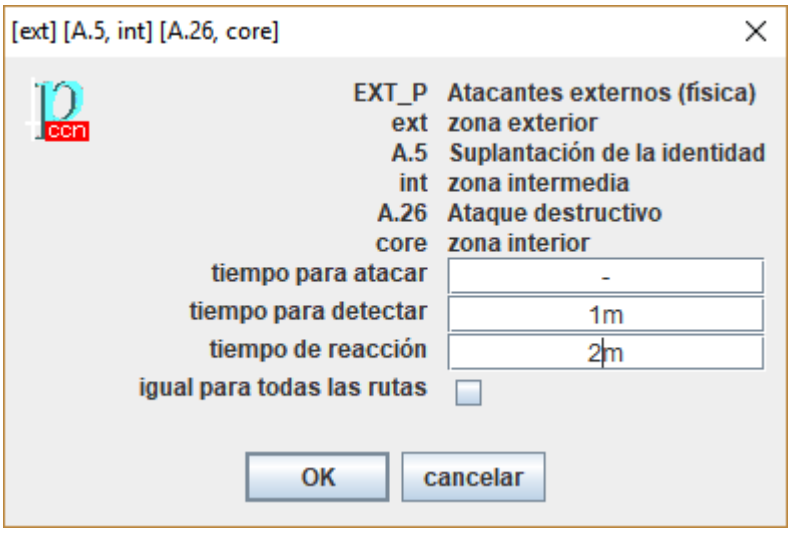
Veamos un ejemplo. Hay 3 zonas: exterior, intermedia e interior. Hay un atacante exterior que intenta llegar al interior. El atacante requiere 10 min. El sistema de protección perimetral tarda 5 min en detectar el ataque y la reacción requiere 1 hora.



En este escenario tenemos un problema y es que el atacante es más rápido

attacker	rutas de ataque	current	target
EXT_P @ ext			
EXT_P @ ext	[A.5, int]	- < - + -	- < - + -
EXT_P @ ext	[A.5, int][A.26, core]	15m < 5m + 1h	15m < 5m + 1h
EXT_P @ ext	[A.5, int][A.5, core]	- < 5m + 1h	- < 5m + 1h
EXT_P @ ext	[A.26, int]	- < - + -	- < - + -
EXT_P @ ext	[A.26, int][A.26, core]	- < 5m + 1h	- < 5m + 1h
EXT_P @ ext	[A.26, int][A.5, core]	- < 5m + 1h	- < 5m + 1h

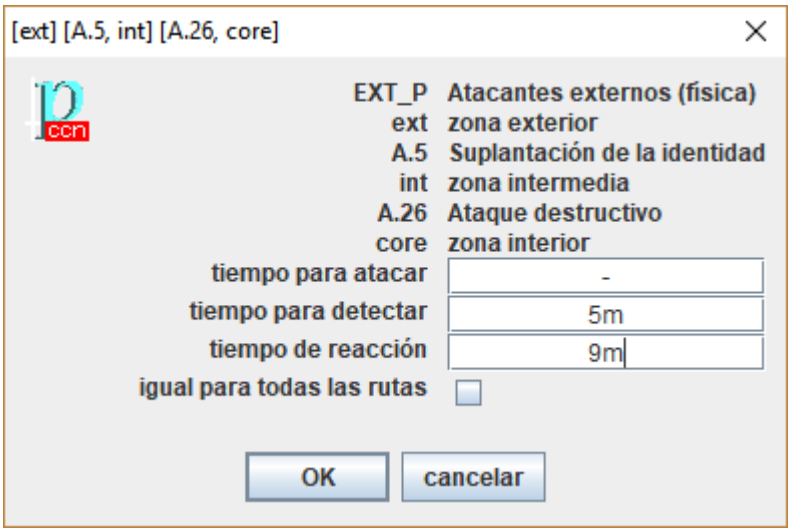
Si mejoramos nuestra respuesta en la fase objetivo



el ataque queda conjurado

attacker	rutas de ataque	current	target
EXT_P @ ext			
EXT_P @ ext	[A.5, int]	- < - + -	- < - + -
EXT_P @ ext	[A.5, int][A.26, core]	15m < 5m + 1h	15m > 1m + 2m
EXT_P @ ext	[A.5, int][A.5, core]	- < 5m + 1h	- < 1m + 2m
EXT_P @ ext	[A.26, int]	- < - + -	- < - + -
EXT_P @ ext	[A.26, int][A.26, core]	- < 5m + 1h	- < 1m + 2m
EXT_P @ ext	[A.26, int][A.5, core]	- < 5m + 1h	- < 1m + 2m

Pudiera ser que el tiempo de detección y respuesta estuviera muy apurado y es arriesgado



attacker	rutas de ataque	current	target
EXT_P @ ext			
EXT_P @ ext	[A.5, int]	- < - + -	- < - + -
EXT_P @ ext	[A.5, int][A.26, core]	15m < 5m + 1h	15m > 5m + 9m
EXT_P @ ext	[A.5, int][A.5, core]	- < 5m + 1h	- < 5m + 9m
EXT_P @ ext	[A.26, int]	- < - + -	- < - + -

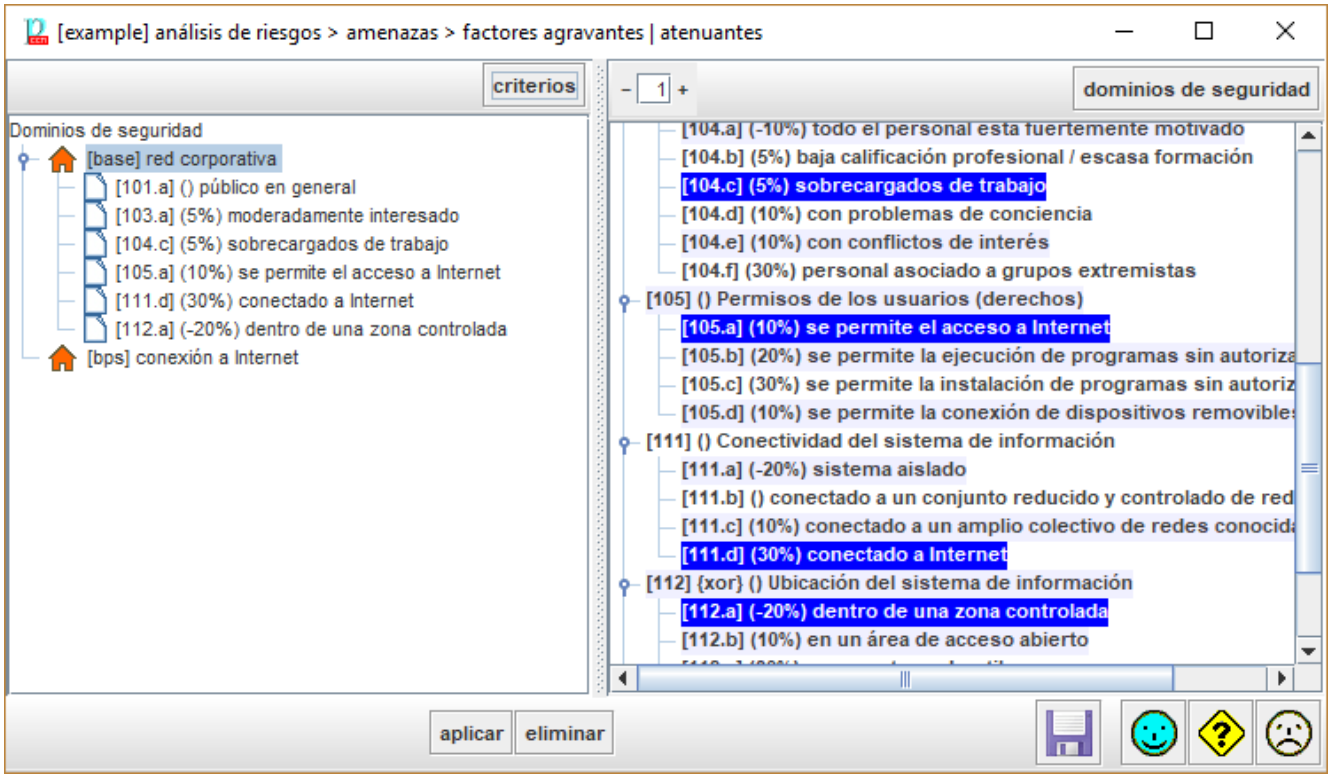
Las rutas en las que hay suficiente margen entre la velocidad del ataque y de la respuesta, desaparecen como riesgo, manteniéndose aquellas en las que no hay velocidad suficiente.

8.9 Amenazas

8.9.1 Factores agravantes | atenuantes

La pantalla permite adjudicar una serie de calificativos a los dominios, calificativos que serán utilizados para establecer el perfil de vulnerabilidad; es decir, para ajustar el perfil de amenazas posibles.

Si modifica esta ventana, no olvide re-aplicar la biblioteca, u otro fichero TSV (ver "*Valoración de las amenazas*). Un TSV se aplica automáticamente si se ha puesto en modo automático (ver "*Opciones / Amenazas*").



Barra superior

criterios	Seleccione un dominio de seguridad a la izquierda. Haga clic en CRITERIOS. PILAR presenta a la derecha los criterios que se aplican en el dominio seleccionado.
– 1 +	Controla el despliegue del árbol de criterios.
dominios	Seleccione un criterio a la derecha. Haga clic en DOMINIOS DE SEGURIDAD. PILAR selecciona a la izquierda los dominios a los que se aplica el criterio.

Barra inferior

aplicar	Seleccione uno o más dominios de seguridad a la izquierda. Seleccione uno o más dominios de seguridad a la derecha. Haga clic en APLICAR. PILAR aplica los criterios seleccionados a los dominios seleccionados.
eliminar	Seleccione uno o más dominios de seguridad a la izquierda. Seleccione uno o más dominios de seguridad a la derecha. Haga clic en ELIMINAR. PILAR retira los criterios seleccionados de los dominios seleccionados.
	Guarda el proyecto en su fichero o en su base de datos.

Para asociar una vulnerabilidad a un dominio

- seleccione el dominio (izquierda)
- seleccione una o más vulnerabilidades (derecha)
- clic en APLICAR

Para eliminar una vulnerabilidad de un dominio

- seleccione la vulnerabilidad (izquierda)
- clic ELIMINAR

Para descubrir las vulnerabilidades asociadas a un dominio

- seleccione el dominio (izquierda)
- clic CRITERIOS (panel izquierdo, barra superior)

Para descubrir a qué dominios aplica una cierta vulnerabilidad

- seleccione la vulnerabilidad (derecha)
- clic DOMINIOS (panel derecho, barra superior)

8.9.2 Identificación

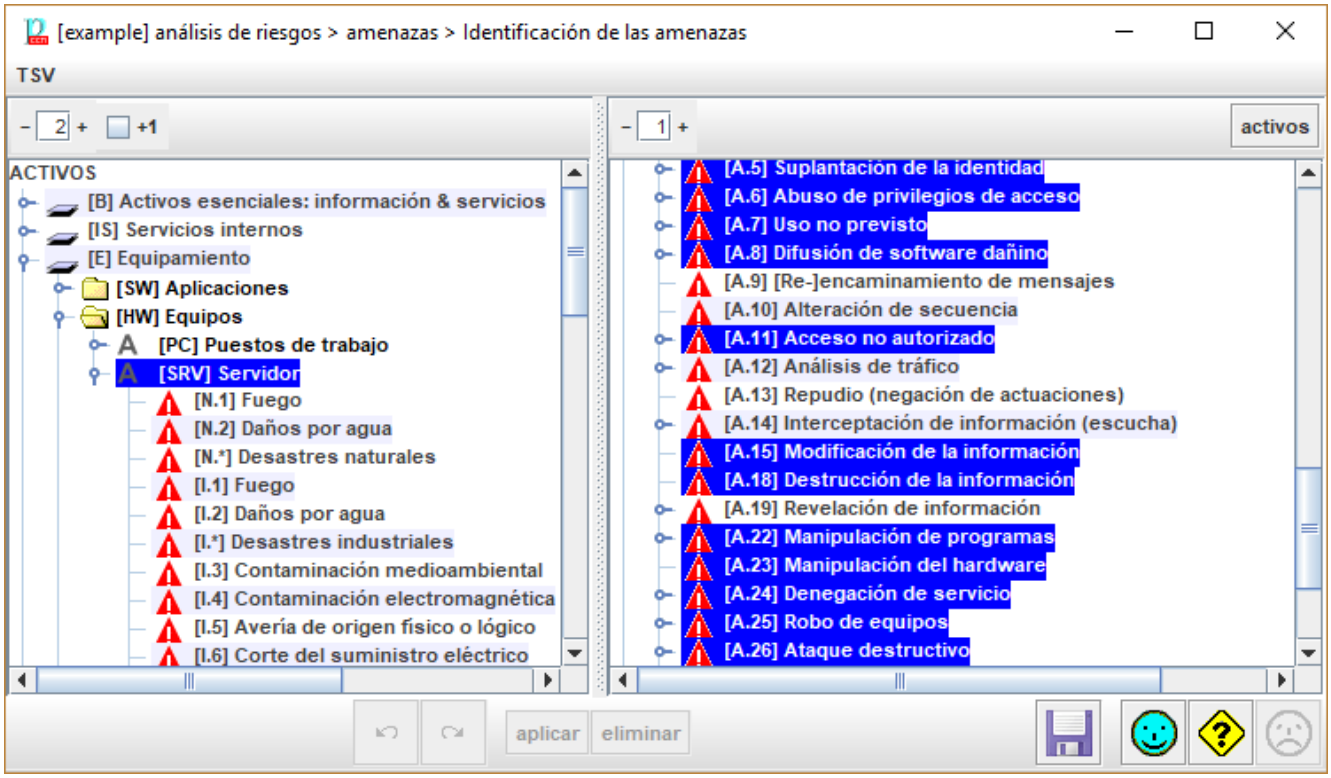
Para empezar rápidamente
Seleccione amenazas automáticas en *Opciones / Amenazas* PILAR aplica las amenazas no opcionales en el TSV.

No tan rápido
Seleccione amenazas MIX en *Opciones / Amenazas* PILAR empieza aplicado las amenazas no opcionales en el TSV. Puede añadir o retirar amenazas. Como ayuda, haga clic con el botón derecho y seleccione.

Identificamos qué amenazas son posibles para cada activo. Más adelante determinaremos la probabilidad de ocurrencia y la degradación causada en el activo.

NOTA. Si está en modo automático (*Opciones / Amenazas*) entonces algunos botones aparecen inhabilitados:

- copiar y pegar
- importar de XML
- aplicar y eliminar
- deshacer / rehacer



Menú superior TSV

TSV	Ver "*Threat Standard Values*

Barra superior

– 1 +	Controla el despliegue del árbol de activos.
+1	Ajusta el efecto del *spinner* de despliegue. Si se marca [+1], PILAR muestra también las amenazas asociadas a cada activo.
– 1 +	Controla el despliegue del árbol de amenazas.
activos	— Seleccione una o más amenazas a la derecha. — Haga clic en ACTIVOS. PILAR selecciona a la izquierda los activos sujetos a dichas amenazas.

Barra inferior

	Revierte la última asociación de activos y amenazas.
	Reaplica la última asociación de activos y amenazas revertida.
aplicar	— Seleccione uno o más activos a la izquierda. — Seleccione una o más amenazas a la derecha. — Haga clic en APLICAR. PILAR asociada las amenazas seleccionadas a los activos seleccionados.
eliminar	— Seleccione uno o más activos a la izquierda. — Seleccione una o más amenazas a la derecha. — Haga clic en ELIMINAR. PILAR disocia las amenazas seleccionadas de los activos seleccionados. Ó — Seleccione una o más amenazas a la izquierda — Haga clic en ELIMINAR PILAR disocia las amenazas seleccionadas de los activos seleccionados.
	Guarda el proyecto en su fichero o en su base de datos.

En activos (panel izquierdo)

- Botón derecho > ACTUAL
  - Selecciona en el panel derechos las amenazas asociadas actualmente
- Botón derecho > ESTÁNDAR
  - Selecciona en el panel derechos las amenazas no opcionales en el TSV
- Botón derecho > OPCIONAL
  - Selecciona en el panel derechos las amenazas opcionales en el TSV

Si *Opciones / Amenazas* está en modo automático

- Algunas funciones están inhabilitadas
  - aplicar y eliminar
  - hacer / deshacer
  - cancelar y cerrar

Si *Opciones / Amenazas* está en modo manual

- aplicar y eliminar están activados
- no se aplica el TSV

Si *Opciones / Amenazas* está en modo mixto

- aplicar y eliminar están activados
- no se aplica el TSV

Para asignar una amenaza a un activo

- seleccione activos a la izquierda (uno o más)

- seleccione amenazas a la derecha (uno o más)
- APLICAR

Para quitar una amenaza de un activo

- seleccione activos a la izquierda (uno o más)
- seleccione amenazas a la derecha (uno o más)
- ELIMINAR

o

- seleccione amenazas a la izquierda (una o más)
- ELIMINAR

Para que el sistema sugiera amenazas para un activo

- seleccione activos a la izquierda (uno o más)
- SUGERIR

La sugerencia es similar al estándar; pero las amenazas solo se seleccionan, sin aplicarse.

¿Qué amenazas afectan a un activo?

- seleccione activos a la izquierda (uno o más)
- AMENAZAS

“Copiar y pegar” amenazas de un activo sobre otro

- seleccione el activo origen en el panel de la izquierda
- clic en AMENAZAS para que PILAR seleccione a la derecha las amenazas usadas
- seleccione activos destinatarios a la izquierda (uno o más)
- APLICAR

¿Qué activos están afectados por una amenaza?

- seleccione amenazas a la derecha (una o más)
- seleccione los ACTIVOS

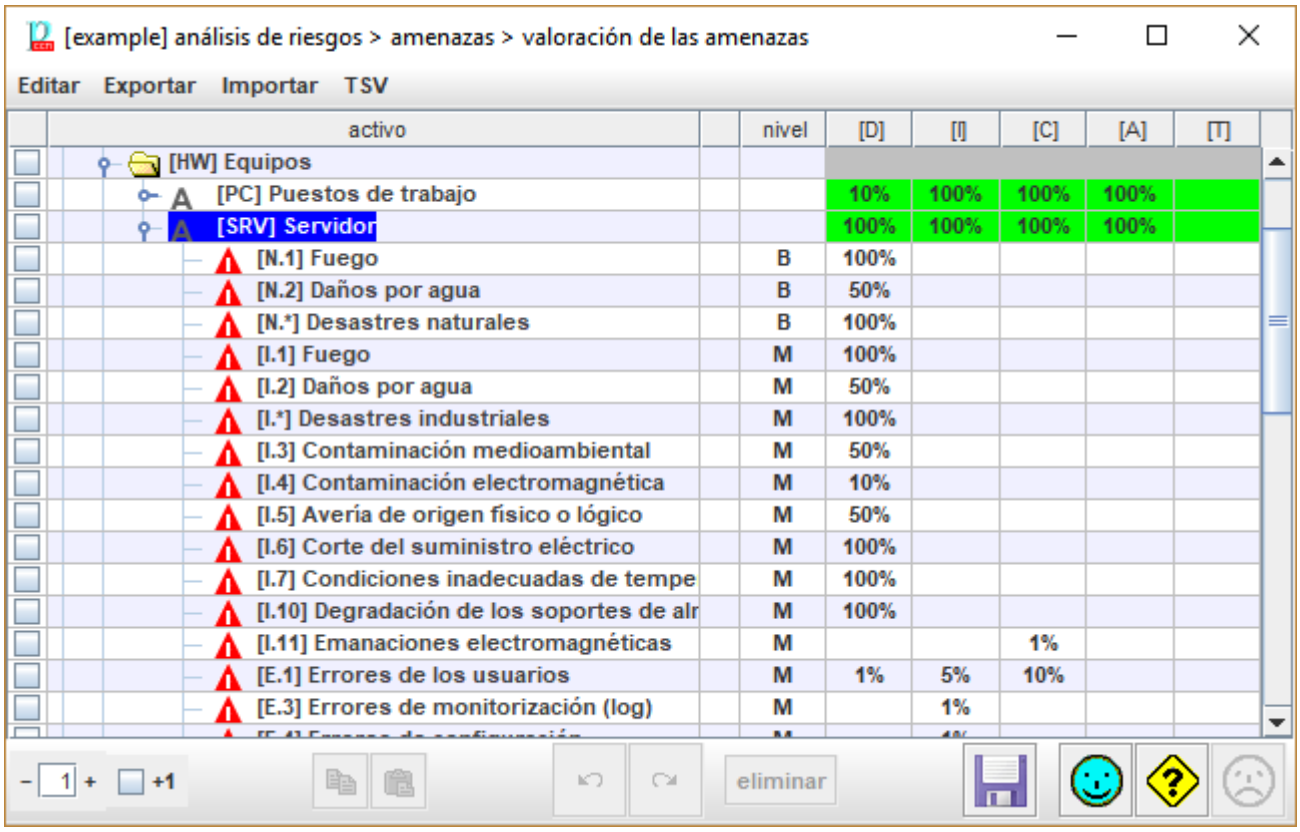
Puede utilizar la biblioteca para que le ayude. Seleccione uno o más activos en el panel izquierdo y ...

- clic SUGERIR para que la biblioteca muestra su conocimiento a la derecha
- clic BIBLIOTECA para aplicar la mejor opinión de la biblioteca
- clic CARGA para usar un perfil diferente

8.9.3 Valoración

Para empezar rápidamente
Si *Opciones / Amenazas* está en modo automático o mix, PILAR aplica el TSV.

Una vez elegidas las amenazas sobre un activo, hay que cuantificarlas: sus consecuencias y su probabilidad.



Menú superior EDITAR

opciones	ver *Editar / Opciones*
copiar	Seleccione una o más celdas en la tabla. Haga clic para copiar los valores.
cortar	Seleccione una o más celdas en la tabla. Haga clic para eliminar los valores.
pegar	Seleccione una o más celdas de destino. Pegue los valores que antes copió. Si el original era una celda y el destino son varias, se repite el valor.

Menú superior EXPORTAR

CSV	Comma Separated Values (para excel)
XML	eXtensible Markup Language

Menú superior IMPORTAR

de XML	eXtensible Markup Language

Menú superior TSV

TSV	Ver "*Threat Standard Values*
aplicar	Aplica el TSV correspondiente a los activos / amenazas seleccionados

Tabla

1	**selección**	Haga clic en las cajitas para seleccionar / deseleccionar. Haga MAYÚSCULAS + clic para seleccionar un rango. Haga clic en la cabecera de la columna para eliminar la selección actual. La selección determina a qué filas se aplica una valoración estándar TSV o se borran los valores
2	**activos**	árbol de activos
3		indica el modo de cada activo o amenaza: • rojo: manual, bien todo el activo, bien una cierta amenaza • naranja: dentro de un activo, algunas amenazas son manuales • transparente: automático (según TSV) En modo mix, haga clic para cambiar.
4	**nivel**	Esta columna presenta la probabilidad de ocurrencia. El formato se puede ajustar en *Opciones / Probabilidad*
5 …		Estas columnas presentan la degradación causada por la amenaza en cada dimensión. El formato se puede ajustar en *Opciones / Efectos*

Barra inferior

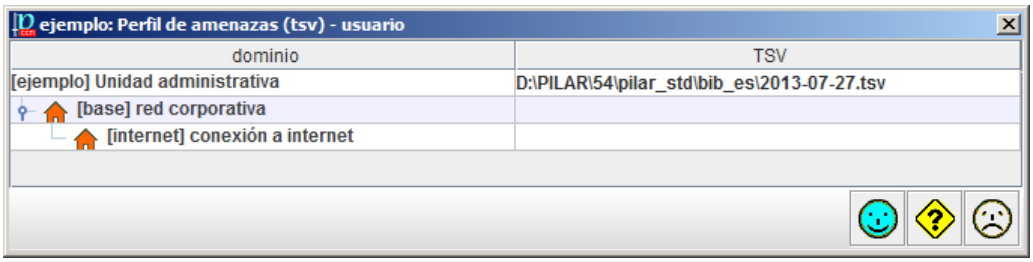
	Controla el despliegue del árbol de activos.
+1	Ajusta el despliegue. Si se marca [+1], PILAR muestra las amenazas asociadas a cada activo.
	Revierte los últimos cambios
	Aplica de nuevo los últimos cambios revertidos
	Guarda el proyecto en su fichero o en su base de datos.

8.9.4 TSV – Threat Standard Values

Puede editar las amenazas y sus valores manualmente o, mucho mejor, usar un fichero TSV.

Los ficheros TSV se explican en personalización, en https://www.ar-tools.com/doc/

Cuando esté *identificando* amenazas o *valorándolas* puede hacer clic en TSV / CARGAR para elegir el fichero TSV



en donde puede especificar un fichero TSV para el proyecto, y diferentes ficheros TSV para diferentes dominios de seguridad. Si un dominio no tiene un fichero propio asignado, recurre al del dominio que lo ampara y, en última instancia, al fichero del proyecto.

Para cada activo, PILAR identifica a qué dominio pertenece y le aplica el TSV correspondiente.

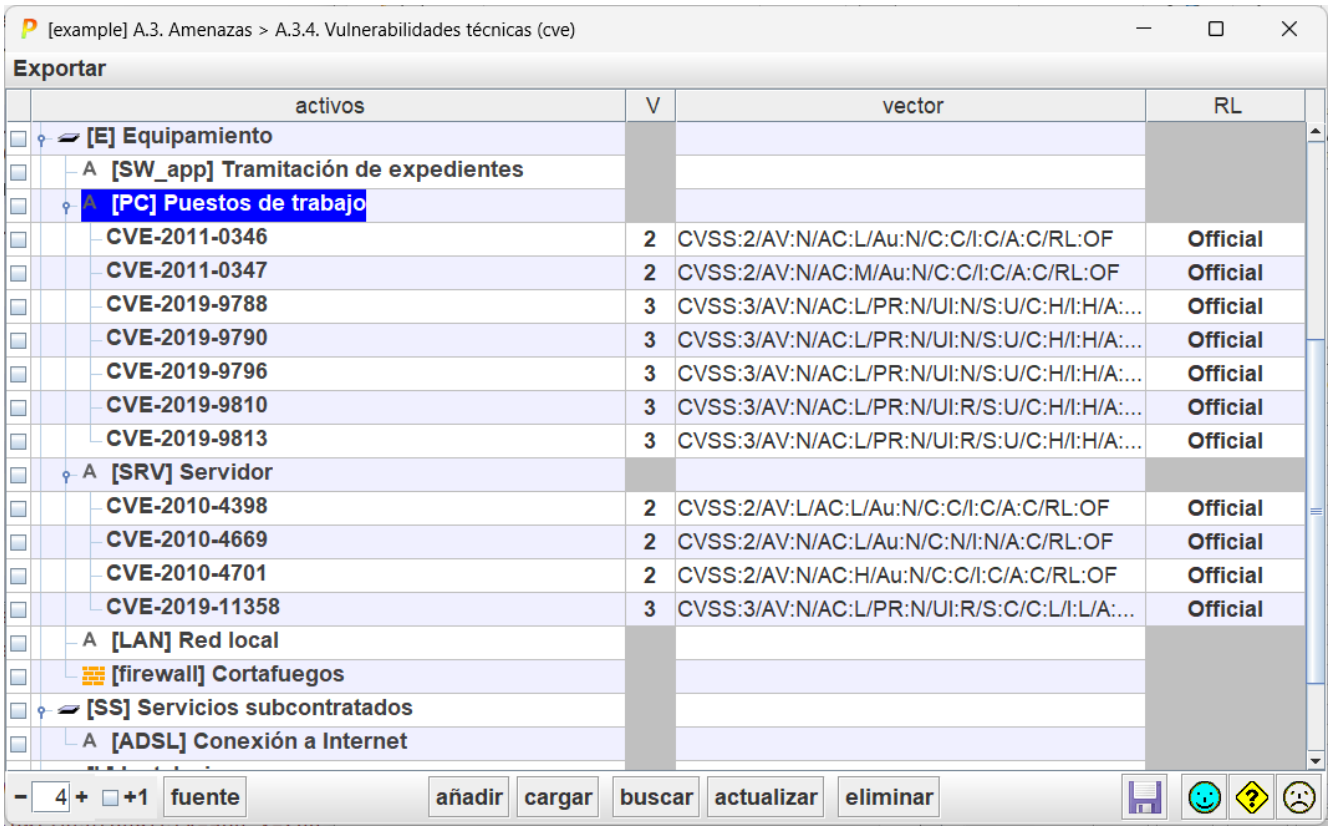
El nombre y la ruta de los ficheros TSV se almacenan con el proyecto. Cuando se abre el proyecto, pilar intenta recargarlo y verifica si el fichero ha cambiado. PILAR se queja amargamente si el proceso no funciona como la seda.

8.9.5 Vulnerabilidades técnicas (CVE)

Ver

https://www.ar-tools.com/doc/

Para asociar vulnerabilidades CVE a los activos, estos necesitan tener asociados *Activos / CPE*.



Tabla

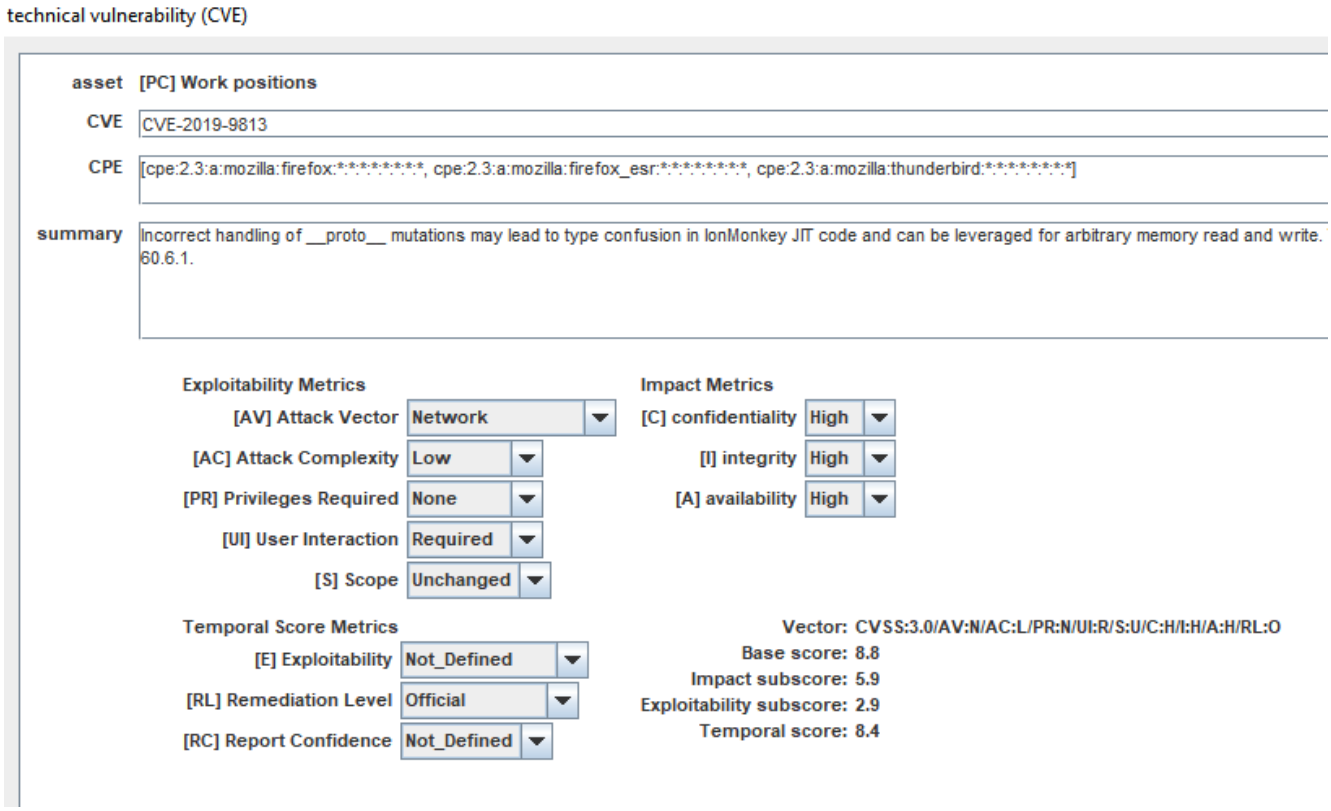
selección	Haga clic en las cajitas para seleccionar / deseleccionar. Haga MAYÚSCULAS + clic para seleccionar un rango. Haga clic en la cabecera de la columna para eliminar la selección actual. La selección determina a qué filas se aplican los botones
activos	Activos y vulnerabilidades CVE.
Versión	Versión CVSS. Suele ser 2 o 3.
vector	Resumen CVSS.
RL	Remediation level (ver CVSS)

Barra inferior

	Controla el despliegue del árbol de activos y CVE.
+1	Ajusta el funcionamiento del *spinner*.

	Si se marca [+1], PILAR presenta las CVE asociados a cada activo.
añadir	— Seleccione un activo a la izquierda. — Haga clic en AÑADIR para introducir manualmente una CVE.
cargar	— Seleccione uno o más activos a la izquierda. — Haga clic en CARGAR para asociar uno o más activos a una CVE leída de un fichero en formato XML o JSON, de acuerdo a los formatos del NIST.
buscar	— Seleccione uno o más activos a la izquierda. — Haga clic en BUSCAR PILAR carga CVE asociados desde la base de datos de vulnerabilidades. Para ser más precisos, PILAR lee un fichero XML con vulnerabilidades CVE y usa los nombre CPE asociados a los activos para seleccionar las que aplican.
actualizar	Como BUSCAR, pero ahora solo se actualizan datos ya cargados.
eliminar	— Seleccione uno o más activos a la izquierda — Haga clic en ELIMINAR PILAR elimina las CVE asociadas Ó — Seleccione una o más vulnerabilidades a la izquierda — Haga clic en ELIMINAR PILAR elimina las CVE marcadas
	Guarda el proyecto en su fichero o en su base de datos.

Puede editar los valores (clic-clic en el nombre de la CVE).



Por compatibilidad, PILAR también soporta CVSS versión 2.

Para añadir vulnerabilidades manualmente

- seleccione un activo (primera columna
- clic en AÑADIR
- edite los datos

Para buscar vulnerabilidades que aplican a un activo

- seleccione uno o más activos (primera columna)
- clic en BUSCAR
- elija el fichero XML de datos

Para actualizar las vulnerabilidades asociadas a un activo

- seleccione uno o más activos (primera columna)
- clic en ACTUALIZAR
- elija el fichero XML de datos

Para eliminar vulnerabilidades asociadas a un activo

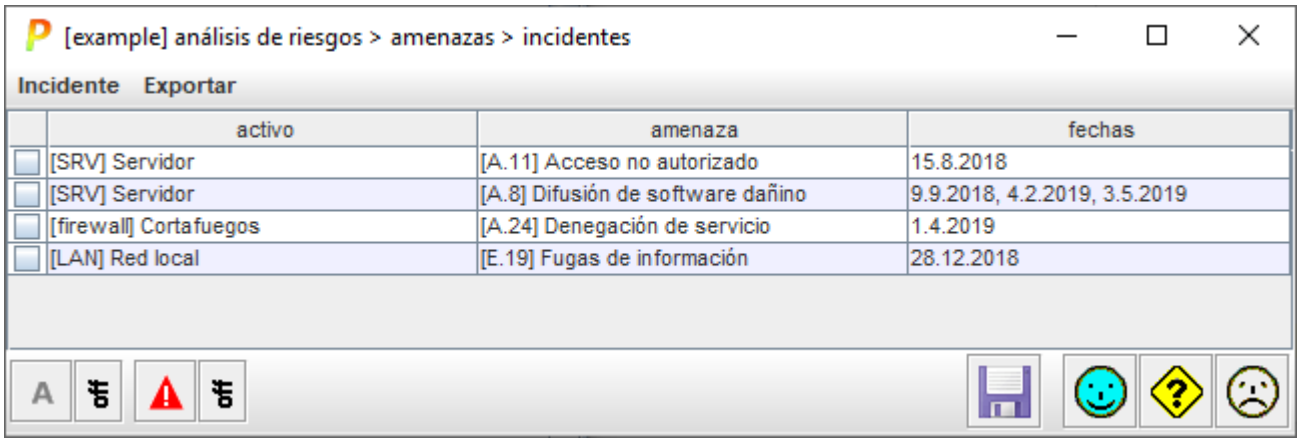
- seleccione uno o más activos (primera columna)
- clic en ELIMINAR

Para editar los parámetros que caracterizan a una vulnerabilidad asociada a un activo

- doble clic en el activo
- introduzca datos en la pantalla de edición

8.10 Incidentes

Se puede hacer el análisis de riesgos más dinámico, adaptándolo a los incidentes observados.



Menú superior

incidente	nuevo	crea un nuevo incidente
	editar	edita un incidente ya reportado: seleccione en la primera columna y edite
	eliminar	elimina un incidente: seleccione en la primera columna y elimine
exportar	a CSV	lo que ve, para excel

Barra inferior

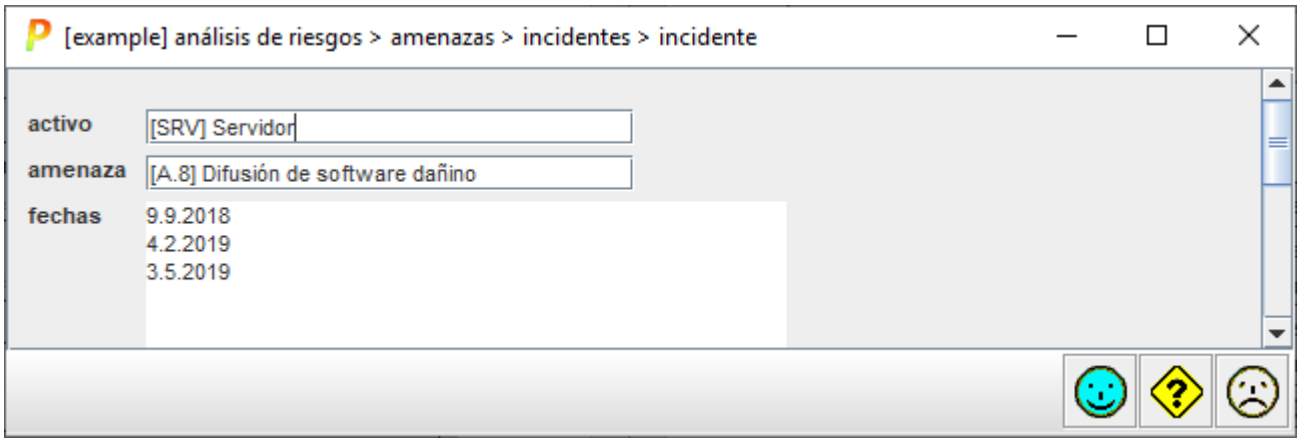
	Seleccione activos y active el filtro para ver solamente los seleccionados.
	Seleccione amenazas y active el filtro para ver solamente las seleccionadas.

Si hace clic en las cabeceras de las columnas, PILAR ordena los incidentes por activo, amenaza o última incidencia observada.

PILAR adapta la probabilidad de las amenazas a los incidentes observados, por delante de lo que diga la TSV. Este cálculo dinámico calcula la tasa anual observada durante el último año. Para alinear incidentes con fases del proyecto, debe asociar una fecha a la fase.

8.10.1 Editar un incidente

Bien el menú superior (incidente > editar) o haciendo doble clic en una fila, puede editar un incidente individual



Haga clic en ACTIVO para seleccionar un activo.

Haga clic en AMENAZA para seleccionar una amenaza.

Puede especificar una o más fechas en las que se observó un incidente. El formato es

DÍA . MES . AÑO

PILAR ordena las fechas.

8.11 Salvaguardas

8.11.1 Aspecto

Aspecto que trata la salvaguarda:

- G para Gestión
- T para Técnico
- F para seguridad Física
- P para gestión del Personal

8.11.2 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 – norma
- proc – procedimiento
- cert – certificación o acreditación

8.11.3 Peso relativo

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

8.11.4 Hooks

Se pueden asociar enlaces a salvaguardas por medio de ficheros hook-. Estos son ficheros en el directorio de librería, con un nombre que empieza por “hooks-…”. El formato es JSON.

Se presenta un ejemplo:

/bib_en/hooks-sp800-53.json

```
{
  "encoding" : "áéíóú",
  "title" : "SP 800-53 rev.5",
  "defs" : [
    {
      "sm" : [ "ACb" ],
      "links" : [
        {
          "label" : "ACCESS CONTROL",
          "url" : "https://nvd.nist.gov/800-53/Rev4/family/ACCESS%20CONTROL"
        }
      ]
    },
    {
      "sm" : [ "AC-1", "AC-1(0)" ],
      "links" : [
        {
          "label" : "Policy and procedures",
          "url" : "https://nvd.nist.gov/800-53/Rev4/control/AC-1"
        }
      ]
    },
```

8.11.5 Información adicional

Una ventana separada presenta información adicional relativa a la salvaguarda

8.11.6 En el árbol de salvaguardas

Si hace clic-clic en alguna salvaguarda de árbol de salvaguardas, se le presentan varias opciones …

editar

presenta una vista por dominios y fases; ver más abajo

copiar

copia en el portapapeles el nombre de la salvaguarda

copiar ruta

copia en el portapapeles el camino completo de la salvaguarda

texto completo

código y nombre de la salvaguarda

camino completo

muestra la salvaguarda en su contexto; es decir, la serie de pasos desde la raíz hasta ella

cerrar el padre

compacta el árbol, cerrando el padre del nodo seleccionado

cerrar los hermanos

compacta el árbol cerrando todos los hermanos del nodo seleccionado

…

En algunas salvaguardas, PILAR puede proporcionar algo más de información.

Cuando una salvaguarda procede de la SP800-53, o existe una relación con una medida en la SP800-53, PILAR salta a la página web donde se describe la correspondiente medida. Dado que la URL puede verse modificada, se puede actualizar en el fichero de configuración.

`bib_xx/hooks-sp800-53.json`

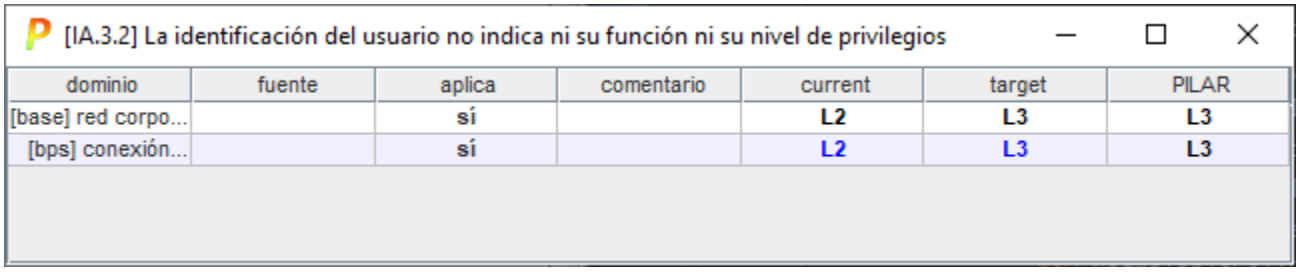
Ver *Salvaguardas / hooks*

más información

presenta información adicional sobre la salvaguarda.

Ver "*Salvaguardas / Información adicional*".

Vista por dominios y fases. Haciendo clic en una salvaguarda puede acceder a una vista de los valores de madurez que cubra simultáneamente todos los dominios y todas las fases:

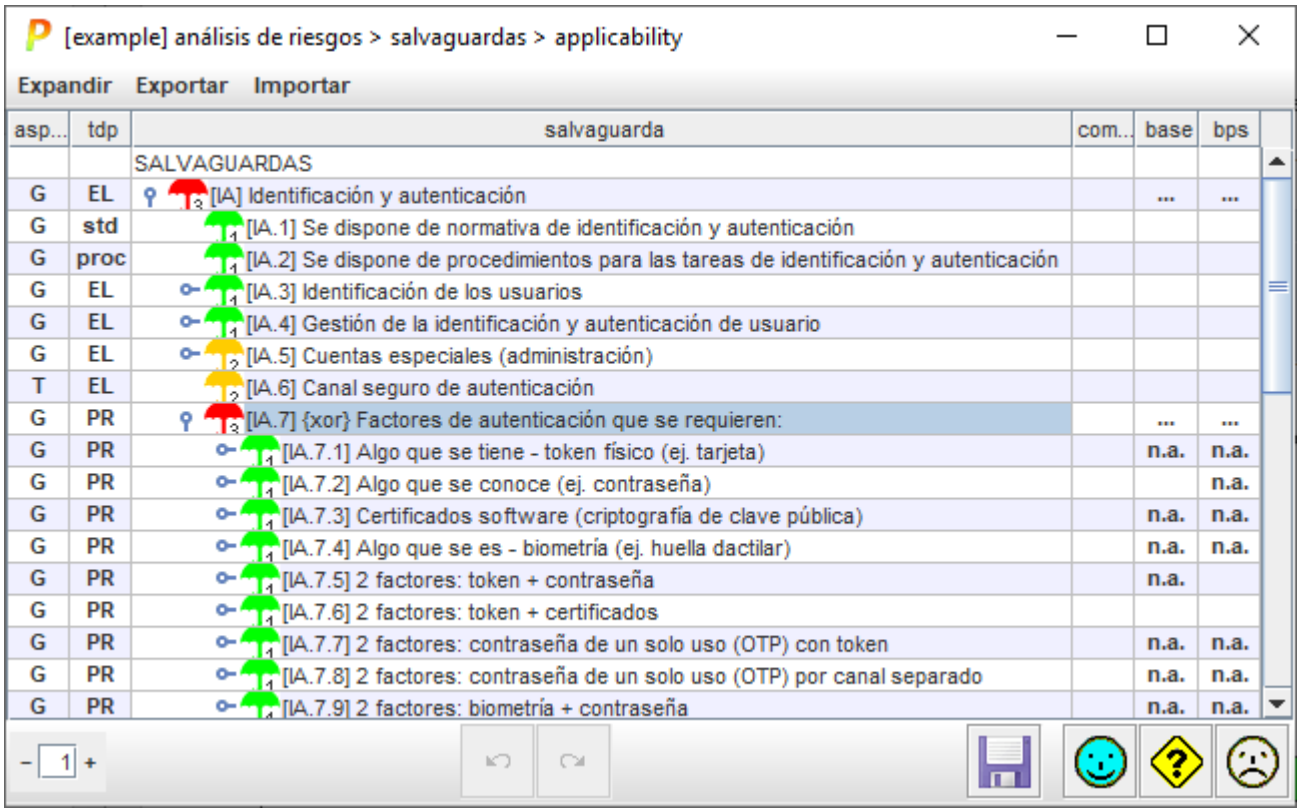


Los datos del usuario aparecen en negro sobre blanco, mientras que los derivados por PILAR aparecen en cian.

8.11.7 Resumen de aplicabilidad

Se refiere a la etapa de aplicabilidad actual.

Esta pantalla presenta un resumen de las salvaguardas que aplican en cada dominio de seguridad.



Por favor, no olvide que algunas salvaguardas pueden ser inhabilitadas más adelante en fases específicas del proyecto.

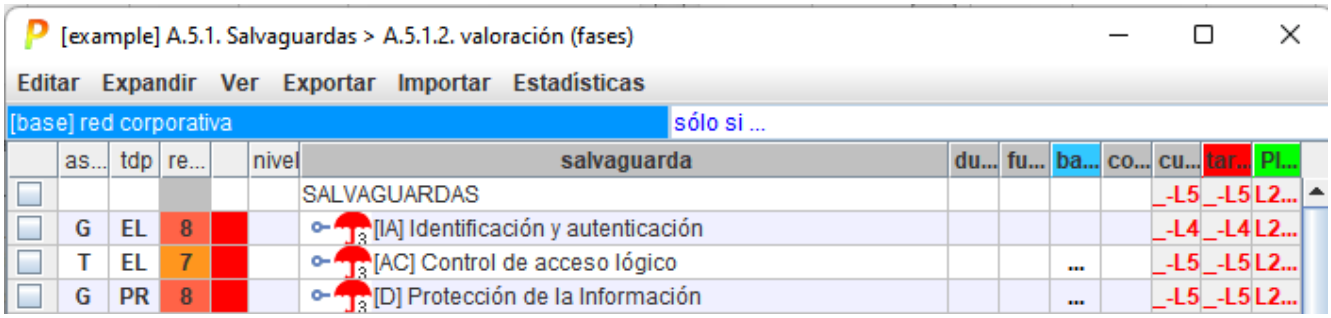
8.11.8 Valoración (fases)

Para empezar rápidamente

- Sitúese en la celda que está en la fila **SALVAGUARDAS**, y en la columna de la fase ACTUAL. Selecciónela.
- Botón derecho. Seleccione la madurez que, en líneas generales, mejor califica su sistema (por ejemplo, L2).
- Puede visitar cualquier salvaguarda, en cualquier nivel de detalle, e ir refinando su estimación global.

Si tiene un plan en mente…

- Sitúese en la celda que está en la fila **SALVAGUARDAS**, y en la columna de la fase **OBJETIVO.**
  Selecciónela.
- Seleccione el nivel de madurez al que aspira llegar.



Menú superior EDITAR

copiar	se copia al portapapeles el valor de las celdas de madurez seleccionadas
pegar	se pegan en las celdas los valores copiados previamente
buscar	Ver "*Salvaguardas / Buscar*

Menú superior EXPANDIR

salvaguardas no evaluadas	Expande el árbol hasta llegar a las salvaguardas que no han sido evaluadas
recomendación = 0	Expande el árbol hasta llegar a las salvaguardas sin recomendación (recomendación en gris)
n.a.	Expande el árbol hasta las salvaguardas no-aplicables
{xor}	Expande el árbol hasta salvaguardas marcadas como XOR Son candidatas para seleccionar una variante.
dudas	Expande el árbol hasta llegar a las salvaguardas marcadas con dudas
selección	dentro de nodos XOR; avanza al nodo seleccionado
perímetro	Expande el árbol hasta perímetros definidos por el usuario (ver *Perímetros*

Menú superior EXPORTAR

SoA	*SoA – Declaración de Aplicabilidad*
CSV	Se copian a un fichero CSV las filas visibles
XML	Se copian los valores a un fichero XML
informe	Se genera un informe (RTF o HTML)
< Lx	Se genera un informe con las salvaguardas que aplican pero están por debajo de un cierto umbral de madurez
< objetivo	Se genera un informe con las salvaguardas que están por debajo de la fase OBJETIVO. Ver *Salvaguardas / Fases de referencia y objetivo*

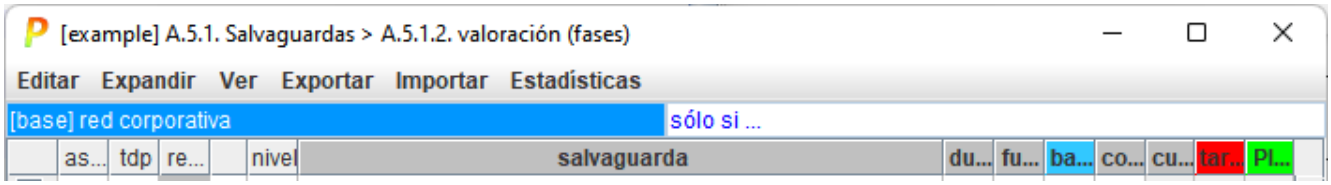
Menú superior IMPORTAR

de CSV	lee los valores de madurez de un fichero CSV
de XML	lee los valores de madurez de un fichero XML
importar (mgr)	
importar (db)	

Menú superior ESTADÍSTICAS

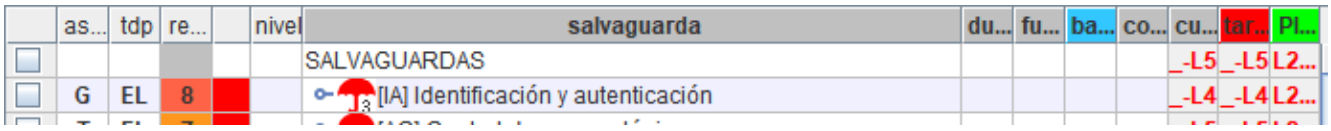
por dominio	Resumen con el número de salvaguardas evaluadas en cada dominio de seguridad

Bandas superiores



dominio de seguridad	Pueden haber diferentes salvaguardas en diferentes dominios. Haga clic para seleccionar el dominio en el que vamos a trabajar.
solo si …	Haga clic para seleccionar un subconjunto de salvaguardas basado en algunos atributos de las mismas. PILAR recortará el árbol para mostrar solo las que cumplan los criterios Se pueden usar diferentes criterios • salvaguardas que aplican; o que no • fuentes de información • nivel de la salvaguarda

8.11.8.1 Tabla central



1	**selección**	
2	**aspecto**	Ver "*Salvaguardas / Aspecto*".
3	**tdp**	Ver "*Salvaguardas / Tipo de protección*".

4	**recomendación**	Es una valoración en el rango [nada .. 10] estimada por PILAR teniendo en cuenta el tipo de activos y su valoración en cada dimensión. La celda queda gris si PILAR no ve ningún motivo para poner esta salvaguarda; es decir, si PILAR no sabe qué riesgo mitigaría esta salvaguarda. (o) – significa que PILAR opina que es excesiva ("overkill") (u) – significa que PILAR opina que es insuficiente ("underkill"). Haga clic con el botón derecho y aparecerá una nueva ventana con un resumen de las razones que han llevado a PILAR a su recomendación; es decir, los activos y dimensiones que protege.
5	**semáforo**	Ver "*Salvaguardas / Fases de referencia y objetivo*".
6		Árbol de salvaguardas. Haga clic-clic para colapsar / expandir el árbol. Clic con el botón derecho para acceder a *Salvaguardas / tree*
7	**dudas**	Haga clic para marcar / desmarcar la caja. La marca se usa, típicamente, para recordar que hay asuntos pendientes de una respuesta. La marca "mancha" todo el árbol, desde donde se pone hasta la raíz, para que sea evidente que hay algo pendiente.
8	**fuentes**	Haga clic para asociar fuentes de información a la salvaguarda (la marcada y sus descendientes).
9	**aplica**	Todas las salvaguardas aplican, salvo que se marquen como "n.a.". Haga clic para conmutar. Cuando una salvaguarda cambia, esto se propaga a todos los hijos en el árbol. Cuando algunos hijos son de aplicación y otros no, se pintan puntos suspensivos.
10	**comentario**	Haga clic para asociar un comentario a la salvaguarda.
…		Fases del proyecto. Ver "*Valoración de salvaguardas por dominios*".

En APLICA

- clic botón izquierdo
  - para seleccionar / deseleccionar; si una salvaguarda se marca como "no aplica", sus hijos se marcan como "no aplica"; si algunos hijos aplican y otros, no, la salvaguarda que los cubre se marca como "…·
- clic botón derecho

eliminar	elimina todas las marcas de aplicabilidad
recomendación	recomendación: para aplicar la recomendación de PILAR: todo aplica salvo que la recomendación esté en gris

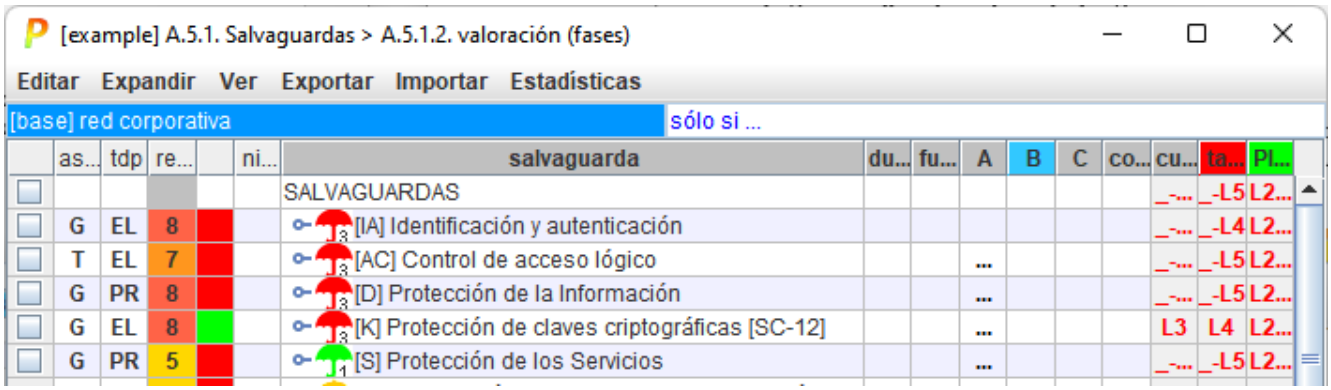
sólo si …	seleccione uno o más perfiles de seguridad (evl); nada aplica salvo que algún perfil referencie la salvaguarda directa o indirectamente
n.a.	la salvaguarda (y sus hijos) no son aplicables en este sistema
bajar valores	los valores de aplicabilidad se copian a los dominios de seguridad bajo el presente
copiar	los valores de aplicabilidad del dominio superior se copian a este

Ejemplo. Si tenemos dos dominios de seguridad: A encima de B, entonces …

- si estamos viendo A, bajar-valores copia los valores de A en B
- si estamos viendo B, copiar lleva los valores de A a B

Etapas de aplicabilidad

Cuando hay varias etapas de aplicabilidad, las opciones anteriores aplican independientemente a cada etapa. Aparece una columna por cada etapa, estando resaltada en azul la etapa actual



Puede hacer clic en la cabecera de la columna para seleccionar la etapa actual.

8.11.8.2 Barra inferior de herramientas

– 1 +	Controla el despliegue del árbol de salvaguardas.
fuentes	Seleccione una o más fuentes de información. PILAR seleccionará todas las salvaguardas a las que está asociada.
	Revierte los últimos cambios
	Rehace los últimos cambios revertidos
operación	Ver "*Salvaguardas / Valoración / Operaciones*".

sugiere	Ver "*Salvaguardas / Sugiere*".
buscar	Ver "*Salvaguardas / Buscar*".
>>	Ver "*Salvaguardas / Buscar*".
	Guarda el proyecto en su fichero o en su base de datos.

8.11.8.3 SoA – Declaración de Aplicabilidad

Algunos auditores lo consideran un documento fundamental. En cualquier caso, recoge aquellas salvaguardas que se consideran relevantes y que serán objeto de inspección.

Es importante saber qué es lo que sí aplica para centrarse en ello.

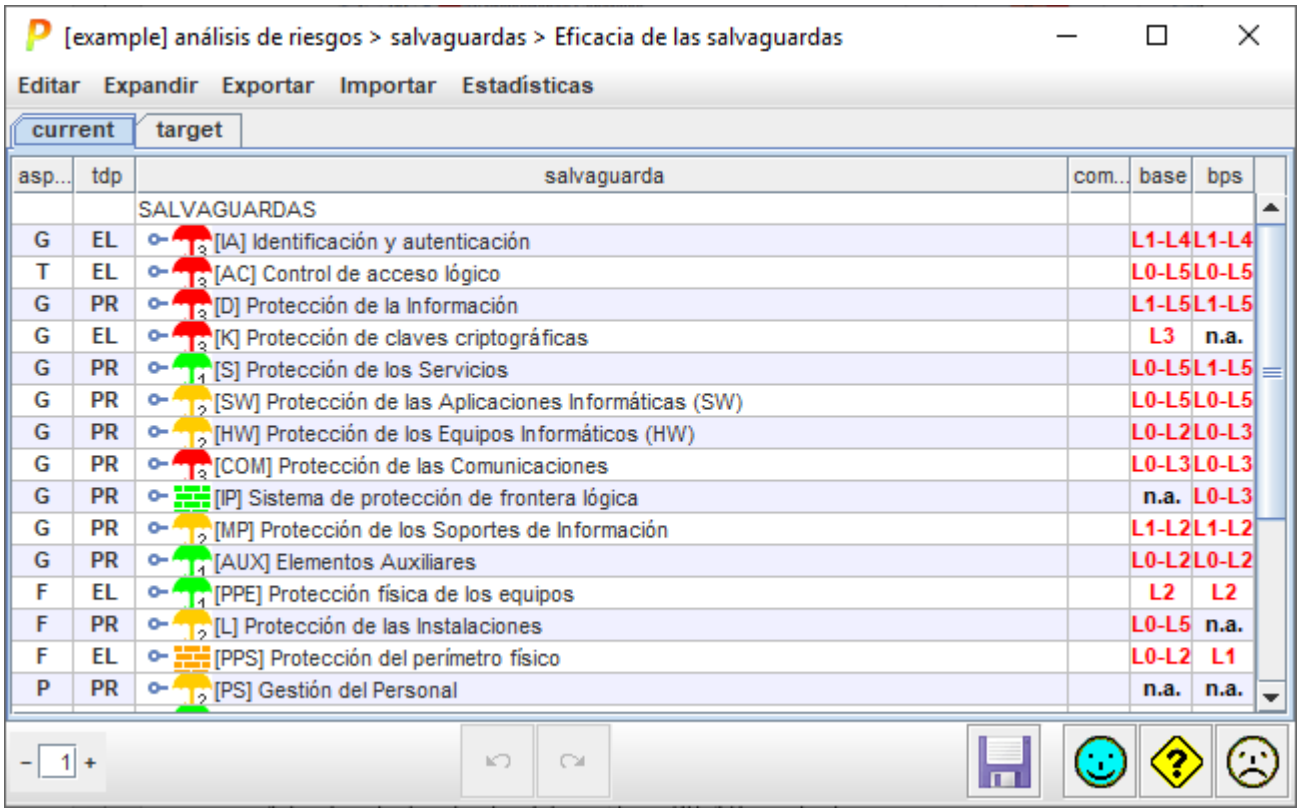
También es importante saber qué es lo que no aplica pues una inspección puede tener otra opinión.

A veces, "n.a." significa que la salvaguarda aplicaría, pero que no está justificada (que el riesgo es menor que el coste de la salvaguarda). Eso hay que explicarlo.

Clasificación	Fija la marca de clasificación del informe. Se marca un mínimo en *Datos del proyecto*. Aquí se puede poner una marca más restrictiva.
Fecha	La fecha por defecto es HOY.
Dominios de seguridad	Puede seleccionar un subconjunto de los dominios para el informe. Mientras no indique lo contrario, se imprimen todos.
Perímetro	Ver *Perímetros*
Incluye	Puede incluir solo las salvaguardas que aplican, solo las que no, o ambas categorías.
Formato	El formato RTF es útil para documentos. El formato HTML es útil para intranets.

8.11.9 Valoración (dominios)

Es una vista similar a "*Valoración de salvaguardas por dominios*", pero ahora las columnas son dominios de seguridad y las fases aparecen como pestañas.



asp...	tdp	salvaguarda	com...	base	bps
		SALVAGUARDAS			
G	EL	[IA] Identificación y autenticación		L1-L4	L1-L4
T	EL	[AC] Control de acceso lógico		L0-L5	L0-L5
G	PR	[D] Protección de la Información		L1-L5	L1-L5
G	EL	[K] Protección de claves criptográficas		L3	n.a.
G	PR	[S] Protección de los Servicios		L0-L5	L1-L5
G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)		L0-L5	L0-L5
G	PR	[HW] Protección de los Equipos Informáticos (HW)		L0-L2	L0-L3
G	PR	[COM] Protección de las Comunicaciones		L0-L3	L0-L3
G	PR	[IP] Sistema de protección de frontera lógica		n.a.	L0-L3
G	PR	[MP] Protección de los Soportes de Información		L1-L2	L1-L2
G	PR	[AUX] Elementos Auxiliares		L0-L2	L0-L2
F	EL	[PPE] Protección física de los equipos		L2	L2
F	PR	[L] Protección de las Instalaciones		L0-L5	n.a.
F	EL	[PPS] Protección del perímetro físico		L0-L2	L1
P	PR	[PS] Gestión del Personal		n.a.	n.a.

8.11.10 Fase de referencia y fase objetivo

El semáforo resume en un color si la madurez de la salvaguarda 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

Veamos un ejemplo.

La fase roja es [3m].

La fase verde es [PILAR]

El semáforo, en la primera columna se ajusta a la diferente madurez en las fases ROJA y VERDE

	current	3m	1y	target	PILAR
		_-L5	_-L5	_-L5	L4-L5
					L4
		L0			L4
		L1			L5
		L2			L4
		L3			L4
		L4			L4
		L5			L4
		L4			L4
		L4			L4

8.11.11 Valoración de la madurez de las salvaguardas

Las celdas de valoración recogen el valor de la madurez de cada salvaguarda en cada fase del proyecto.

El valor es un nivel de madurez en el rango L0 a L5, o una marca de no aplicabilidad (n.a.), o está vacío. A efectos matemáticos, “n.a.” es como si la salvaguarda no existiera.

Si una celda está en blanco, PILAR intenta reutilizar el valor de la fase anterior o del dominio que engloba a este dominio (ver “*Opciones / Dominios y fases*”). Si después de esa búsqueda sigue sin valor, se usa el marcado por “*Tratamiento del riesgo*”.

Los valores de madurez se le asignan a las salvaguardas individuales. Los grupos de salvaguardas muestran el rango (min-max) de su despliegue. La agregación se propaga hacia arriba hasta el primer nivel de salvaguardas.

código de color	
caracteres rojos	cuando el valor se calcula a partir de otros
negro sobre blanco	cuando el valor es explícito
negro sobre amarillo	cuando el valor viene de un dominio inferior

Para cambiar un valor de madurez

- haga clic con el botón derecho y elija un valor
- seleccione una madurez en los combos de la baffa inferior de herramientas
- puede usar las operaciones copiar y pegar del menú EDITAR para trasladar el valor de unas celdas a otras

En las celdas de valoración, también puede trasladar valores de madurez de una fase, dominio de seguridad e incluso de un proyecto a otro:

copia el árbol

PILAR copia en el portapapeles el valor de la celda en la fila seleccionada, y los valores de las celdas es que se descompone la salvaguarda (el sub-árbol).

pega el árbol

Pega los valores previamente copiados.

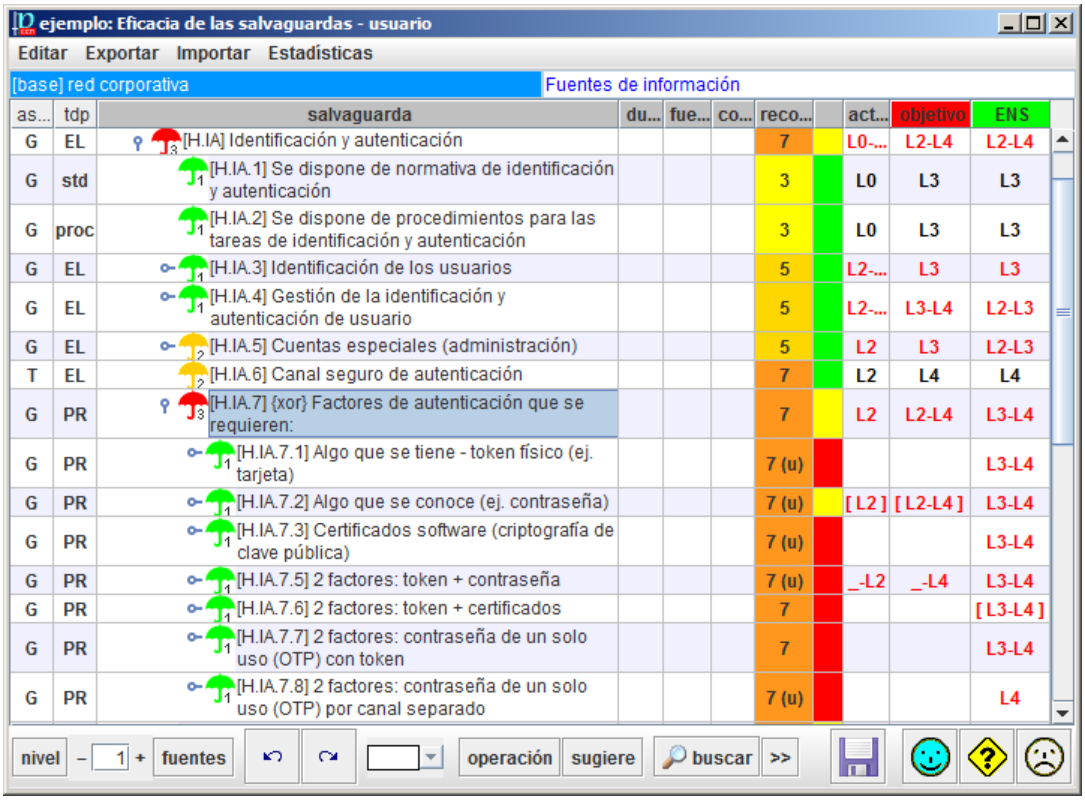
Nótese que los valores pueden ir de una fase a otra fase, de un dominio a otro, e incluso de un proyecto a otro proyecto; pero siempre se aplican al mismo sub-árbol.

También debe tener en cuenta que PILAR copia y pega dentro de sí misma. No es posible copiar valores en un proceso y volcarlos en otro.

Salvaguardas XOR

En salvaguardas de tipo XOR, podemos indicar cual e s la opción seleccionada dentro de las posibles.

La salvaguarda seleccionada aparece entre llaves cuadradas:



En salvaguardas que realmente son un enlace a otra salvaguarda, no podremos establecer una valoración: hay que ir al sitio enlazado.

8.11.12 Operaciones

PILAR puede aplicar una serie de operaciones estándar a las celdas seleccionadas en las columnas de valoración de la madurez.

APLICAR

aplica el valor seleccionado en el combo de madurez a las celdas seleccionadas

RELLENAR

aplica el valor seleccionado en el combo de madurez a las celdas seleccionadas si están vacías

PREDECIR

mira alrededor, calcula una media de la madurez circundante, y rellena las celdas seleccionadas que estén vacías

SIMPLIFICAR

elimina valores que pueden ser heredados, bien del dominio inferior, bien de la fase anterior;

es útil cuando estamos moviendo las fases arriba y abajo para buscar el orden óptimo de ejecución

MÍNIMOS

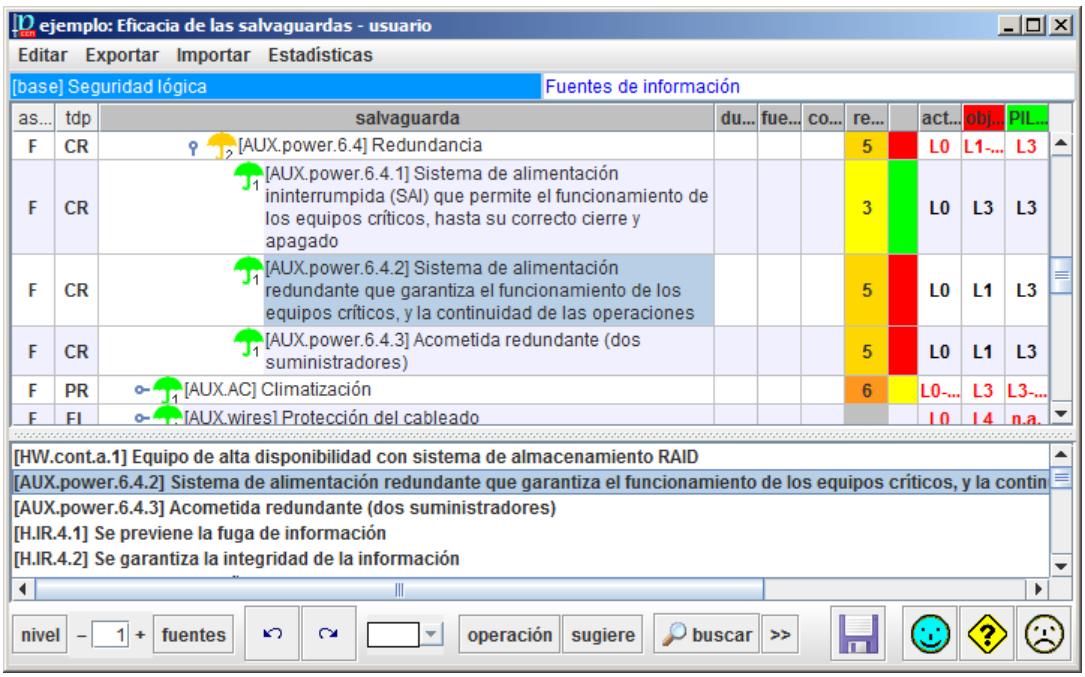
teniendo en cuenta la recomendación, PILAR sugiere unos valores de madurez que considera mínimos para satisfacer las necesidades del sistema. Meramente heurístico, con ánimo de marcar una referencia por debajo de la cual no se debería operar el sistema

RECOMENDACIÓN

teniendo en cuenta la recomendación, PILAR sugiere unos valores de madurez que considera adecuados para satisfacer las necesidades del sistema. Meramente heurístico, con ánimo de marcar una referencia digna para operar el sistema

8.11.13 Operación SUGERENCIA

Seleccione una fase haciendo clic en la cabecera de su columna. La cabecera de la fase seleccionada se pone ROJA. Haga clic en SUGIERE. PILAR parte la pantalla en dos. En la parte superior sigue el árbol con todas las salvaguardas y sus valores en cada fase. En la parte inferior aparecen una serie de salvaguardas ordenadas según el orden en que PILAR sugiere que se mejore su valoración en la fase seleccionada. Haga clic en la salvaguarda en la parte inferior y PILAR se la presentará en su contexto en la parte superior.



8.11.14 Buscar

PILAR puede buscar entre las salvaguardas con ciertos criterios:

CAMBIOS (fases | dominios)

se detiene en las salvaguardas que cambian de una fase a otra / entre dominios

EMPEORAS

se detiene en las salvaguardas que van a peor de una fase a otra

UMBRAL

se detiene en las salvaguardas por debajo de un umbral dado de madurez

< OBJETIVO

se detiene en las salvaguardas por debajo de un umbral marcado en la fase OBJETIVO (verde)

N.A.

se detiene en las salvaguardas valoradas como n.a. (no aplican)

NO EVALUADAS

se detiene en las salvaguardas no valoradas (en blanco)

XOR

se detiene en las salvaguardas que presentan alternativas excluyentes entre las que hay que elegir

COMENTARIO

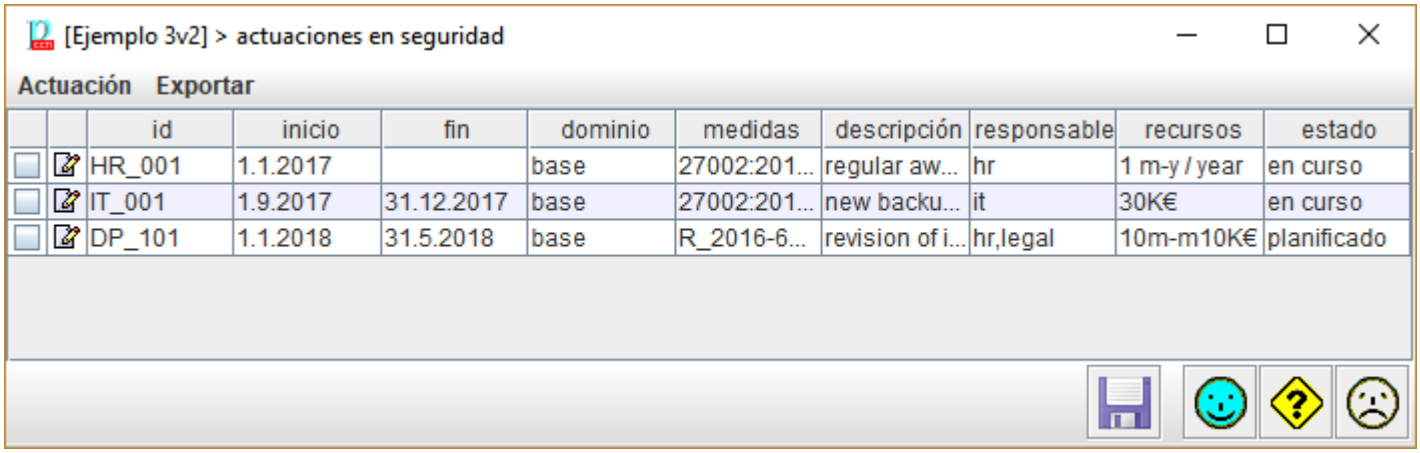
se detiene en salvaguardas con comentarios asociados

>>

busca la siguiente salvaguarda que cumple el criterio de búsqueda

8.12 Actuaciones en seguridad

PILAR permite identificar actuaciones de seguridad que son actividades con un principio y un fin, que actúan sobre un subconjunto de salvaguardas o de controles. Esta agrupación no cambia los cálculos matemáticos de riesgo, simplemente permite un enfoque de gestión de proyectos.



Menú barra superior

Actuación	**nuevo** permite crear una fila más en la tabla de actuaciones **editar** permite modificar una actuación **eliminar** elimina una fila de la tabla de actuaciones
Exportar	**CSV** vacía la tabla de actuaciones en formato CSV para Excel **XML** vacía la tabla de riesgos en formato XML

Opciones barra inferior

	Guarda el proyecto en su fichero o en su base de datos.
	ACEPTAR. Se guardan los cambios realizados y se cierra la ventana.
	CANCELAR. Se desestiman los cambios y se cierra la ventana.
	AYUDA. Abre un navegador con estas páginas de ayuda.

Tabla

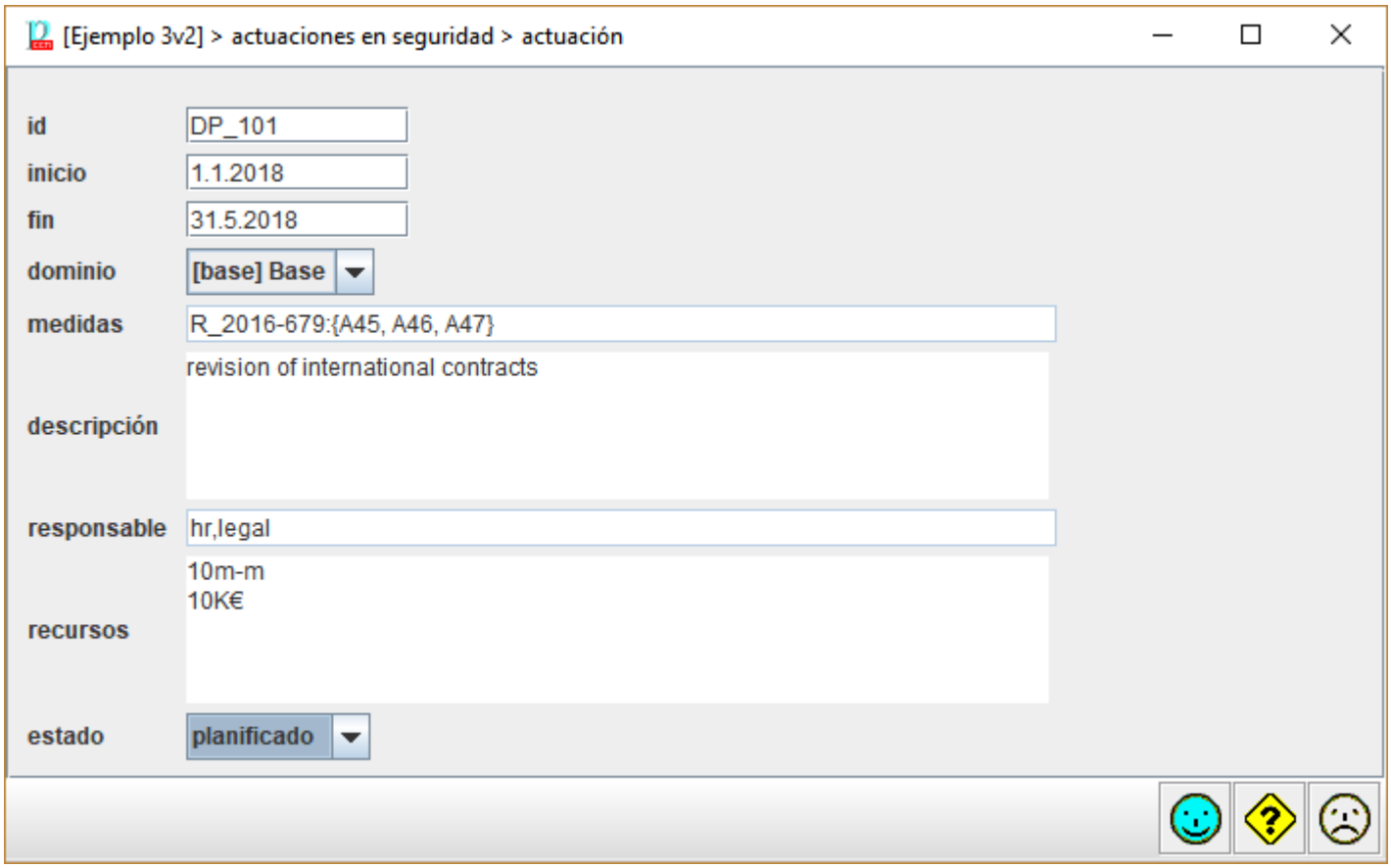
	Permite seleccionar algunas filas; haga clic para seleccionar u olvidar; con la tecla de mayúsculas puede seleccionar un rango
	Haga clic para editar la actuación de la fila
id	Un identificador de la actuación; debería ser un identificador singular, sin duplicados
inicio	Fecha de inicio. Formato día.mes.año.
fin	Fecha de terminación. Formato día.mes.año.
dominio	
descripción	Una descripción textual de la actuación.
responsable	Referencia a las fuentes de información.
recursos	Descripción textual de los recursos requeridos, típicamente esfuerzo humano y económico.
estado	{ planificado, en curso, suspendido, hecho }

Puede seleccionar una o más actuaciones y hacer MAYÚSCULA-ARRIBA para desplazarlas hacia arriba.

Puede seleccionar una o más actuaciones y hacer MAYÚSCULA-ABAJO para desplazarlas hacia abajo.

8.12.1 Actuación en seguridad

Permite introducir datos que describen la actuación.



id

escriba un identificador de la actuación; debería ser un nombre singular, no duplicado

inicio

fecha de inicio; formato: día.mes.año; ejemplo: 21.12.2002

fin

fecha terminación inicio; formato: día.mes.año; ejemplo: 21.12.2002

medidas

haga clic para seleccionar medidas de seguridad; pueden ser salvaguardas técnicas o controles de algún perfil de evaluación

haga clic para valorar la madurez de las salvaguardas y controles seleccionados

dominio

seleccione el dominio de seguridad sobre el que se actúa

descripción

describa la actuación; texto libre

responsable

referencia fuentes de información

recursos

describa los recursos necesarios, típicamente esfuerzo humano y económico; texto libre

estado

estado de la actuación: { planificado, en curso, suspendido, hecho }

8.13 Escenarios de riesgo

En su versión clásica, PILAR asocia amenazas TIC a los activos del sistema, amenazas que afectan a las dimensiones TIC (confidencialidad, integridad, etc.) y calcula el efecto mitigador de medidas de seguridad TIC para estimar el riesgo residual.

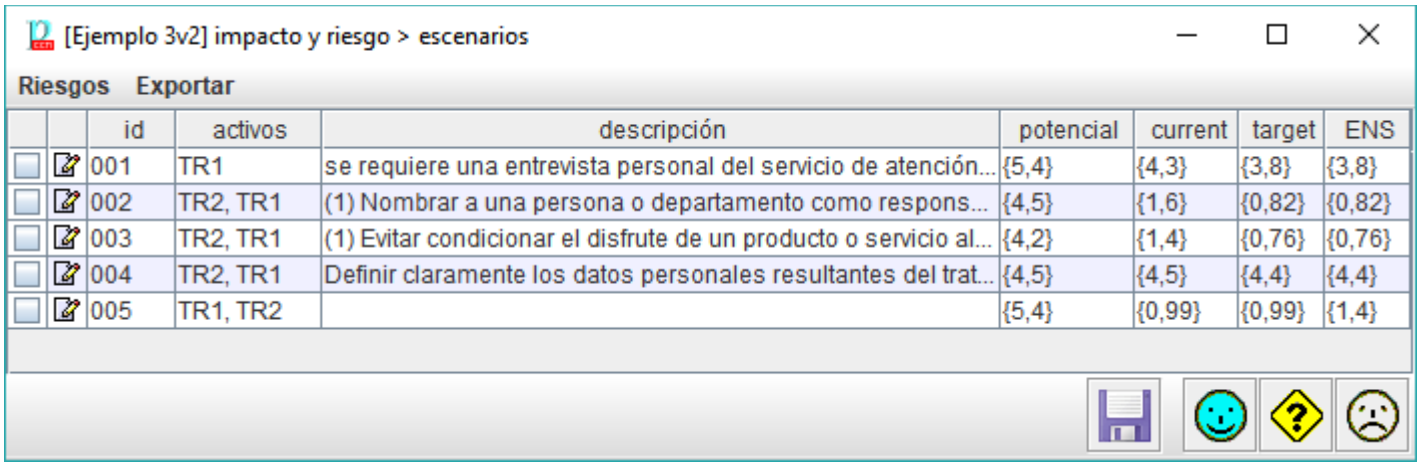
El mismo planteamiento de

$$\frac{activos \times amenazas}{medidas\ de\ protección}$$

se puede aplicar en escenarios más amplios. En lo que sigue lo aplicaremos a los aspectos jurídicos (riesgo legal) de los activos que tienen valor por su carácter personal.

El planteamiento es asociar amenazas sobre los aspectos legales del tratamiento de datos personales, y aplicar medidas que atajen dichas amenazas.

El valor lo determina la valoración del activo en la dimensión de privacidad. La amenaza debe identificarse junto con su impacto sobre el valor del activo y la probabilidad estimada de ocurrencia (ARO). Las medidas que se adopten reducen el riesgo. Todo ello dentro del marco unificado de estimación de riesgos potenciales y residuales.



		id	activos	descripción	potencial	current	target	ENS
☐	✎	001	TR1	se requiere una entrevista personal del servicio de atención...	{5,4}	{4,3}	{3,8}	{3,8}
☐	✎	002	TR2, TR1	(1) Nombrar a una persona o departamento como respons...	{4,5}	{1,6}	{0,82}	{0,82}
☐	✎	003	TR2, TR1	(1) Evitar condicionar el disfrute de un producto o servicio al...	{4,2}	{1,4}	{0,76}	{0,76}
☐	✎	004	TR2, TR1	Definir claramente los datos personales resultantes del trat...	{4,5}	{4,5}	{4,4}	{4,4}
☐	✎	005	TR1, TR2		{5,4}	{0,99}	{0,99}	{1,4}

Menú barra superior

Riesgos	**nuevo** permite crear una fila más en la tabla de escenarios de riesgos **editar** permite modificar un escenario de riesgo **eliminar** elimina una fila de la tabla de escenarios de riesgo
Exportar	**CSV** vacía la tabla de escenarios en formato CSV para Excel **XML** vacía la tabla de riesgos en formato XML

Opciones barra inferior

	Guarda el proyecto en su fichero o en su base de datos.
	ACEPTAR. Se guardan los cambios realizados y se cierra la ventana.
	CANCELAR. Se desestiman los cambios y se cierra la ventana.
	AYUDA. Abre un navegador con estas páginas de ayuda.

Tabla

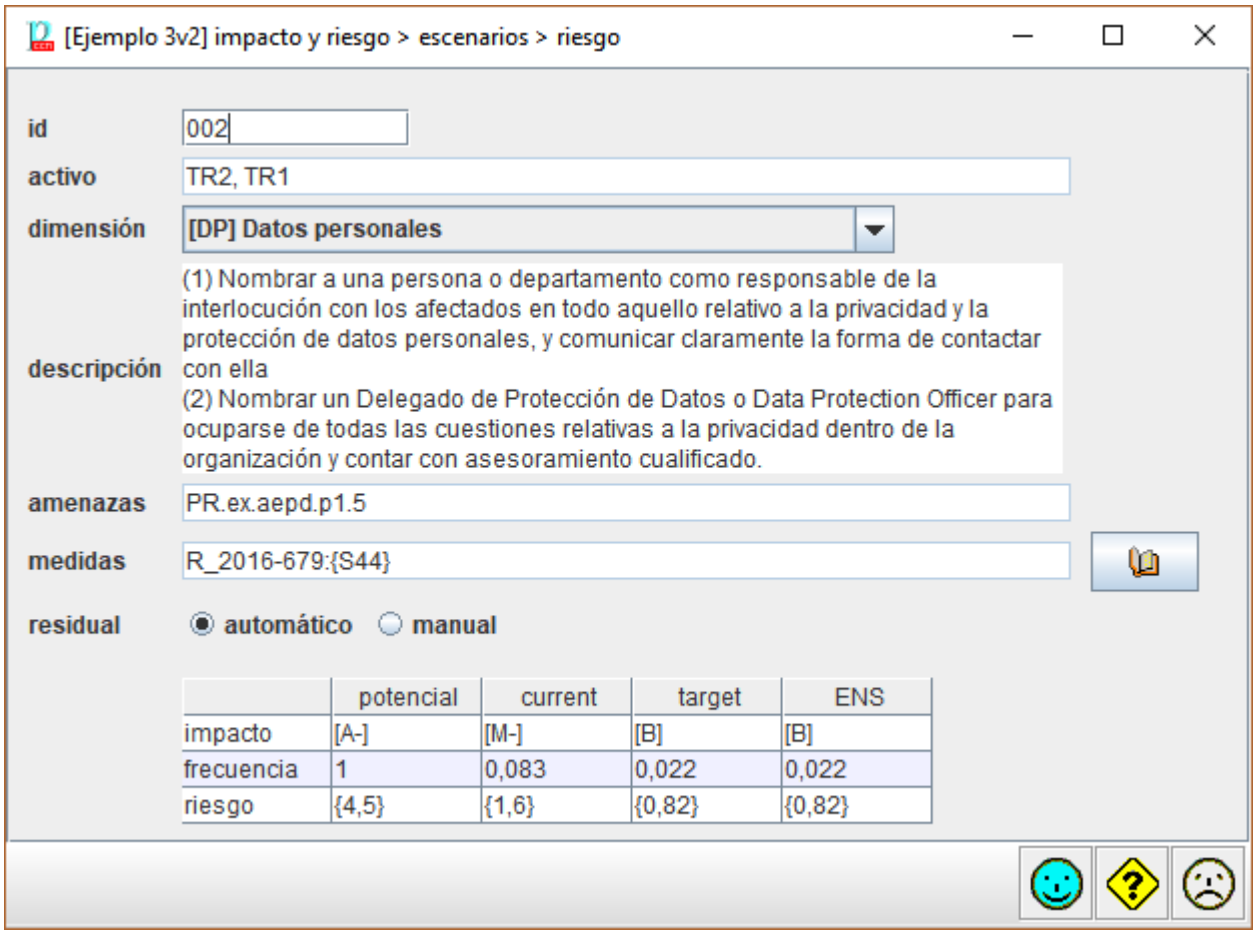
	Permite seleccionar algunas filas; haga clic para seleccionar u olvidar; con la tecla de mayúsculas puede seleccionar un rango
	Haga clic para editar el escenario de riesgo de la fila
id	Un identificador del escenario; debería ser un identificador singular, sin duplicados
activos	Uno o más activos a los que afecta el escenario descrito
descripción	Una descripción textual del escenario de riesgo. Puede describir la amenaza y puede describir las medidas tomadas para atajarla.
fases	Tantas columnas como fases del proyecto, empezando por la fase potencial (riesgo inherente). Muestra el riesgo en cada fase.

Puede seleccionar uno o más escenarios y hacer MAYÚSCULA-ARRIBA para desplazarlos hacia arriba.

Puede seleccionar uno o más escenarios y hacer MAYÚSCULA-ABAJO para desplazarlos hacia abajo.

8.13.1 Edición de un escenario de riesgo

Permite introducir datos que describen el escenario de riesgo.



id

escriba un identificador del escenario; debería ser un nombre singular, no duplicado

activo

haga clic en la zona de texto para seleccionar uno o más activos objeto del escenario de riesgo

dimensión

haga clic en el combo para seleccionar la dimensión de seguridad que se ve afectada

descripción

describa el escenario; habitualmente se describe la amenaza y las medidas adoptadas para atajarla

amenazas

haga clic para seleccionar las amenazas dentro del catálogo de PILAR

medidas

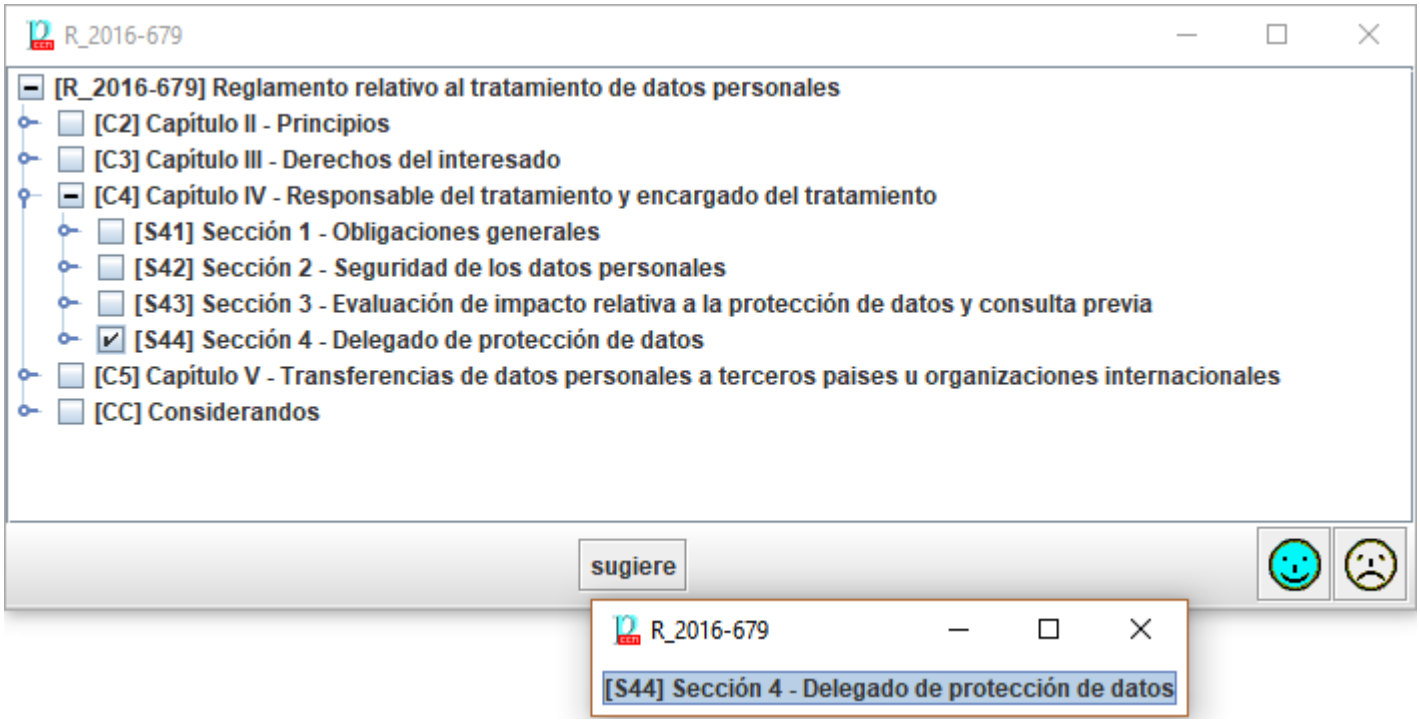
haga clic para seleccionar que medidas o controles de perfiles de seguridad actúan en el escenario descrito

haga clic para valorar la madurez de las salvaguardas y controles seleccionados

residual

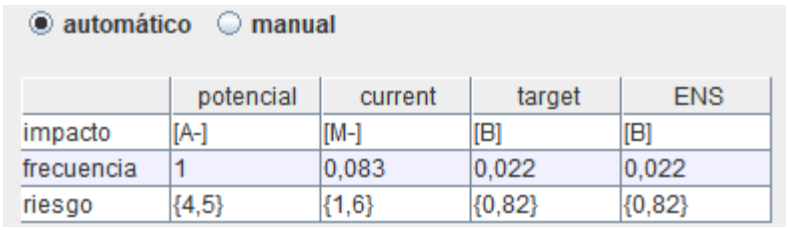
la evolución del riesgo puede ser automática o manual

Para seleccionar salvaguardas y controles, PILAR puede sugerir elementos que parecen adecuados para la dimensión y la amenaza utilizadas. Es solamente una sugerencia.



8.13.2 Cálculo automático del riesgo residual

Una vez seleccionadas las salvaguardas y controles con un efecto sobre el escenario descrito, podemos ver su valoración en términos de madurez ( ) y pedir a aplique dicha madurez como mitigador del riesgo. Esto, para cada fase del proyecto, incluida la pseudo fase de recomendación de PILAR.



	potencial	current	target	ENS
impacto	[A-]	[M-]	[B]	[B]
frecuencia	1	0,083	0,022	0,022
riesgo	{4,5}	{1,6}	{0,82}	{0,82}

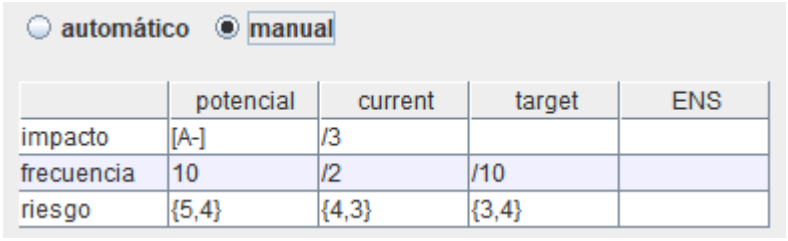
El impacto potencial es el valor asignado al activo en la dimensión que nos afecta.

La probabilidad potencial se introduce manualmente.

PILAR calcula las demás entradas de la tabla.

8.13.3 Cálculo manual del riesgo residual

En modo manual indicaremos en qué medida se reduce el impacto y la probabilidad en cada fase del proyecto



	potencial	current	target	ENS
impacto	[A-]	/3		
frecuencia	10	/2	/10	
riesgo	{5,4}	{4,3}	{3,4}	

El impacto potencial es el valor asignado al activo en la dimensión que nos afecta.

La probabilidad potencial se introduce manualmente.

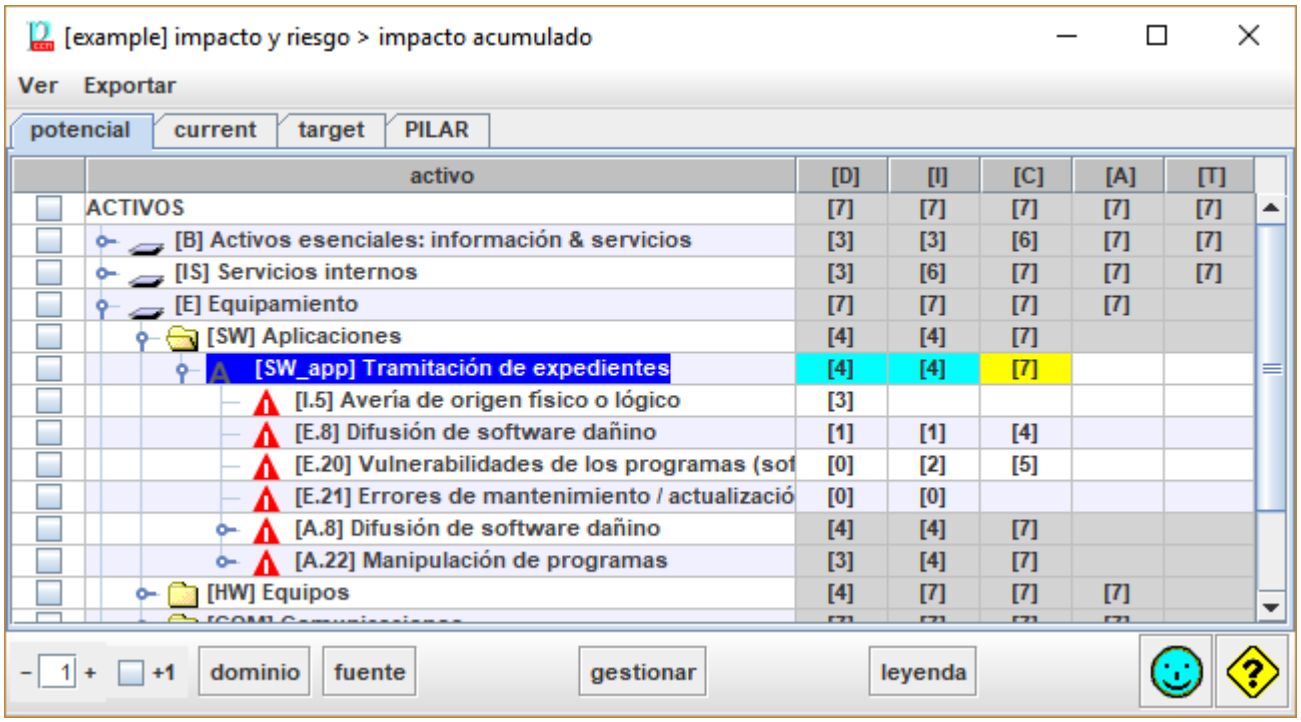
En cada fase, podemos indicar la reducción estimada. Lo más normal es aplicar un cociente reductor. PILAR calcula el riesgo dados el impacto y la probabilidad estimadas.

8.14 Impacto y Riesgo

8.14.1 Niveles de criticidad – Código de colores

PILAR presenta los niveles de riesgo en el rango 0.00 a 9.9, con un coloreado para realzar la visibilidad:

8.14.2 Impacto acumulado



Hay una pestaña por fase del proyecto. Haga clic para cambiar.

La pseudo fase POTENCIAL muestra el impacto potencial (sin salvaguarda alguna).

Menú superior VER

capas	árbol organizado por capas, luego por activos
zonas lógicas	árbol organizado por zonas lógicas, luego por activos
zonas físicas	árbol organizado por zonas físicas, luego por activos
zonas tempest	árbol organizado por zonas tempest, luego por activos
amenazas	árbol organizado por amenazas, luego por activos

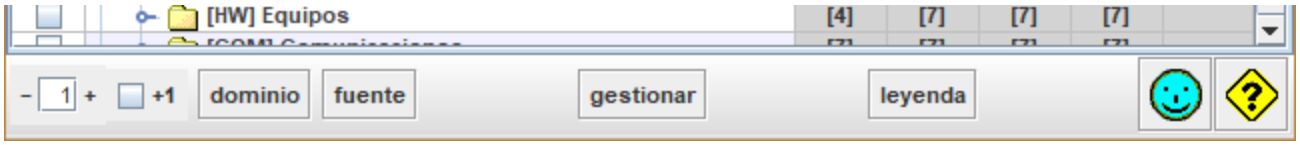
Menú superior EXPORTAR

html	exporta las filas seleccionadas a formato HTML, para la web
csv	exporta las filas seleccionadas a formato CSV, para Excel
xml	exporta las filas seleccionadas a formato XML
db	exporta las filas seleccionadas a una base de datos. solamente si está activado del módulo SQL

Columnas de la tabla

selección	Haga clic en las cajitas para seleccionar / deseleccionar. Haga MAYÚSCULAS + clic para seleccionar un rango. Haga clic en la cabecera de la columna para eliminar la selección actual. La selección determina a qué filas se aplica GESTIONAR
activos	Activos y amenazas
dimensiones	Una columna por dimensión de seguridad. Haga clic en la cabecera para tener una *vista alternativa*, por dimensión.
	Valores de impacto. El impacto se evalúa por amenaza, y se agrega por activos, grupos y capas.

Barra inferior

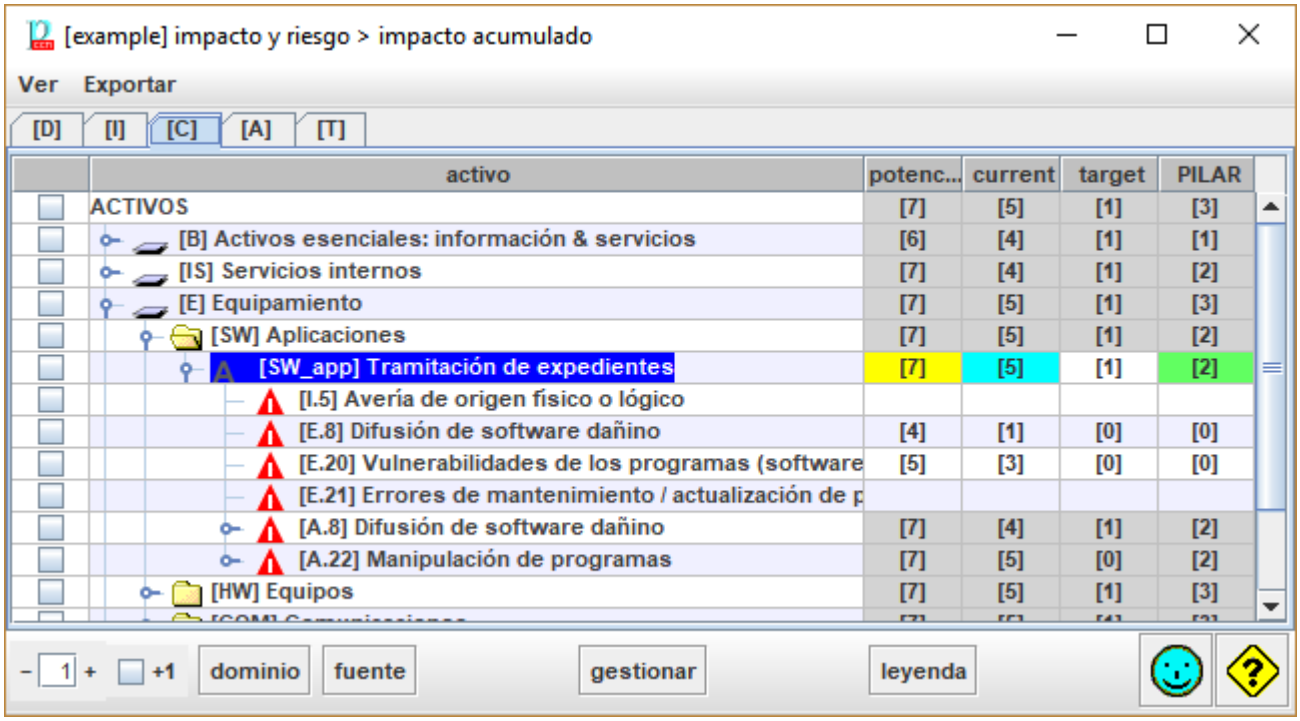


– 1 +	Para controlar el despliegue del árbol de activos.
+1	Ajusta la expansión del *spinner*. Si se marca, se incluyen las amenazas en el árbol.
dominio	Seleccione un dominio de seguridad. PILAR seleccionará los activos en ese dominio.
fuente	Seleccione una o más fuentes de información. PILAR seleccionará los activos asociados a esa fuente.

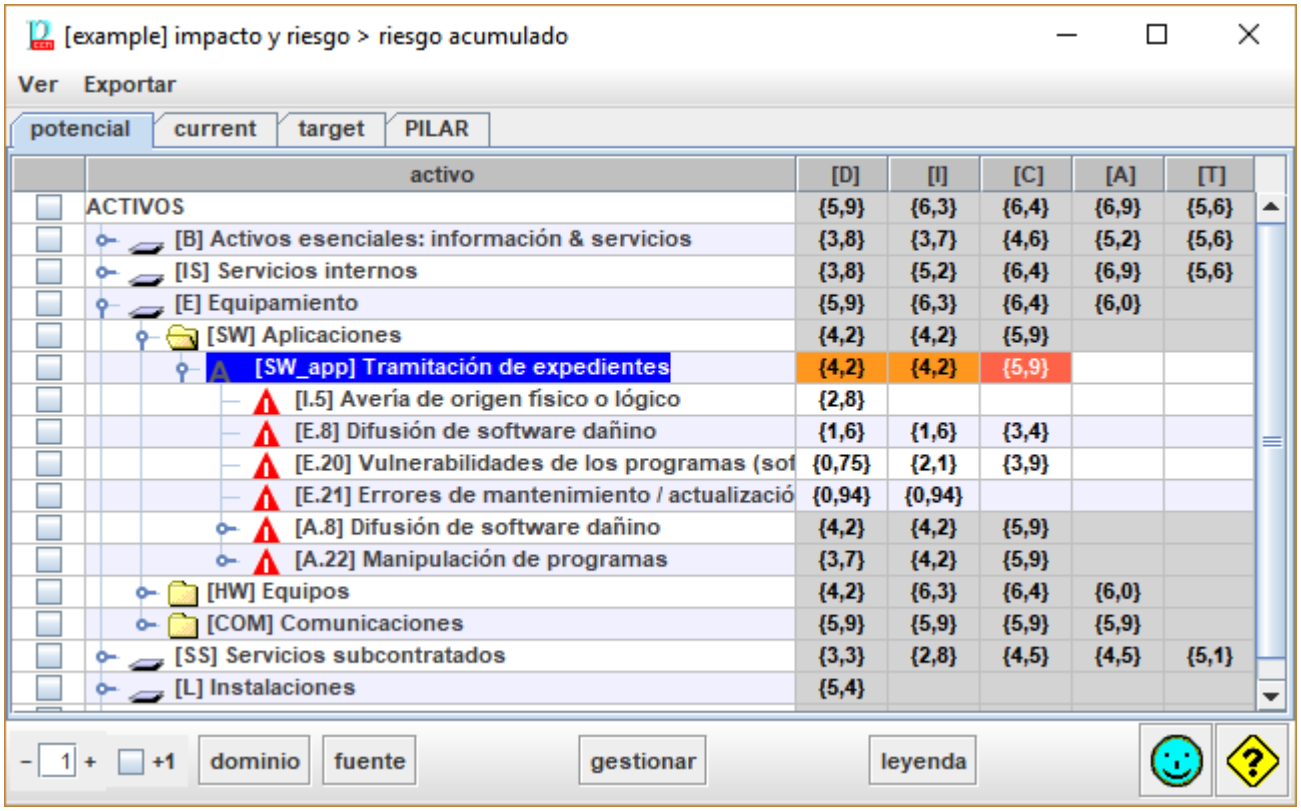
gestionar	Para las filas seleccionadas en la columna 1, PILAR recolecta los riesgos asociados y salta a la ventana de *valoración de salvaguardas*, teniendo en cuenta solo dichos riesgos.
leyenda	niveles y colores de las valoraciones de impacto

8.14.2.1 Vista alternativa

Si hace clic en la cabecera de una columna, PILAR conmuta entre columnas y pestañas:



8.14.3 Riesgo acumulado



Hay una pestaña por fase del proyecto. Haga clic para cambiar.
La pseudo-fase POTENCIAL muestra el riesgo potencial (sin salvaguarda alguna).

Menú superior VER

capas	árbol organizado por capas, luego por activos
zonas lógicas	árbol organizado por zonas lógicas, luego por activos
zonas físicas	árbol organizado por zonas físicas, luego por activos
zonas tempest	árbol organizado por zonas tempest, luego por activos
amenazas	árbol organizado por amenazas, luego por activos

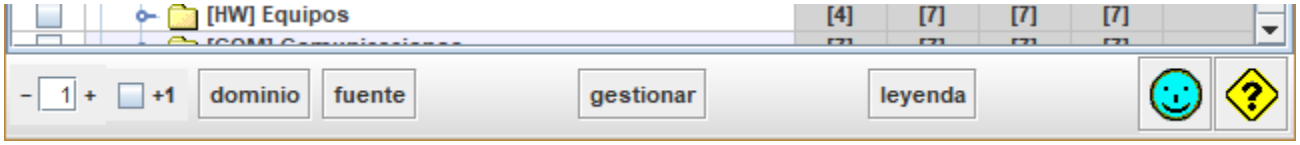
Menú superior EXPORTAR

html	exporta las filas seleccionadas a formato HTML, para la web
csv	exporta las filas seleccionadas a formato CSV, para Excel
xml	exporta las filas seleccionadas a formato XML
db	exporta las filas seleccionadas a una base de datos. solamente si está activado del módulo SQL

Columnas de la tabla

selección	Haga clic en las cajitas para seleccionar / deseleccionar. Haga MAYÚSCULAS + clic para seleccionar un rango. Haga clic en la cabecera de la columna para eliminar la selección actual. La selección determina a qué filas se aplica GESTIONAR.
activos	Activos y amenazas
dimensiones	Una columna por dimensión de seguridad. Haga clic en la cabecera para tener una *vista alternativa*, por dimensión.
	Valores de riesgo. El riesgo se evalúa por amenaza, y se agrega por activos, grupos y capas.

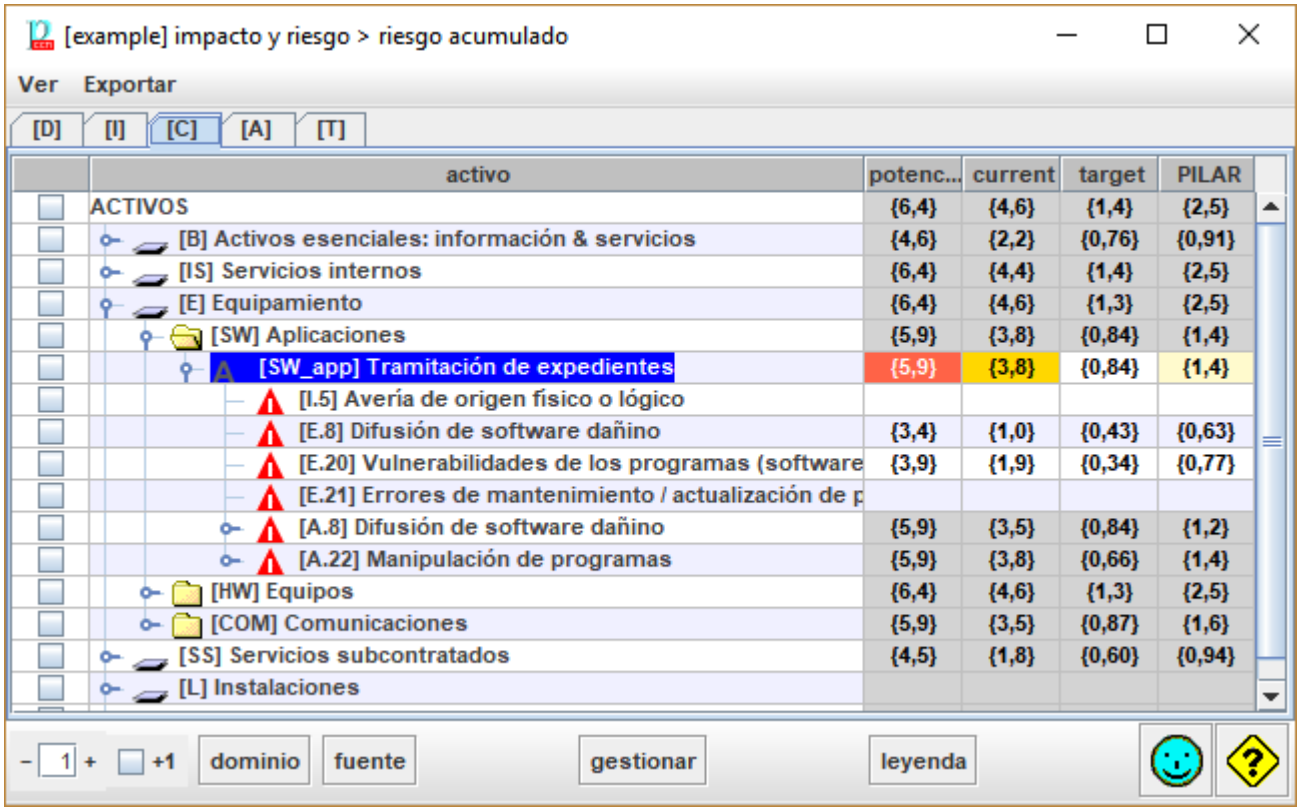
Barra inferior



	Para controlar el despliegue del árbol de activos.
+1	Ajusta la expansión del *spinner*. Si se marca, se incluyen las amenazas en el árbol.
dominio	Seleccione un dominio de seguridad. PILAR seleccionará los activos en ese dominio.
fuente	Seleccione una o más fuentes de información. PILAR seleccionará los activos asociados a esa fuente.
gestionar	Para las filas seleccionadas en la columna 1, PILAR recolecta los riesgos asociados y salta a la ventana de *valoración de salvaguardas*, teniendo en cuenta solo dichos riesgos.
leyenda	niveles y colores de las valoraciones de impacto

8.14.3.1 Vista alternativa

Si hace clic en la cabecera de una columna, PILAR conmuta entre columnas y pestañas:



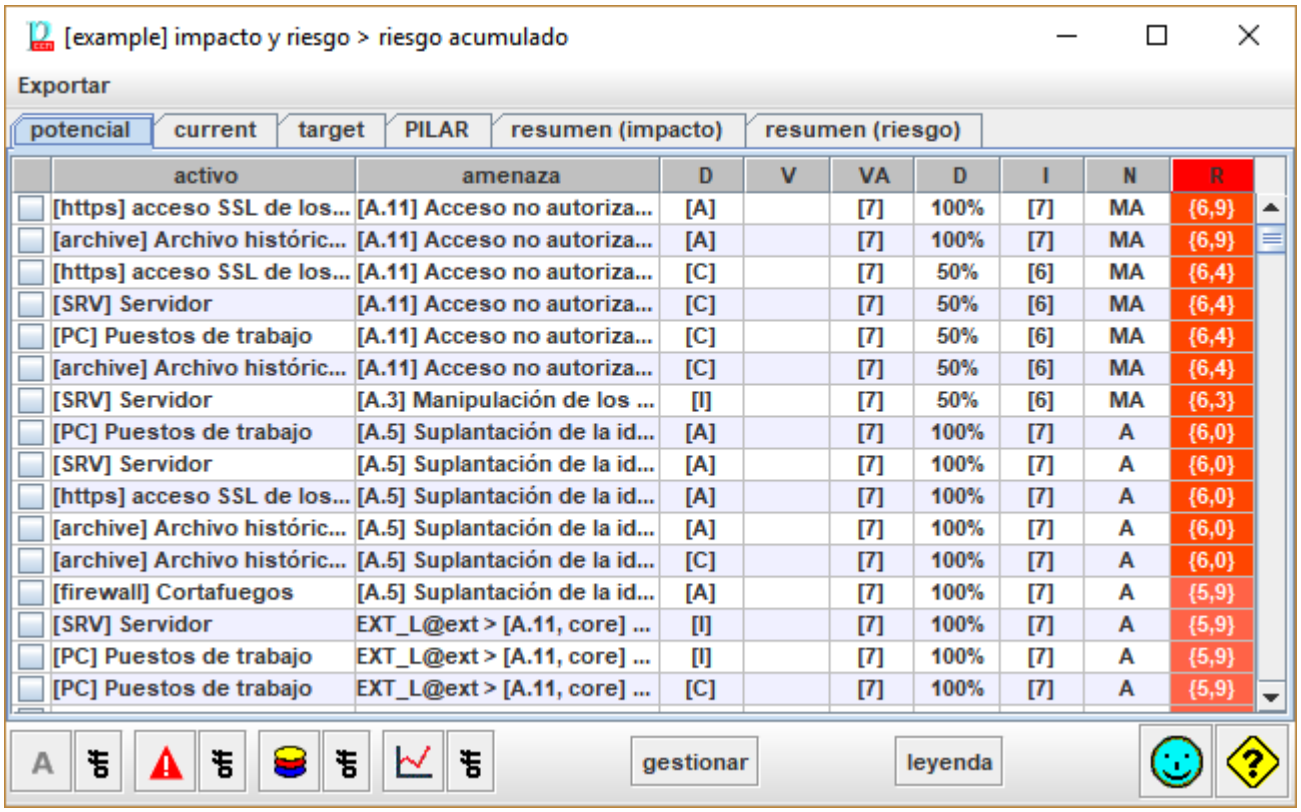
8.14.4 Tabla de impacto y riesgo acumulado

Una por fase del proyecto. Haga clic para seleccionar.

La pseudo fase POTENCIAL muestra los valores inherentes, sin salvaguarda alguna.

Ver *resumen (impacto)*

Ver *resumen (riesgo)*



activo	amenaza	D	V	VA	D	I	N	R
[https] acceso SSL de los...	[A.11] Acceso no autoriza...	[A]		[7]	100%	[7]	MA	{6,9}
[archive] Archivo histórico...	[A.11] Acceso no autoriza...	[A]		[7]	100%	[7]	MA	{6,9}
[https] acceso SSL de los...	[A.11] Acceso no autoriza...	[C]		[7]	50%	[6]	MA	{6,4}
[SRV] Servidor	[A.11] Acceso no autoriza...	[C]		[7]	50%	[6]	MA	{6,4}
[PC] Puestos de trabajo	[A.11] Acceso no autoriza...	[C]		[7]	50%	[6]	MA	{6,4}
[archive] Archivo histórico...	[A.11] Acceso no autoriza...	[C]		[7]	50%	[6]	MA	{6,4}
[SRV] Servidor	[A.3] Manipulación de los ...	[I]		[7]	50%	[6]	MA	{6,3}
[PC] Puestos de trabajo	[A.5] Suplantación de la id...	[A]		[7]	100%	[7]	A	{6,0}
[SRV] Servidor	[A.5] Suplantación de la id...	[A]		[7]	100%	[7]	A	{6,0}
[https] acceso SSL de los...	[A.5] Suplantación de la id...	[A]		[7]	100%	[7]	A	{6,0}
[archive] Archivo histórico...	[A.5] Suplantación de la id...	[A]		[7]	100%	[7]	A	{6,0}
[archive] Archivo histórico...	[A.5] Suplantación de la id...	[C]		[7]	100%	[7]	A	{6,0}
[firewall] Cortafuegos	[A.5] Suplantación de la id...	[A]		[7]	100%	[7]	A	{5,9}
[SRV] Servidor	EXT_L@ext > [A.11, core] ...	[I]		[7]	100%	[7]	A	{5,9}
[PC] Puestos de trabajo	EXT_L@ext > [A.11, core] ...	[I]		[7]	100%	[7]	A	{5,9}
[PC] Puestos de trabajo	EXT_L@ext > [A.11, core] ...	[C]		[7]	100%	[7]	A	{5,9}

Columnas de la tabla

Puede hacer clic en la cabecera de cualquier columna. PILAR ordena los datos de acuerdo a la columna seleccionada. La cabecera de la columna seleccionada se pone ROJA.

activo – el activo

amenaza – la amenaza

dimensión – la dimensión de seguridad

V – el valor propio del activo en esa dimensión, si lo tiene

VA – el valor acumulado del activo en esa dimensión

D – la degradación causada por la amenaza (ver "*Opciones / Efectos*")

I – el impacto

N – la probabilidad (ver *Opciones / Probabilidad*

R – el riesgo

Menú superior EXPORTAR

csv	Exporta valores en formato CSV (Comma Separated Values), para excel.
xml	Exporta valores en formato XML.
db	Exporta valores a una base de datos.

Barra inferior

	Filtro de activos: solo se presentan los activos seleccionados. Haga clic en la imagen para seleccionar activos. Haga clic en ON / OFF para activar / desactivar el filtro.
	Filtro de amenazas: solo se presentan las amenazas seleccionadas. Haga clic en la imagen para seleccionar amenazas. Haga clic en ON / OFF para activar / desactivar el filtro.
	Filtro de dimensiones: solo se presentan las dimensiones seleccionadas. Haga clic en la imagen para seleccionar dimensiones. Haga clic en ON / OFF para activar / desactivar el filtro.
	Filtro para ver solo algunos riesgos. Haga clic en la imagen para elegir la fracción que desea ver. Puede elegir un porcentaje para impacto y un porcentaje para riesgos. Los valores típicos son 10% y 10%, seleccionando el 10% de mayor impacto y el 10% de mayor riesgo (es decir, la parte superior derecha de la tabla de impacto-probabilidad)  0% implica no ver ninguno. 100% sería como eliminar el filtro. Haga clic en ON / OFF para activar / desactivar el filtro.
gestionar	Para las filas seleccionadas en la columna 1, PILAR recolecta los riesgos asociados y salta a la ventana de *valoración de salvaguardas*, teniendo en cuenta solo dichos riesgos.
leyenda	Ver *Riesgos / Niveles de criticidad / código de colores*

Inicialmente, los datos se ordenan por riesgo, después por impacto y por ultimo por probabilidad.

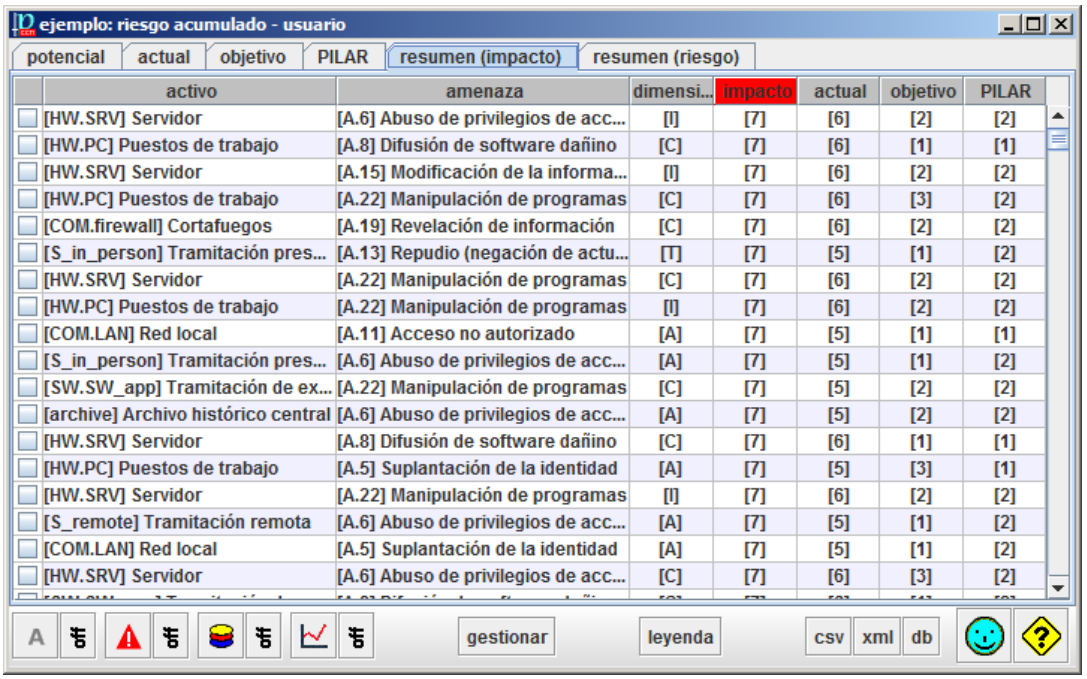
Si hace clic en una cabecera, PILAR ordena por dicha cabecera:

activos	ordenado según su posición en el árbol de activos (ascendente)
amenazas	ordenado según su posición en el árbol de amenazas (ascendente)
dimensión	ordenado según su posición en la lista de dimensiones (ascendente)
V	ordenado por el valor de activo (descendente)
A	ordenado por el valor acumulado (descendente)
D	ordenado por la degradación (descendente)
I	ordenado por el impacto (descendente)
F	ordenado por la probabilidad (descendente)

riesgo	ordenado por el riesgo (descendente)

8.14.4.1 Resumen de impacto

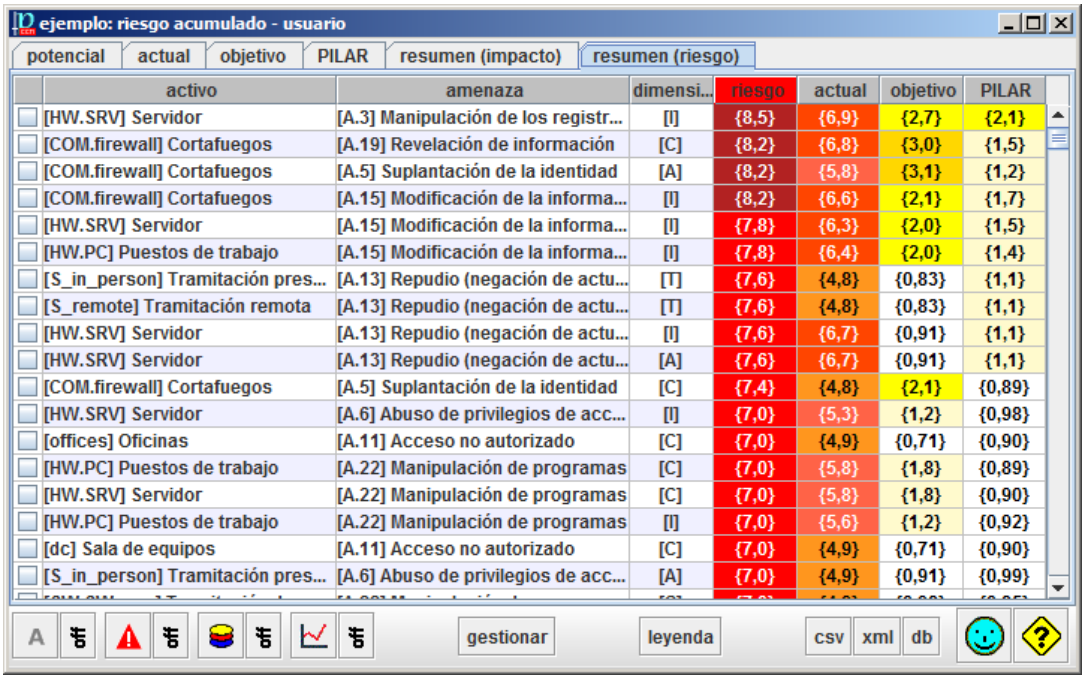
PILAR presenta la evolución del impacto a lo largo de las fases del proyecto:



activo	amenaza	dimensi...	impacto	actual	objetivo	PILAR
[HW.SRV] Servidor	[A.6] Abuso de privilegios de acc...	[I]	[7]	[6]	[2]	[2]
[HW.PC] Puestos de trabajo	[A.8] Difusión de software dañino	[C]	[7]	[6]	[1]	[1]
[HW.SRV] Servidor	[A.15] Modificación de la informa...	[I]	[7]	[6]	[2]	[2]
[HW.PC] Puestos de trabajo	[A.22] Manipulación de programas	[C]	[7]	[6]	[3]	[2]
[COM.firewall] Cortafuegos	[A.19] Revelación de información	[C]	[7]	[6]	[2]	[2]
[S_in_person] Tramitación pres...	[A.13] Repudio (negación de actu...	[T]	[7]	[5]	[1]	[2]
[HW.SRV] Servidor	[A.22] Manipulación de programas	[C]	[7]	[6]	[2]	[2]
[HW.PC] Puestos de trabajo	[A.22] Manipulación de programas	[I]	[7]	[6]	[2]	[2]
[COM.LAN] Red local	[A.11] Acceso no autorizado	[A]	[7]	[5]	[1]	[1]
[S_in_person] Tramitación pres...	[A.6] Abuso de privilegios de acc...	[A]	[7]	[5]	[1]	[2]
[SW.SW_app] Tramitación de ex...	[A.22] Manipulación de programas	[C]	[7]	[5]	[2]	[2]
[archive] Archivo histórico central	[A.6] Abuso de privilegios de acc...	[A]	[7]	[5]	[2]	[2]
[HW.SRV] Servidor	[A.8] Difusión de software dañino	[C]	[7]	[6]	[1]	[1]
[HW.PC] Puestos de trabajo	[A.5] Suplantación de la identidad	[A]	[7]	[5]	[3]	[1]
[HW.SRV] Servidor	[A.22] Manipulación de programas	[I]	[7]	[6]	[2]	[2]
[S_remote] Tramitación remota	[A.6] Abuso de privilegios de acc...	[A]	[7]	[5]	[1]	[2]
[COM.LAN] Red local	[A.5] Suplantación de la identidad	[A]	[7]	[5]	[1]	[2]
[HW.SRV] Servidor	[A.6] Abuso de privilegios de acc...	[C]	[7]	[6]	[3]	[2]

8.14.4.2 Resumen de riesgo

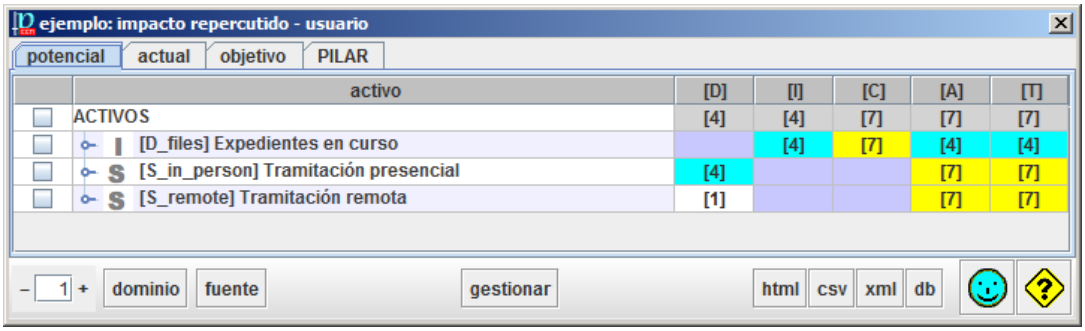
PILAR presenta la evolución del riesgo a lo largo de las fases del proyecto:



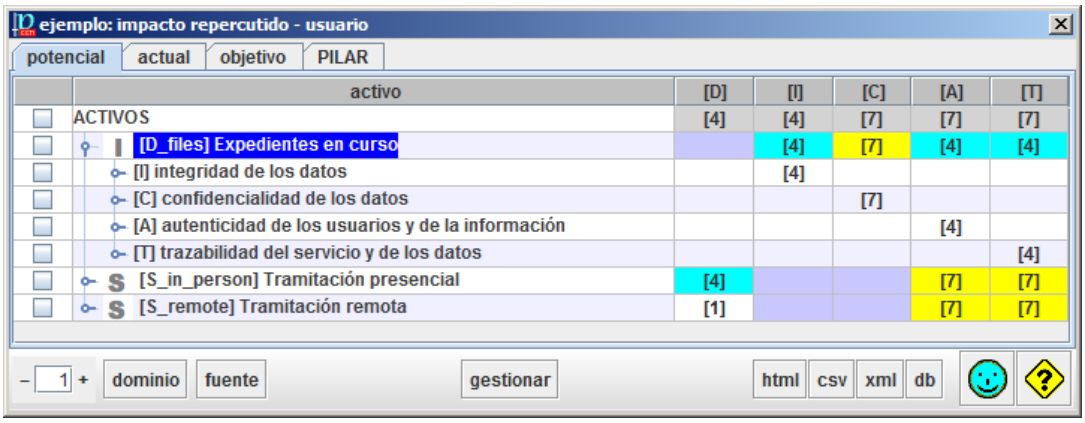
activo	amenaza	dimensi...	riesgo	actual	objetivo	PILAR
[HW.SRV] Servidor	[A.3] Manipulación de los registr...	[I]	{8,5}	{6,9}	{2,7}	{2,1}
[COM.firewall] Cortafuegos	[A.19] Revelación de información	[C]	{8,2}	{6,8}	{3,0}	{1,5}
[COM.firewall] Cortafuegos	[A.5] Suplantación de la identidad	[A]	{8,2}	{5,8}	{3,1}	{1,2}
[COM.firewall] Cortafuegos	[A.15] Modificación de la informa...	[I]	{8,2}	{6,6}	{2,1}	{1,7}
[HW.SRV] Servidor	[A.15] Modificación de la informa...	[I]	{7,8}	{6,3}	{2,0}	{1,5}
[HW.PC] Puestos de trabajo	[A.15] Modificación de la informa...	[I]	{7,8}	{6,4}	{2,0}	{1,4}
[S_in_person] Tramitación pres...	[A.13] Repudio (negación de actu...	[T]	{7,6}	{4,8}	{0,83}	{1,1}
[S_remote] Tramitación remota	[A.13] Repudio (negación de actu...	[T]	{7,6}	{4,8}	{0,83}	{1,1}
[HW.SRV] Servidor	[A.13] Repudio (negación de actu...	[I]	{7,6}	{6,7}	{0,91}	{1,1}
[HW.SRV] Servidor	[A.13] Repudio (negación de actu...	[A]	{7,6}	{6,7}	{0,91}	{1,1}
[COM.firewall] Cortafuegos	[A.5] Suplantación de la identidad	[C]	{7,4}	{4,8}	{2,1}	{0,89}
[HW.SRV] Servidor	[A.6] Abuso de privilegios de acc...	[I]	{7,0}	{5,3}	{1,2}	{0,98}
[offices] Oficinas	[A.11] Acceso no autorizado	[C]	{7,0}	{4,9}	{0,71}	{0,90}
[HW.PC] Puestos de trabajo	[A.22] Manipulación de programas	[C]	{7,0}	{5,8}	{1,8}	{0,89}
[HW.SRV] Servidor	[A.22] Manipulación de programas	[C]	{7,0}	{5,8}	{1,8}	{0,90}
[HW.PC] Puestos de trabajo	[A.22] Manipulación de programas	[I]	{7,0}	{5,6}	{1,2}	{0,92}
[dc] Sala de equipos	[A.11] Acceso no autorizado	[C]	{7,0}	{4,9}	{0,71}	{0,90}
[S_in_person] Tramitación pres...	[A.6] Abuso de privilegios de acc...	[A]	{7,0}	{4,9}	{0,91}	{0,99}

8.14.5 Impacto repercutido

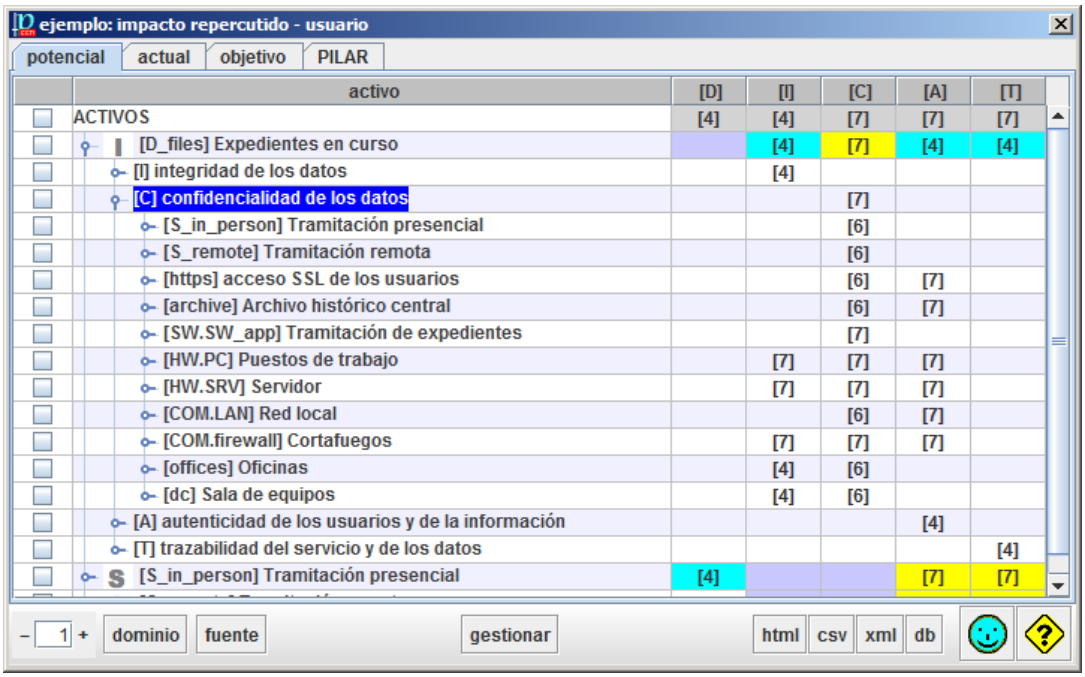
PILAR presenta el impacto repercutido sobre los activos con valor propio:



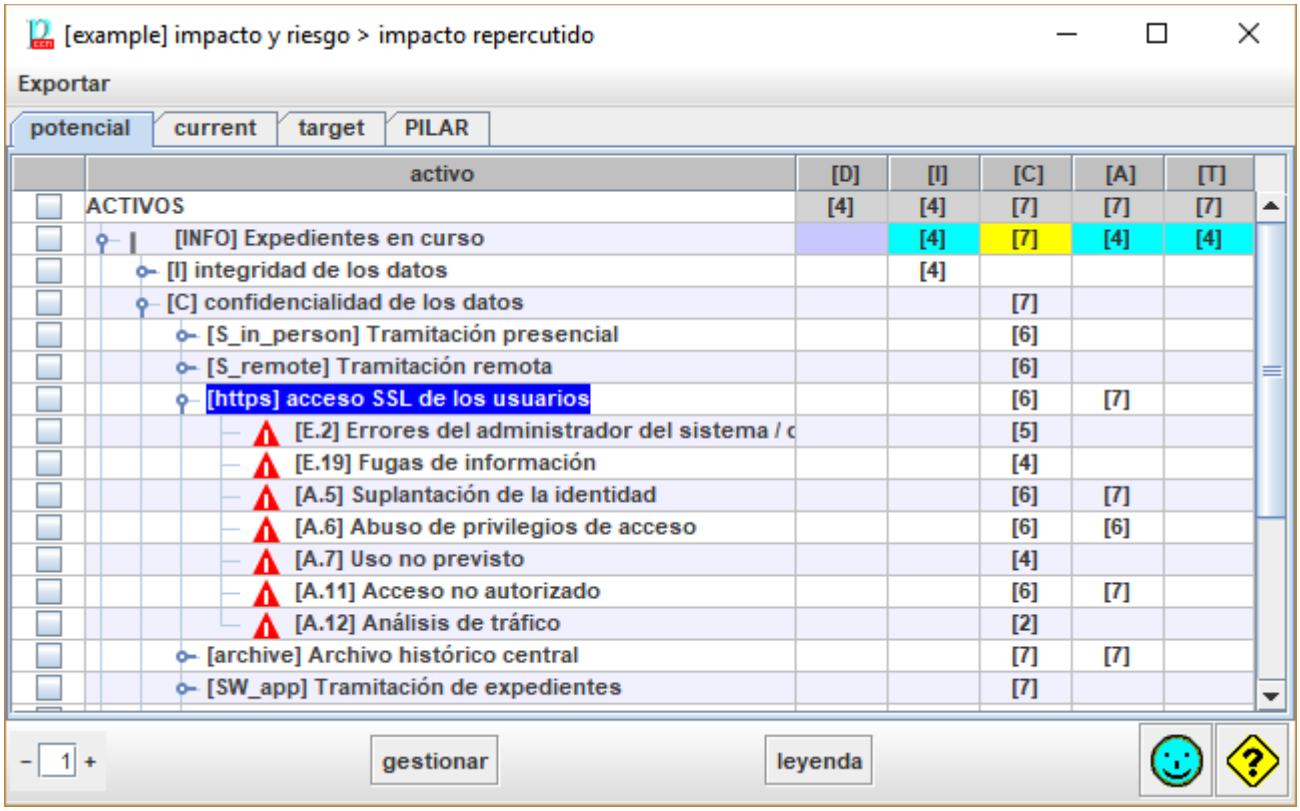
Puede expandir el árbol para segregar cada dimensión:



Puede seguir expandiendo el árbol para ver cómo es afectada cada dimensión en los activos de los que depende:



Y puede llegar a amenazas concretas:



Pestañas - Una por fase del proyecto. Haga clic para cambiar.

Menú superior EXPORTAR

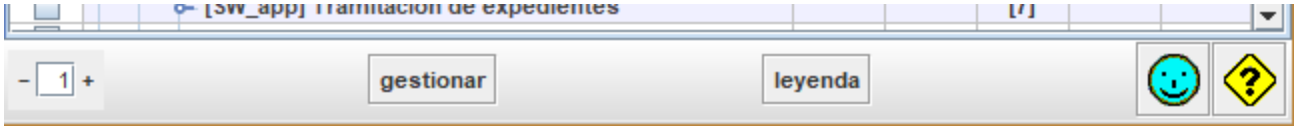
html	exporta las filas seleccionadas a formato HTML, para la web
csv	exporta las filas seleccionadas a formato CSV, para Excel
xml	exporta las filas seleccionadas a formato XML
db	exporta las filas seleccionadas a una base de datos. solamente si está activado del módulo SQL

Columnas de la tabla

1	**selección**	Haga clic en las cajitas para seleccionar / deseleccionar. Haga MAYÚSCULAS + clic para seleccionar un rango. Haga clic en la cabecera de la columna para eliminar la selección actual. La selección determina a qué filas se aplica GESTIONAR.
2	**activos**	Activos y amenazas
3	**dimensiones**	Una columna por dimensión de seguridad.

		Haga clic en la cabecera para tener una *vista alternativa*, por dimensión.

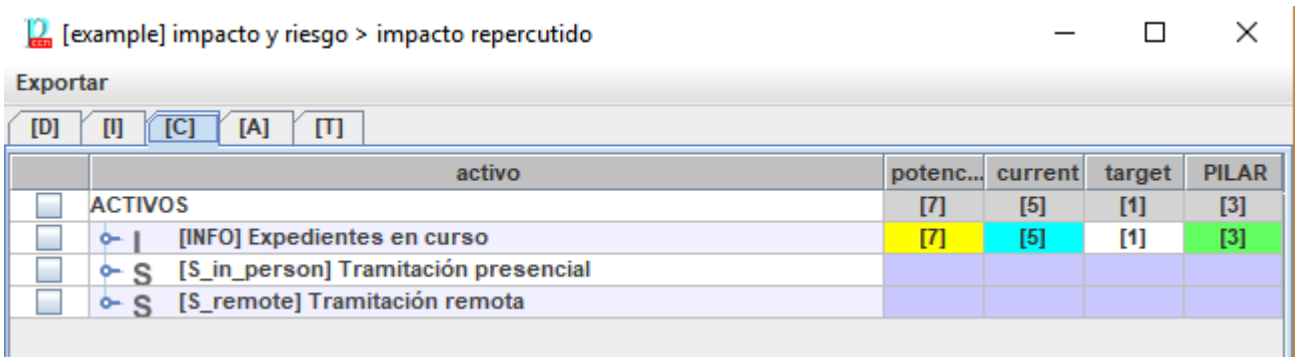
Barra inferior



- 1 +	Para controlar el despliegue del árbol
gestionar	Para las filas seleccionadas en la columna 1, PILAR recolecta los riesgos asociados y salta a la ventana de *valoración de salvaguardas*, teniendo en cuenta solo dichos riesgos.
leyenda	Niveles y colores de los valores de riesgo.

8.14.5.1 Vista alternativa

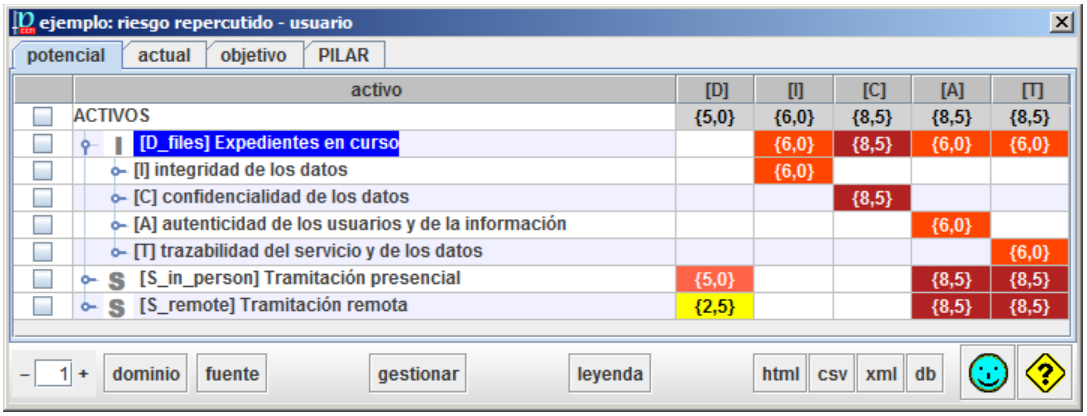
Si hace clic en la cabecera de una columna, PILAR conmuta entre columnas y pestañas:



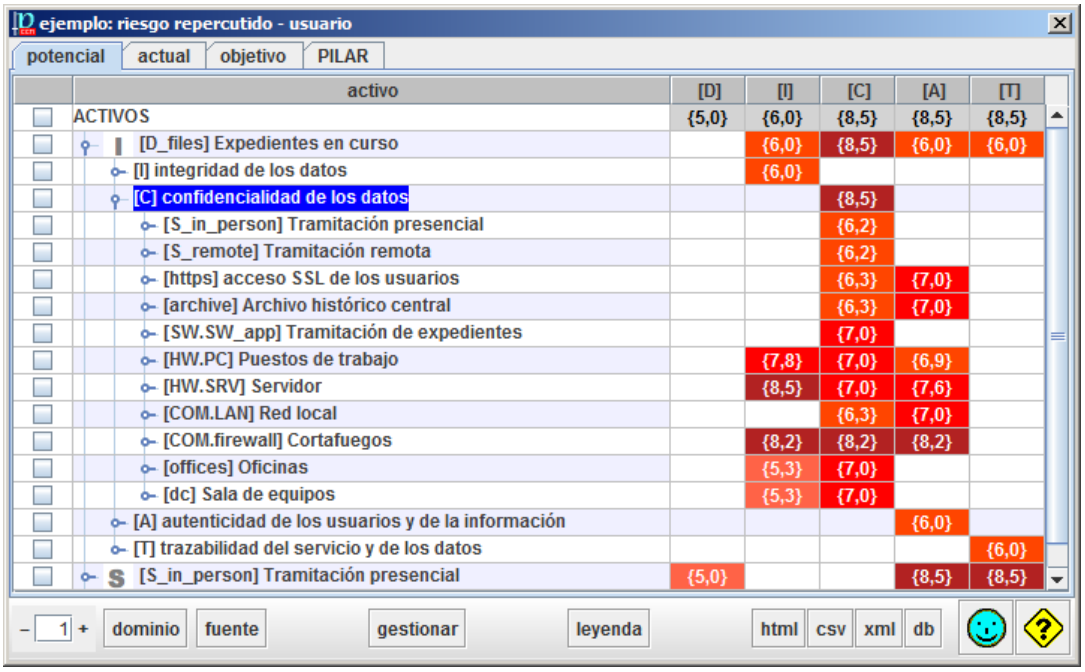
8.14.6 Riesgo repercutido

PILAR presenta el riesgo repercutido sobre los activos con valor propio:

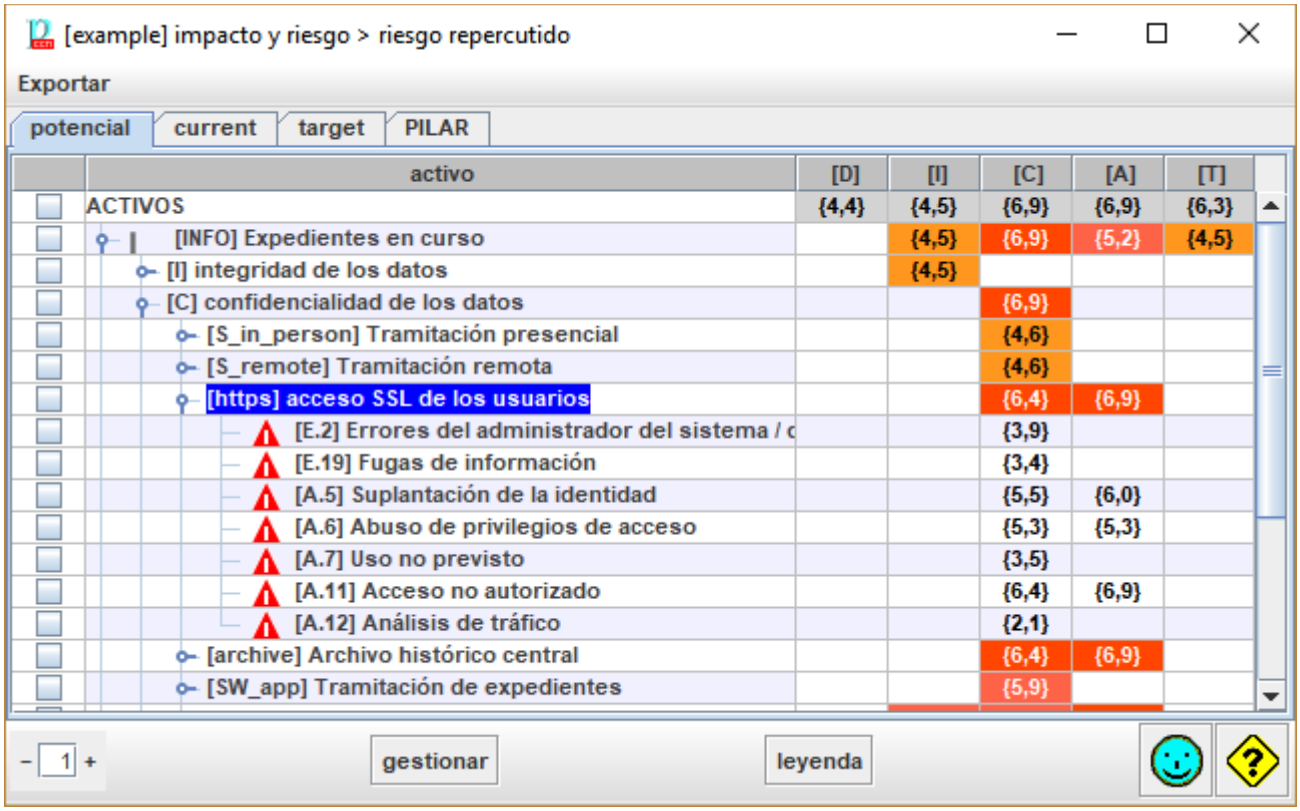
Puede expandir el árbol para segregar cada dimensión:



Puede seguir expandiendo el árbol para ver cómo es afectada cada dimensión en los activos de los que depende:



Y puede llegar a amenazas concretas:



Una pestaña por fase del proyecto. Haga clic para cambiar.
La pseudo-fase POTENCIAL muestra el riesgo potencial (sin salvaguarda alguna).

Menú superior EXPORTAR

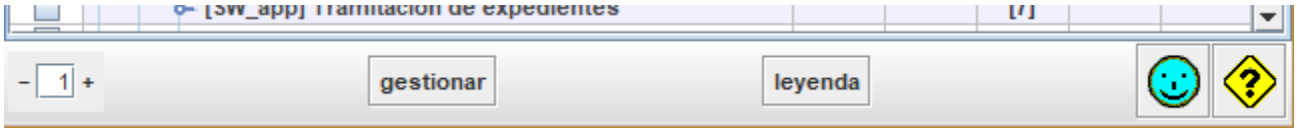
html	exporta las filas seleccionadas a formato HTML, para la web
csv	exporta las filas seleccionadas a formato CSV, para Excel
xml	exporta las filas seleccionadas a formato XML
db	exporta las filas seleccionadas a una base de datos. solamente si está activado del módulo SQL

Columnas de la tabla

1	**selección**	Haga clic en las cajitas para seleccionar / deseleccionar. Haga MAYÚSCULAS + clic para seleccionar un rango. Haga clic en la cabecera de la columna para eliminar la selección actual. La selección determina a qué filas se aplica GESTIONAR.
2	**activos**	Activos y amenazas

3 **…**	**dimensiones**	Una columna por dimensión de seguridad. Haga clic en la cabecera para tener una *vista alternativa*, por dimensión.

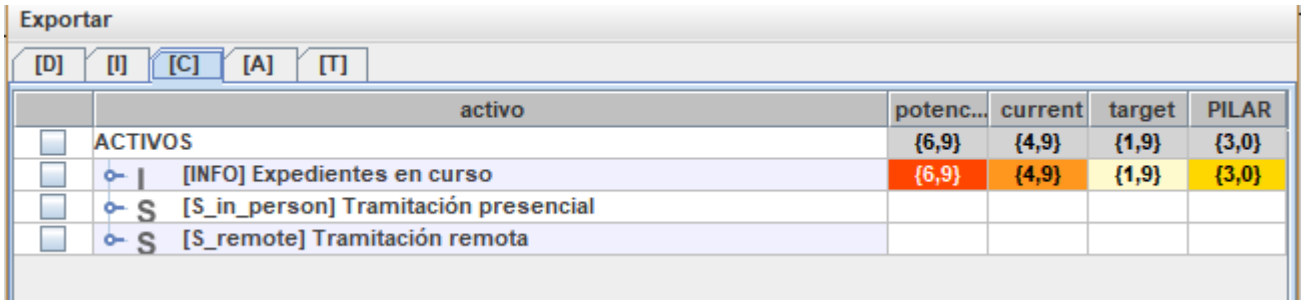
Barra inferior



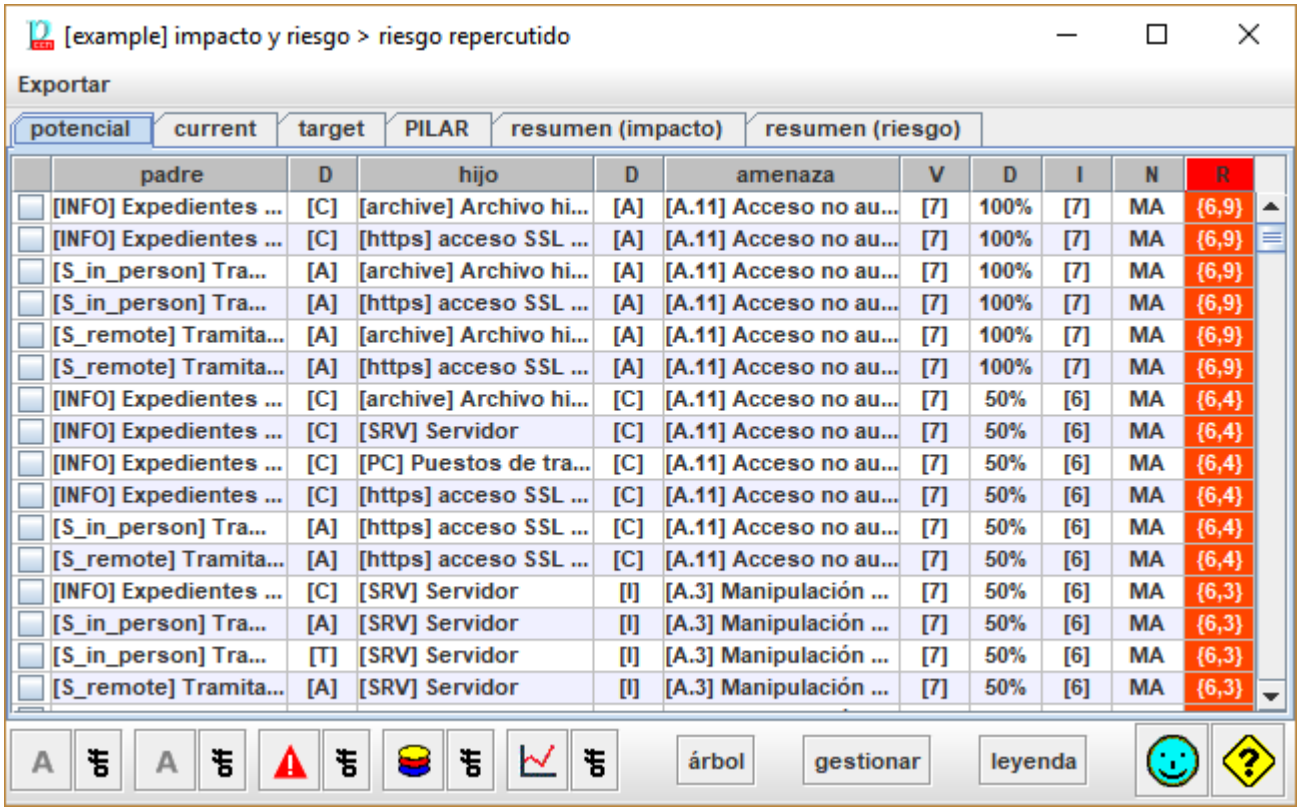
- 1 +	Para controlar el despliegue del árbol
gestionar	Para las filas seleccionadas en la columna 1, PILAR recolecta los riesgos asociados y salta a la ventana de *valoración de salvaguardas*, teniendo en cuenta solo dichos riesgos.
leyenda	Niveles y colores de los valores de riesgo.

8.14.6.1 Vista alternativa

Si hace clic en la cabecera de una columna, PILAR conmuta entre columnas y pestañas:



8.14.7 Tabla de impacto y riesgo repercutido



padre	D	hijo	D	amenaza	V	D	I	N	R
[INFO] Expedientes ...	[C]	[archive] Archivo hi...	[A]	[A.11] Acceso no au...	[7]	100%	[7]	MA	{6,9}
[INFO] Expedientes ...	[C]	[https] acceso SSL ...	[A]	[A.11] Acceso no au...	[7]	100%	[7]	MA	{6,9}
[S_in_person] Tra...	[A]	[archive] Archivo hi...	[A]	[A.11] Acceso no au...	[7]	100%	[7]	MA	{6,9}
[S_in_person] Tra...	[A]	[https] acceso SSL ...	[A]	[A.11] Acceso no au...	[7]	100%	[7]	MA	{6,9}
[S_remote] Tramita...	[A]	[archive] Archivo hi...	[A]	[A.11] Acceso no au...	[7]	100%	[7]	MA	{6,9}
[S_remote] Tramita...	[A]	[https] acceso SSL ...	[A]	[A.11] Acceso no au...	[7]	100%	[7]	MA	{6,9}
[INFO] Expedientes ...	[C]	[archive] Archivo hi...	[C]	[A.11] Acceso no au...	[7]	50%	[6]	MA	{6,4}
[INFO] Expedientes ...	[C]	[SRV] Servidor	[C]	[A.11] Acceso no au...	[7]	50%	[6]	MA	{6,4}
[INFO] Expedientes ...	[C]	[PC] Puestos de tra...	[C]	[A.11] Acceso no au...	[7]	50%	[6]	MA	{6,4}
[INFO] Expedientes ...	[C]	[https] acceso SSL ...	[C]	[A.11] Acceso no au...	[7]	50%	[6]	MA	{6,4}
[S_in_person] Tra...	[A]	[https] acceso SSL ...	[C]	[A.11] Acceso no au...	[7]	50%	[6]	MA	{6,4}
[S_remote] Tramita...	[A]	[https] acceso SSL ...	[C]	[A.11] Acceso no au...	[7]	50%	[6]	MA	{6,4}
[INFO] Expedientes ...	[C]	[SRV] Servidor	[I]	[A.3] Manipulación ...	[7]	50%	[6]	MA	{6,3}
[S_in_person] Tra...	[A]	[SRV] Servidor	[I]	[A.3] Manipulación ...	[7]	50%	[6]	MA	{6,3}
[S_in_person] Tra...	[T]	[SRV] Servidor	[I]	[A.3] Manipulación ...	[7]	50%	[6]	MA	{6,3}
[S_remote] Tramita...	[A]	[SRV] Servidor	[I]	[A.3] Manipulación ...	[7]	50%	[6]	MA	{6,3}

Una pestaña por fase del proyecto. Haga clic para seleccionar.
La pseudo fase POTENCIAL muestra los valores inherentes, sin salvaguarda alguna.
Ver *resumen (impacto)*
Ver *resumen (riesgo)*

Menú superior EXPORTAR

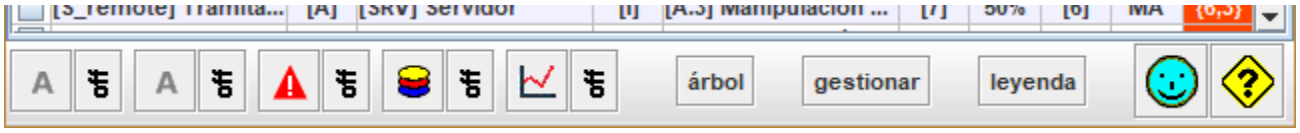
csv	exporta las filas seleccionadas a formato CSV, para Excel
xml	exporta las filas seleccionadas a formato XML
db	exporta las filas seleccionadas a una base de datos. solamente si está activado del módulo SQL

Columnas de la tabla

1	selección	
2	padre	El activo superior sobre el que repercute la amenaza
3	dimensión superior	Dimensión en la que repercute la amenaza
4	hijo	El activo inferior, sobre el que se materializa la amenaza
5	dimensión inferior	La dimensión afectada directamente por la amenaza
6	amenaza	La amenaza

7	valor	El valor del activo superior en la dimensión superior
8	degradación	Degradación causada por la amenaza en la dimensión del activo
9	impacto	Impacto de la amenaza en la dimensión del activo superior
10	probabilidad	Probabilidad de la amenaza sobre el activo. La cabecera se denomina según *Opciones / Probabilidad*
11	risk	Riesgo de la amenaza en la dimensión del activo superior

Barra inferior



	Filtro de activos superiores: solo se presentan los activos seleccionados. Haga clic en la imagen para seleccionar activos. Haga clic en ON / OFF para activar / desactivar el filtro.
	Filtro de activos inferiores: solo se presentan los activos seleccionados. Haga clic en la imagen para seleccionar activos. Haga clic en ON / OFF para activar / desactivar el filtro.
	Filtro de amenazas: solo se presentan las amenazas seleccionadas. Haga clic en la imagen para seleccionar amenazas. Haga clic en ON / OFF para activar / desactivar el filtro.
	Filtro de dimensiones: solo se presentan las dimensiones seleccionadas. Haga clic en la imagen para seleccionar dimensiones. Haga clic en ON / OFF para activar / desactivar el filtro.
	Filtro para ver solo algunos riesgos. Haga clic en la imagen para elegir la fracción que desea ver. Puede elegir un porcentaje para impacto y un porcentaje para riesgos. Los valores típicos son 10% y 10%, seleccionando el 10% de mayor impacto y el 10% de mayor riesgo (es decir, la parte superior derecha de la tabla de impacto-probabilidad)  0% implica no ver ninguno. 100% sería como eliminar el filtro. Haga clic en ON / OFF para activar / desactivar el filtro.
árbol	

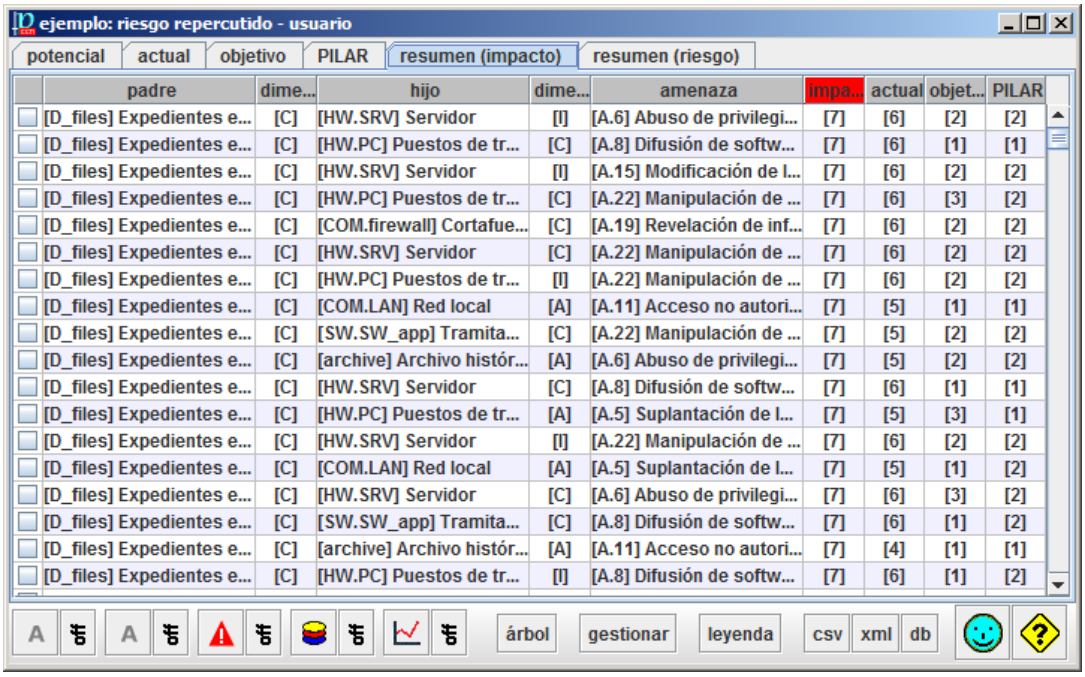
gestionar	Para las filas seleccionadas en la columna 1, PILAR recolecta los riesgos asociados y salta a la ventana de *valoración de salvaguardas*, teniendo en cuenta solo dichos riesgos.
leyenda	Ver *Riesgos / Niveles de criticidad / código de colores*

Las filas se ordenan según criticidad (riesgo), después por impacto y, por último, por probabilidad.

Haga clic en las cabeceras para ordenar por la columna correspondiente.

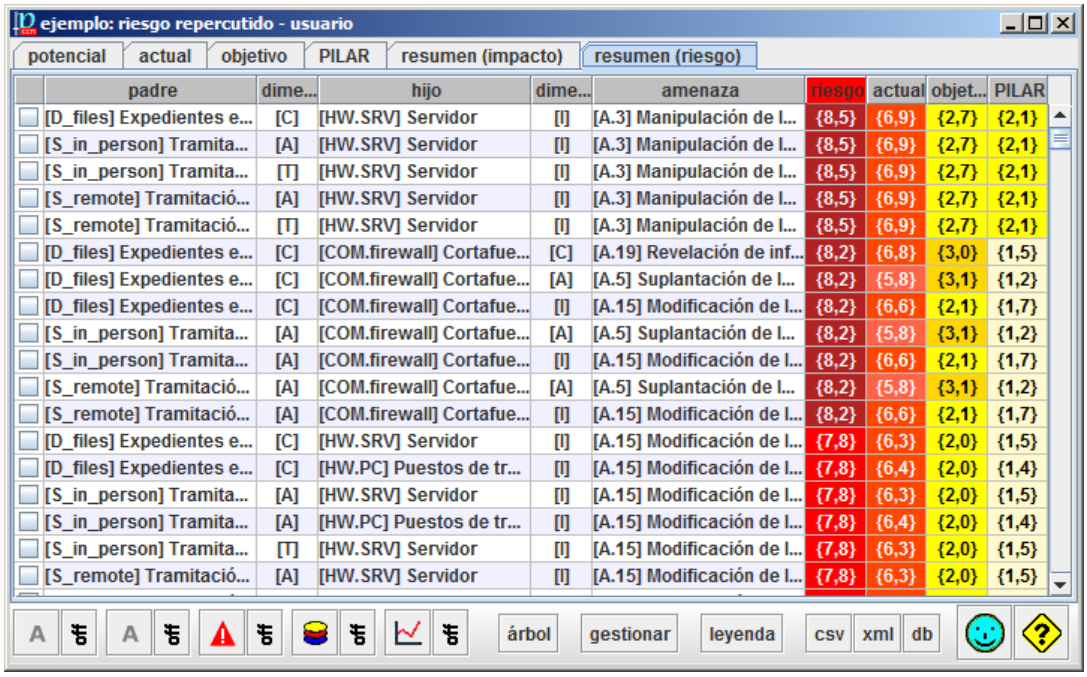
8.14.7.1 Resumen de impacto

PILAR presenta la evolución del impacto a lo largo de las fases de proyecto



8.14.7.2 Resumen de riesgo

PILAR presenta la evolución del riesgo a lo largo de las fases de proyecto



padre	dime...	hijo	dime...	amenaza	riesgo	actual	objet...	PILAR
[D_files] Expedientes e...	[C]	[HW.SRV] Servidor	[I]	[A.3] Manipulación de l...	{8,5}	{6,9}	{2,7}	{2,1}
[S_in_person] Tramita...	[A]	[HW.SRV] Servidor	[I]	[A.3] Manipulación de l...	{8,5}	{6,9}	{2,7}	{2,1}
[S_in_person] Tramita...	[T]	[HW.SRV] Servidor	[I]	[A.3] Manipulación de l...	{8,5}	{6,9}	{2,7}	{2,1}
[S_remote] Tramitació...	[A]	[HW.SRV] Servidor	[I]	[A.3] Manipulación de l...	{8,5}	{6,9}	{2,7}	{2,1}
[S_remote] Tramitació...	[T]	[HW.SRV] Servidor	[I]	[A.3] Manipulación de l...	{8,5}	{6,9}	{2,7}	{2,1}
[D_files] Expedientes e...	[C]	[COM.firewall] Cortafue...	[C]	[A.19] Revelación de inf...	{8,2}	{6,8}	{3,0}	{1,5}
[D_files] Expedientes e...	[C]	[COM.firewall] Cortafue...	[A]	[A.5] Suplantación de l...	{8,2}	{5,8}	{3,1}	{1,2}
[D_files] Expedientes e...	[C]	[COM.firewall] Cortafue...	[I]	[A.15] Modificación de l...	{8,2}	{6,6}	{2,1}	{1,7}
[S_in_person] Tramita...	[A]	[COM.firewall] Cortafue...	[A]	[A.5] Suplantación de l...	{8,2}	{5,8}	{3,1}	{1,2}
[S_in_person] Tramita...	[A]	[COM.firewall] Cortafue...	[I]	[A.15] Modificación de l...	{8,2}	{6,6}	{2,1}	{1,7}
[S_remote] Tramitació...	[A]	[COM.firewall] Cortafue...	[A]	[A.5] Suplantación de l...	{8,2}	{5,8}	{3,1}	{1,2}
[S_remote] Tramitació...	[A]	[COM.firewall] Cortafue...	[I]	[A.15] Modificación de l...	{8,2}	{6,6}	{2,1}	{1,7}
[D_files] Expedientes e...	[C]	[HW.SRV] Servidor	[I]	[A.15] Modificación de l...	{7,8}	{6,3}	{2,0}	{1,5}
[D_files] Expedientes e...	[C]	[HW.PC] Puestos de tr...	[I]	[A.15] Modificación de l...	{7,8}	{6,4}	{2,0}	{1,4}
[S_in_person] Tramita...	[A]	[HW.SRV] Servidor	[I]	[A.15] Modificación de l...	{7,8}	{6,3}	{2,0}	{1,5}
[S_in_person] Tramita...	[A]	[HW.PC] Puestos de tr...	[I]	[A.15] Modificación de l...	{7,8}	{6,4}	{2,0}	{1,4}
[S_in_person] Tramita...	[T]	[HW.SRV] Servidor	[I]	[A.15] Modificación de l...	{7,8}	{6,3}	{2,0}	{1,5}
[S_remote] Tramitació...	[A]	[HW.SRV] Servidor	[I]	[A.15] Modificación de l...	{7,8}	{6,3}	{2,0}	{1,5}

9 Perfiles de seguridad (EVL)

Los perfiles de seguridad son conjuntos de medidas de seguridad para proteger un sistema. Pueden enfocarse en un aspectos específico de la seguridad, o ser de propósito general. Algunos perfiles están muy extendidos y pueden emplearse en procesos de cumplimiento normativo.

PILAR asocia los perfiles de seguridad a sus salvaguardas de forma que

- el usuario puede estimar el grado de cumplimiento
- PILAR puede estimar el riesgo residual tras satisfacer el perfil
- el usuario puede trabajar coordinadamente con varios perfiles

Usaremos ISO/IEC 27002 (2013) como ejemplo.

Para cargarlo en PILAR, necesita el fichero EVL

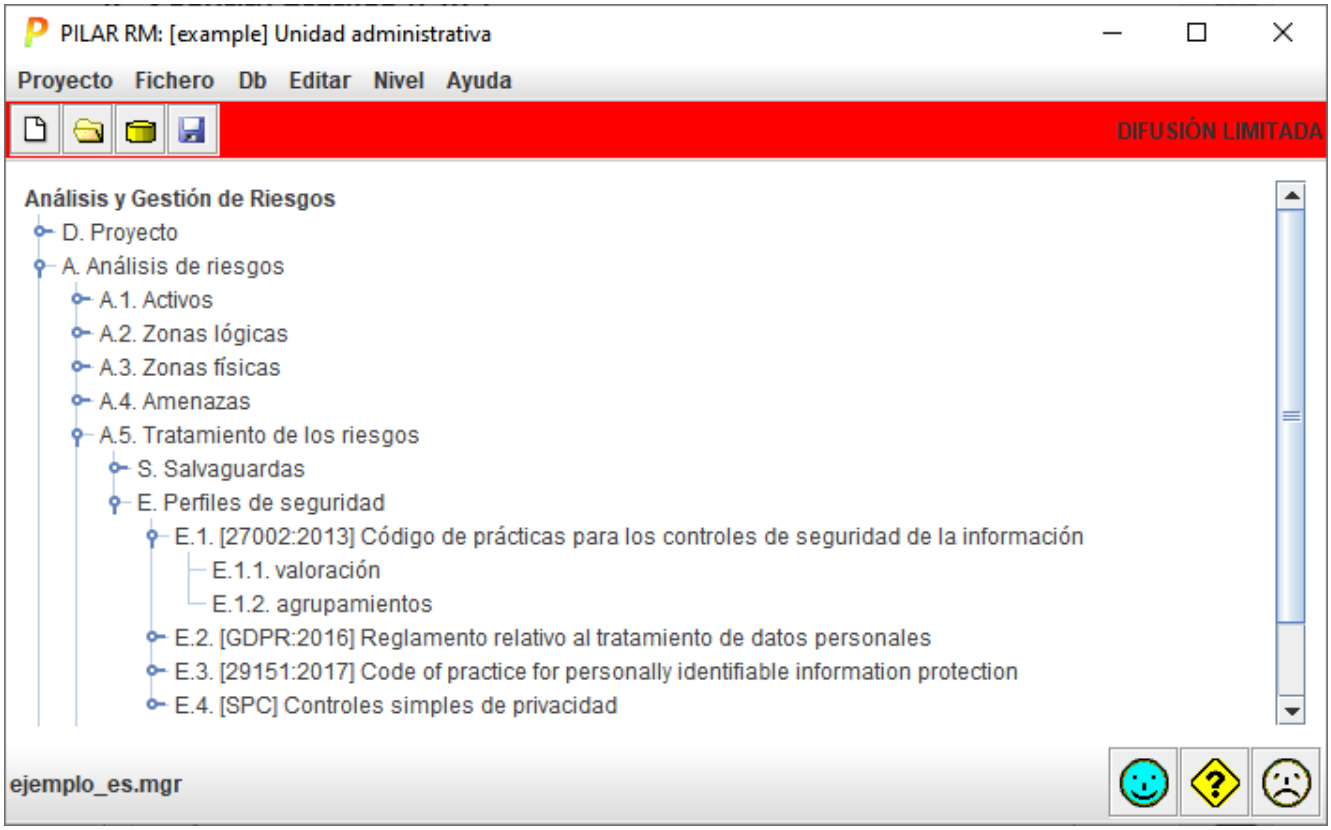
```
bib_en/27002_2013_2014-12-29_es.evl
```

e indicarle a PILAR que lo cargue al arrancar (aunque también puede cargarlo luego manualmente). En el fichero CAR de configuración

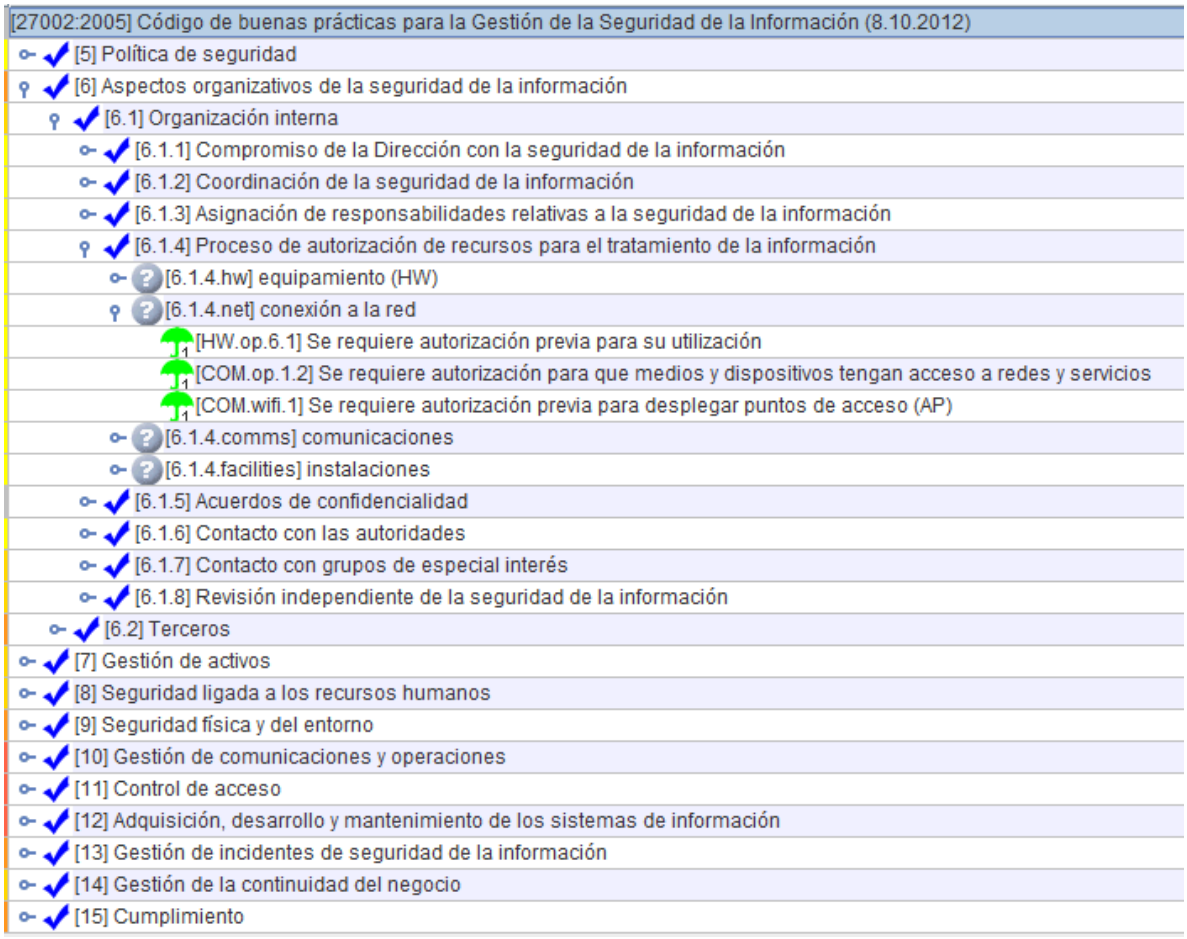
STIC_es.car

```
profile= 27002_2013_2014-12-29_es.evl
```

En la interfaz de usuario:



Y entrando en el perfil, nos encontramos con los controles de la norma asociados a las salvaguardas de PILAR:

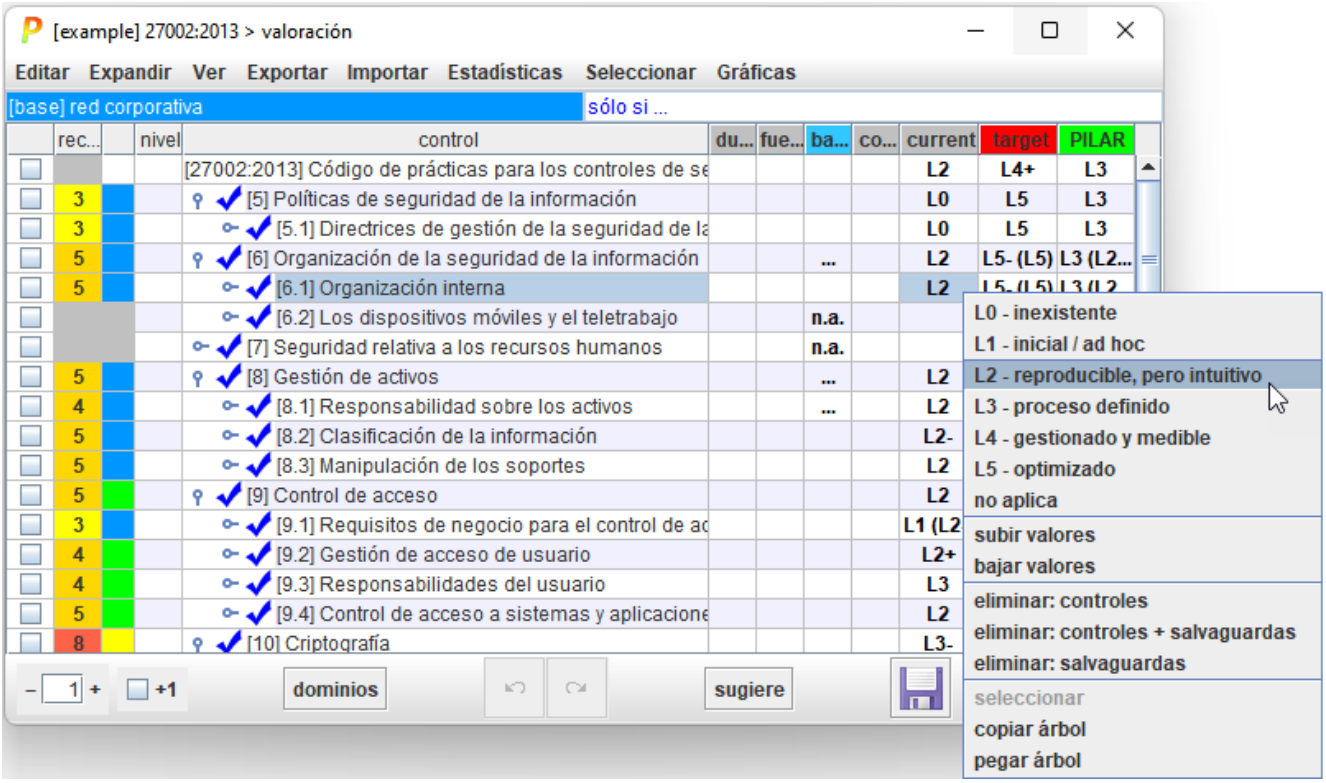


Los perfiles se estructuran como árboles con diferentes tipos de nodos:

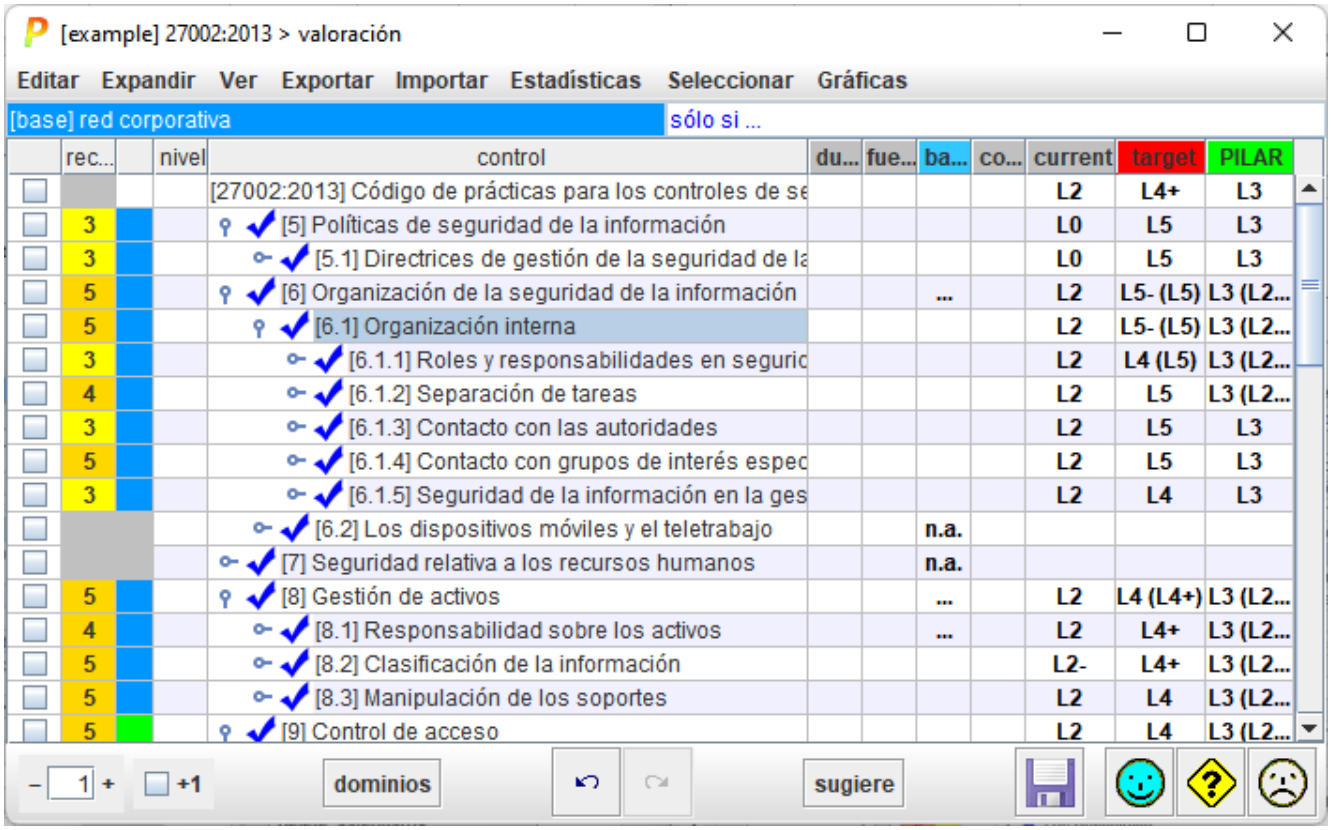
	Controles – requisitos principales
	Preguntas – requisitos auxiliares y nodos para estructurar el árbol
	Enlaces – cuando un control se refiere a otro
	Salvaguardas – medidas de protección de PILAR
	Ver también – información adicional

9.1 EVL - Uso básico

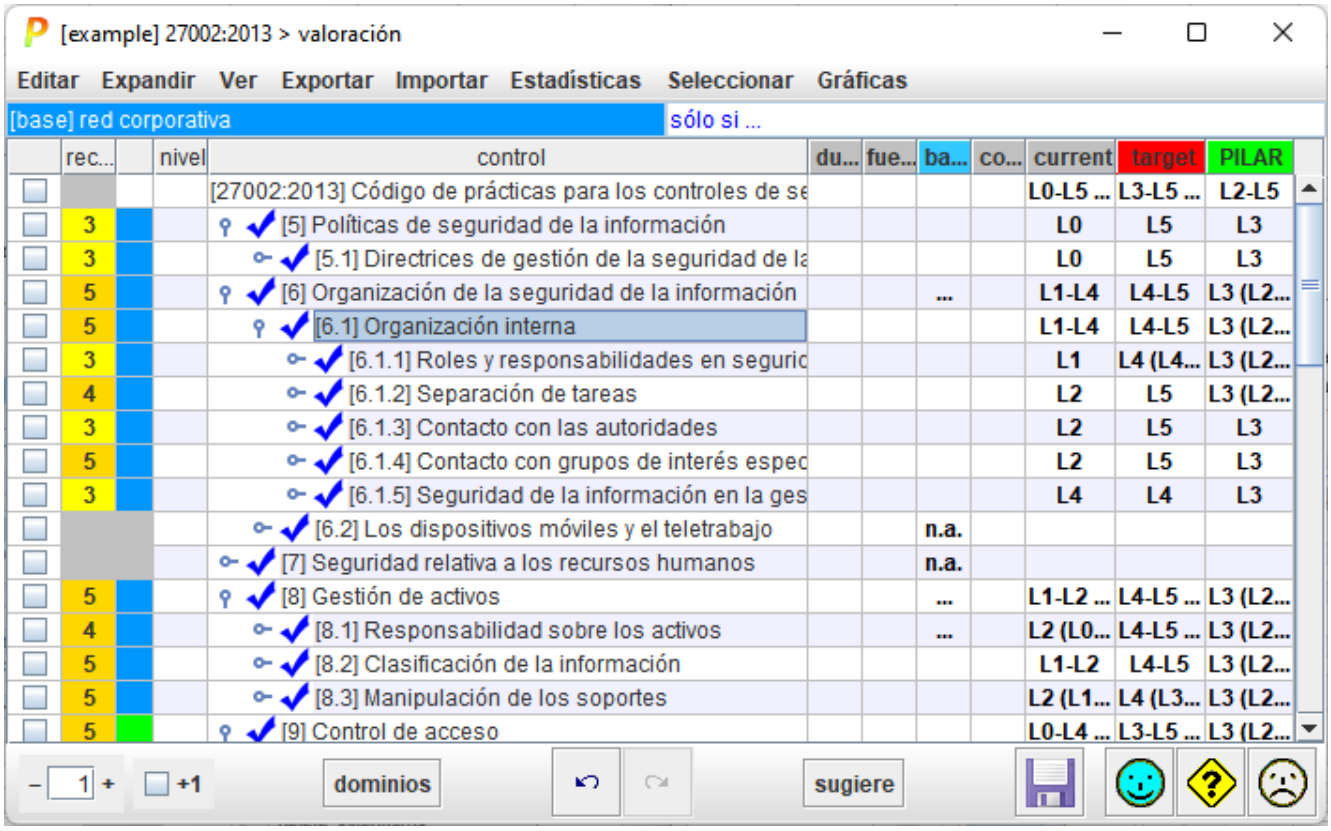
Lo más básico que se hace con un perfil es evaluar los controles en términos de madurez. Seleccione un control y una fase y haga clic con el botón derecho:



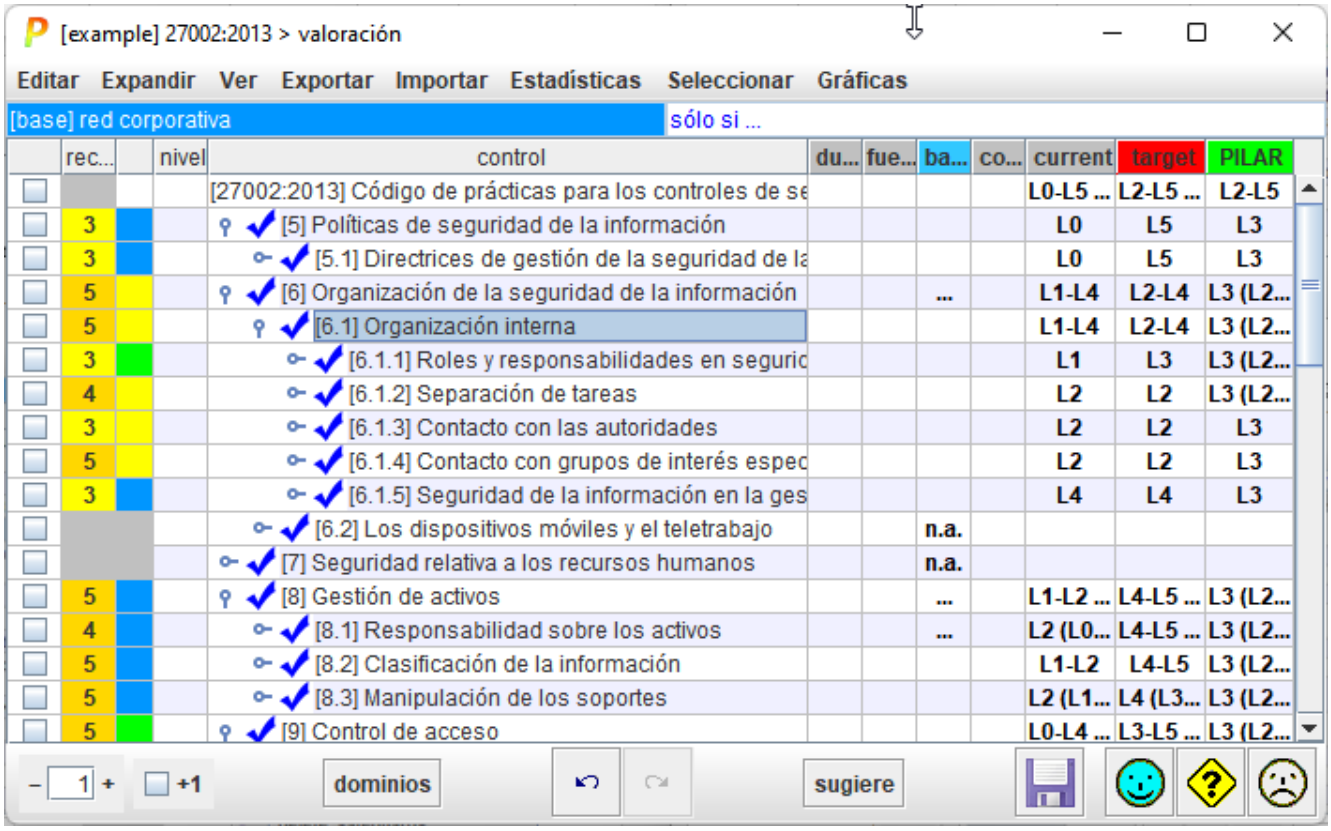
PILAR aplica la madurez seleccionada al control seleccionado. Y se propaga a sus hijos:



De esta manera, el usuario puede marcar un valor en general de la madurez, y luego ir refinando en controles internos. Cuando los hijos tienen una variedad de valores, el padre muestra el rango



El valor marcado en una fase se propaga a las fases siguientes, salvo que se indique otro:

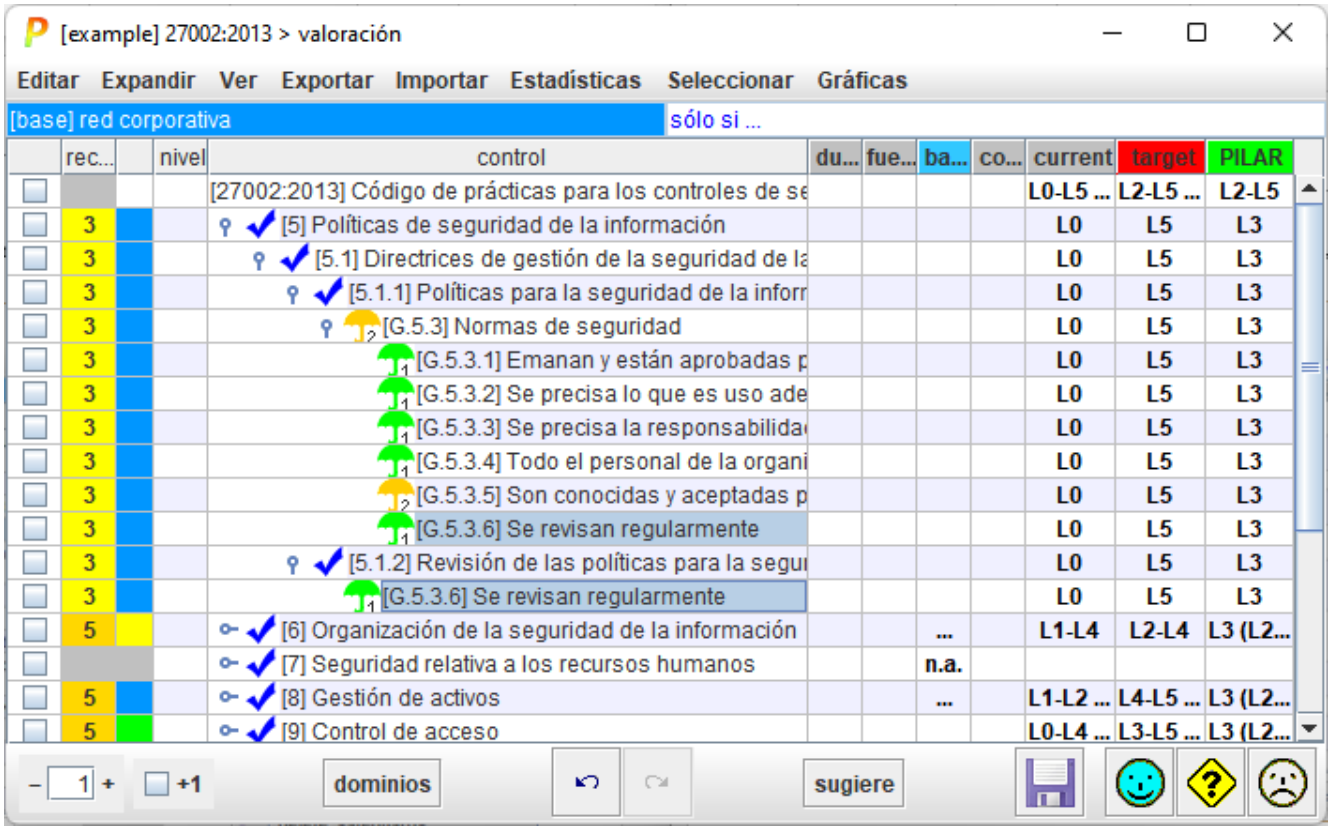


PILAR asocia controles y salvaguardas. Esta asociación no es oficial, ni perfecta. No es oficial porque los perfiles de seguridad son creados por organizaciones independientes. Y no es perfecta porque:

- puede que en PILAR no tengamos una salvaguarda que case 100% con los requisitos del control
- la misma salvaguarda en PILAR puede contribuir a más de un control
- cuando PILAR evoluciona, las salvaguardas evolucionan; pero no de forma sincronizada con la evolución de los perfiles

De forma que PILAR proporciona una asociación razonable.

Cuando una salvaguarda aparece bajo varios controles, modificarla en uno tiene efectos colaterales en los otros:



PILAR puede destacar directamente todas esas salvaguardas que tienen un doble papel

EXPANDIR > Papel doble

9.2 EVL - Opciones de presentación de la madurez

En la barra superior, VER

madurez

Presenta el valor de la madurez de elementos sencillos y el rango de valores de los componentes en elementos compuestos.

~madurez

Presenta una aproximación a la madurez media de los componentes. Por ejemplo, L3- si los componentes están mayoritariamente a nivel L3, pero alguno está un poco más bajo.

porcentaje

Promedia la madurez de las salvaguardas traducidas a un porcentaje. Ver *Opciones / Madurez*

fase (para las diferentes fases cableadas)

Compara la madurez en la columna del usuario frente a la madurez en la columna de referencia. Sirve para ver en qué medida hemos alcanzado la propuesta.

9.3 EVL - Opciones sobre los controles

Si hace clic con el botón derecho en algún control, se le presentan varias opciones …

editar

presenta una vista por dominios y fases; ver más abajo

copiar

copia en el portapapeles el nombre del control

copiar ruta

copia en el portapapeles el camino completo del control

texto completo

código y nombre del control

camino completo

muestra el control en su contexto; es decir, la serie de pasos desde la raíz hasta el

descripción

una descripción más extensa del control; depende de si el perfil incluye o no estas descripciones

cerrar el padre

compacta el árbol, cerrando el padre del nodo seleccionado

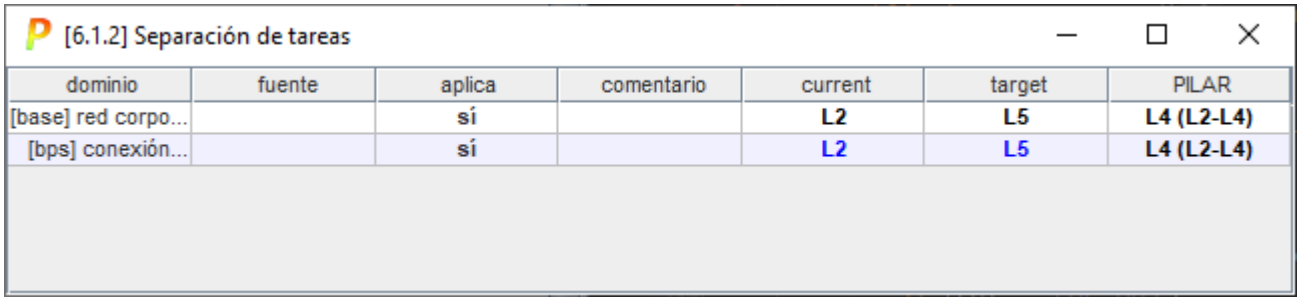
cerrar los hermanos

compacta el árbol, cerrando todos los hermanos del nodo seleccionado

ir a

para enlaces,  , va al control referenciado

Vista por dominios y fases. Haciendo clic en un control puede acceder a una vista de los valores de madurez que cubra simultáneamente todos los dominios y todas las fases:



dominio	fuente	aplica	comentario	current	target	PILAR
[base] red corpo...		sí		L2	L5	L4 (L2-L4)
[bps] conexión...		sí		L2	L5	L4 (L2-L4)

Los datos del usuario aparecen en negro sobre blanco, mientras que los derivados por PILAR aparecen en cian.

9.4 EVL – Hooks

Se pueden asociar enlaces a controles por medio de ficheros hook-. Estos son ficheros en el directorio de librería, con un nombre que empieza por “hooks-…”. El formato es JSON.

Se presenta un ejemplo:

bib_es/hooks-ccn.json

```
{
  "encoding": "áéíóú",
  "title" : "CCN-CERT",
  "defs" : [
    { "controls" : [ [ "ens:2015", "org.1" ],
                     [ "27002:2013", "5.1.1", "6.1.1" ] ],
      "classes" : [ ],
      "links" : [
        { "label" : "CCN-STIC-805 - Política de Seguridad de la Información",
          "url" : "https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-
esquema-nacional-de-seguridad.html"
        },
        { "label" : "CCN-STIC-801 - Responsabilidades y Funciones en el ENS",
          "url" : "https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-
esquema-nacional-de-seguridad.html"
        }
      ]
    },
    { "controls" : [ [ "ens:2015", "org.2" ],
                     [ "27002:2013", "5.1.1" ] ],
      "classes" : [ ],
      "links" : [
        { "label" : "CCN-STIC-821 - Normas de Seguridad en el ENS",
          "url" : "https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-
esquema-nacional-de-seguridad.html"
        }
      ]
    },
```

9.5 EVL – Aplicabilidad

Para cada control ( ), cada pregunta ( ), y cada una de las salvaguardas ( ), se puede indicar si aplica o no haciendo clic en la columna APLICA.

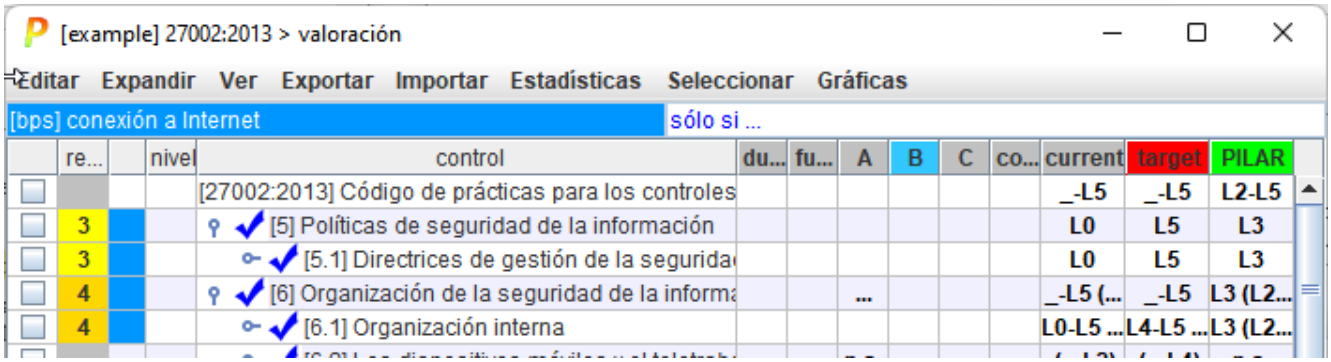
control	dud...	fuen...	aplica	com...
[27002:2013] Código de prácticas para los controles de seguridad de la información				
[5] Políticas de seguridad de la información				
[6] Organización de la seguridad de la información			...	
[6.1] Organización interna				
[6.2] Los dispositivos móviles y el teletrabajo			...	
[6.2.1] Política de dispositivos móviles				
[6.2.2] Teletrabajo			n.a.	
[7] Seguridad relativa a los recursos humanos			n.a.	
[8] Gestión de activos			...	

"n.a." índice que la fila no aplica. Los puntitos significan que algunos de los subelementos aplican y otros, no.

Cuando se marca como n.a. una medida, todas las medidas por debajo se marcan como n.a.

Etapas de aplicabilidad

Cuando hay varias etapas de aplicabilidad, las opciones anteriores aplican independientemente a cada etapa. Aparece una columna por cada etapa, estando resaltada en azul la etapa actual



Puede hacer clic en la cabecera de la columna para seleccionar la etapa actual.

Salvaguardas

La aplicabilidad de las salvaguardas se recomienda que se especifique en las pantallas de gestión de salvaguardas. La relación entre la aplicabilidad de los controles y la de las salvaguardas asociadas no se automatiza en PILAR; de forma que se pueden marcar controles y salvaguardas independientemente.

9.6 EVL – Controles obligatorios

Algunos perfiles de seguridad imponen la obligación de cumplir ciertos controles. Es una cuestión de cumplimiento. A veces es incondicional; otras veces puede que dependa de ciertas circunstancias (como puede ser el nivel de clasificación de la información que se maneja, por ejemplo). Cuando se conocen estos requisitos, PILAR colorea la celda de aplicabilidad (incluso si la celda no es aplicable por alguna circunstancia).

Por ejemplo:

[M] Medidas de seguridad de nivel medio			...		12%	41%	95%
[95] Responsable de seguridad			M		10%	10%	95%
[96] Auditoría			M		0%	21%	94%
[97] Gestión de soportes y documentos			M		5%	47%	95%
[98] Identificación y autenticación			M		10%	90%	95%
[99] Control de acceso físico			n.a.				
[100] Registro de incidencias			M		35%	35%	95%
[A] Medidas de seguridad de nivel alto					49%	66%	96%
[101] Gestión y distribución de soportes					7%	68%	96%
[102] Copias de respaldo y recuperación					67%	67%	96%
[103] Registro de accesos					20%	37%	95%
[104] Telecomunicaciones					100%	92%	98%

Si marca un control obligatorio como “n.a.”, PILAR retiene el coloreado de la celda para recordarle que deberá justificar su decisión.

9.7 EVL – Valoración

Para los controles y salvaguardas que aplican, puede especificar una valoración para cada fase del proyecto.

Para elementos que no tienen desarrollo, se presenta un valor simple; por ejemplo, L3.

Para elementos que tienen desarrollo (expandibles), se presenta el rango de valores de los subelementos

[AC.1.1] Se dispone de normativa para el control de accesos					_-L3	L0-L3	L2
[AC.1.1.1] Se basa en los requisitos de seguridad y del negocio						L0	L2
[AC.1.1.2] Se definen los tipos de acceso					L2	L3	L2
[AC.1.1.3] Se definen los motivos para modificar los derechos de acceso					L2	L3	L2
[AC.1.1.4] Se revisa regularmente					L3	L3	L2

Cuando el elemento es un control o medida de seguridad, PILAR distingue entre una valoración técnica y una valoración oficial. La valoración técnica la calcula PILAR a partir de las salvaguardas asociadas, y se presenta entre paréntesis. La valoración oficial la introduce el usuario y se presenta fuera de los paréntesis. Cada una de estas valoraciones puede ser un valor sencillo o un rango. Cuando la valoración oficial y la técnica son iguales, solo se presenta la oficial. Por ejemplo

L3(L3) se simplifica a L3

Ejemplo:

[9.1.1] Política de control de acceso					L1 (_-L3)	L4 (L0-L5)	L3 (L2-L3)
[AC.1.1] Se dispone de normativa para el control de accesos					_-L3	L0-L3	L2
[H.ST.3] Se definen roles con autorización exclusiva para realizar tareas			...		L2	L5	L2-L3
[9.1.2] Acceso a las redes y a los servicios de red					L1	L5 (L4)	L2

PILAR ofrece algunos atajos para evaluar rápidamente un conjunto de medidas y salvaguardas:

- cuando se valora una salvaguarda con subelementos, el valor se propaga a los subelementos
- cuando se valora una medida con subelementos, el valor se propaga a los subelementos, de forma controlada
    - si el subelemento es otra medida, se propaga
    - si el subelemento es una referencia a una salvaguarda, depende de la opción de configuración *Tratamiento del riesgo*
- los valores de las medidas se pueden "bajar" manualmente a los subelementos
- los valores de las salvaguardas se pueden "subir" manualmente a las medidas.

Lo más sencillo es dejar que la propia PILAR traslade los valores de madurez de los controles a las salvaguardas y viceversa. Este automatismo se puede seleccionar en *Tratamiento del riesgo*

En elementos de tipo XOR, debemos indicar cual es la opción seleccionada dentro de las posibles.

En salvaguardas que realmente son un enlace a otra salvaguarda, no podremos establecer una valoración: hay que ir al sitio enlazado.

En las celdas de valoración, también puede trasladar valores de madurez de una fase, dominio de seguridad e incluso de un proyecto a otro:

copia el árbol

PILAR copia en el portapapeles el valor de la celda en la fila seleccionada, y los valores de las celdas es que se descompone el control (el sub-árbol).

pega el árbol

Pega los valores previamente copiados.

Nótese que los valores pueden ir de una fase a otra fase, de un dominio a otro, e incluso de un proyecto a otro proyecto; pero siempre se aplican al mismo sub-árbol.

También debe tener en cuenta que PILAR copia y pega dentro de sí misma. No es posible copiar valores en un proceso y volcarlos en otro.

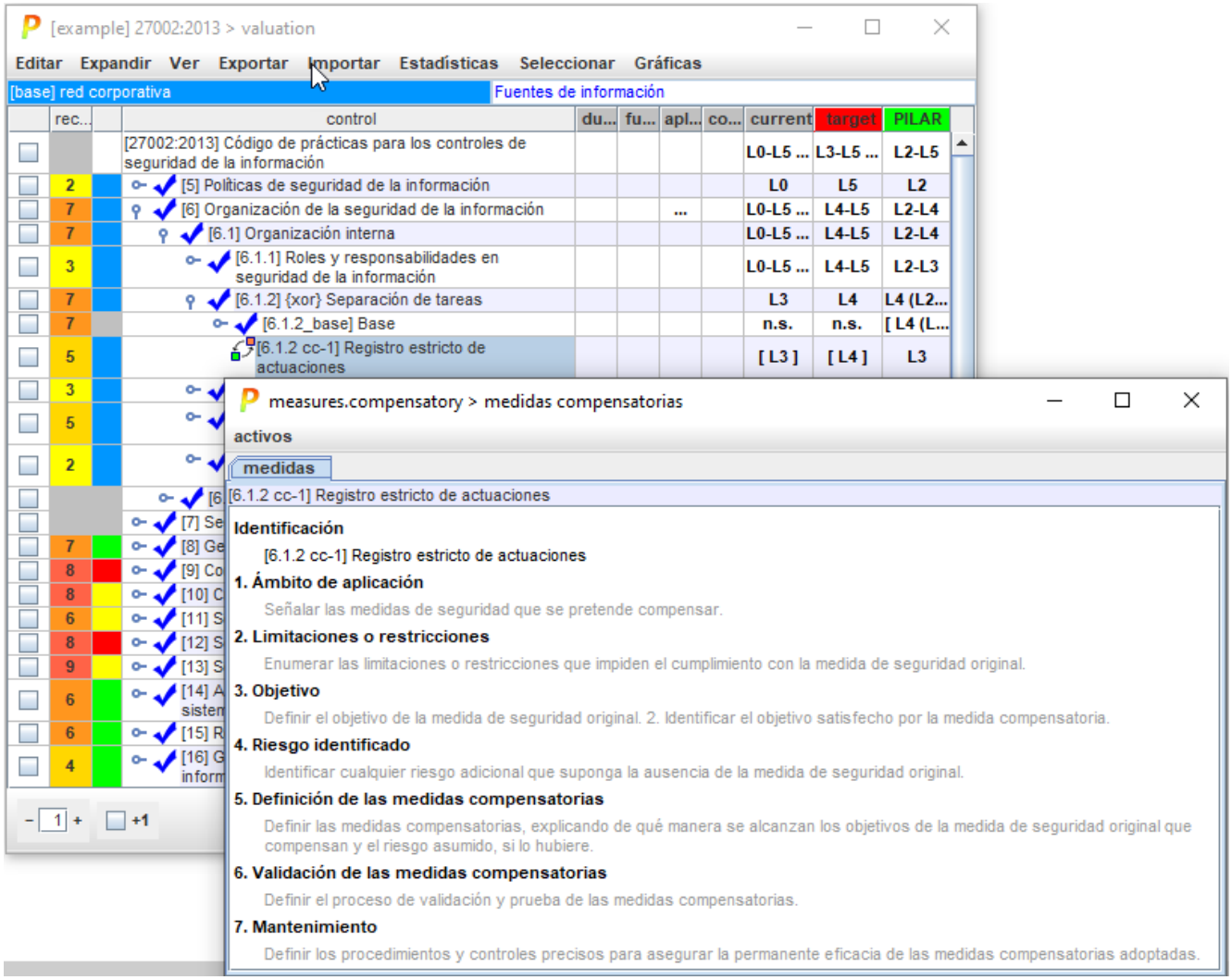
9.8 EVL – Controles compensatorios

El propósito de un control puede alcanzarse por medios diferentes de los previstos en PILAR. En la norma PCI-DSS, tenemos el concepto de "controles compensatorios", que se describen como

> *"los controles de compensación se consideran cuando una entidad no puede cumplir un requisito de manera explícita según lo establecido, debido a limitaciones técnicas legítimas o comerciales documentadas, pero ha mitigado de manera suficiente el riesgo asociado con el requisito a través de la implementación de controles."*

El concepto consiste en alcanzar el objetivo por otros medios.

En PILAR, el usuario puede desconectar un control de sus hijos. Haga clic con el botón derecho en el control para el que ha aplicado un control compensatorio y descríbalo

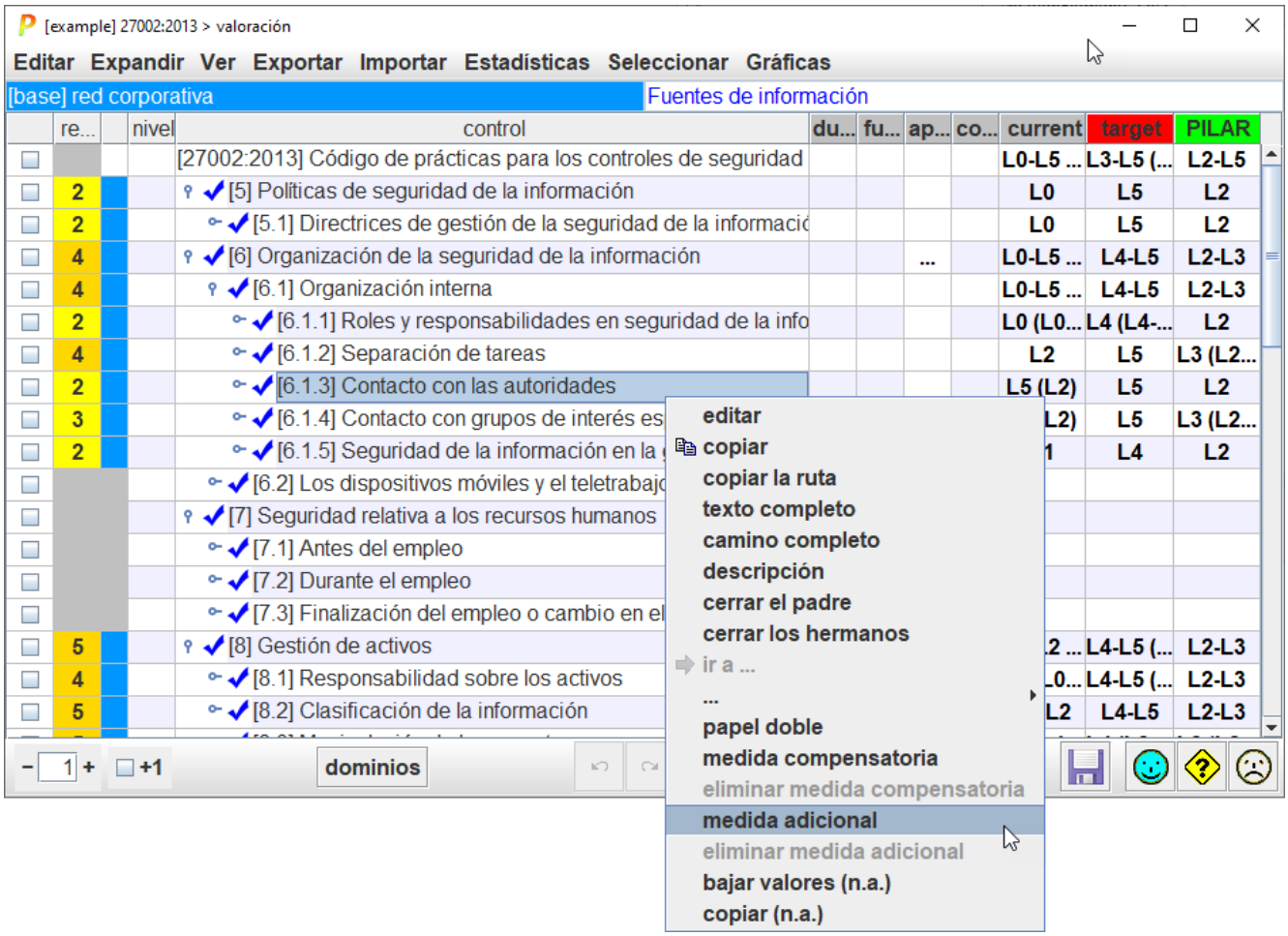


El control seleccionado queda marcado como “compensado”, y puede ser seleccionado y evaluado independientemente de sus hijos.

No olvide que el análisis de riesgos lo sigue realizando PILAR en base a las salvaguardas aplicables, a fin de determinar el riesgo residual estimado.

9.9 EVL – Medidas adicionales

Puede extender la colección de controles con otros adicionales. Estos nuevos controles pueden considerar salvaguardas adicionales que se aplicarán para el tratamiento del riesgo. Los nuevos controles pueden afinarse para que se apliquen exclusivamente a algunas clases de activos y amenazas.



Para el nuevo control, puede especificar varios parámetros

código (obligatorio)

un código único que identifique el nuevo control

nombre

un descripción sucinta en 1 línea

clases de activos (opcional)

cero o más clases de activos; el nuevo control solamente se aplicará a riesgos que involucren activos de alguna de las clases enumeradas

amenazas (opcional)

cero o más clases de actamenazasivos; el nuevo control solamente se aplicará a riesgos que involucren activos de alguna de las amenazas enumeradas

salvaguardas (opcional)

cero o más salvaguardas del catálogo (de PILAR o del NIST); el nuevo control puede subir, bajar, o simplemente compararse con la valoración de estas salvaguardas

descripción

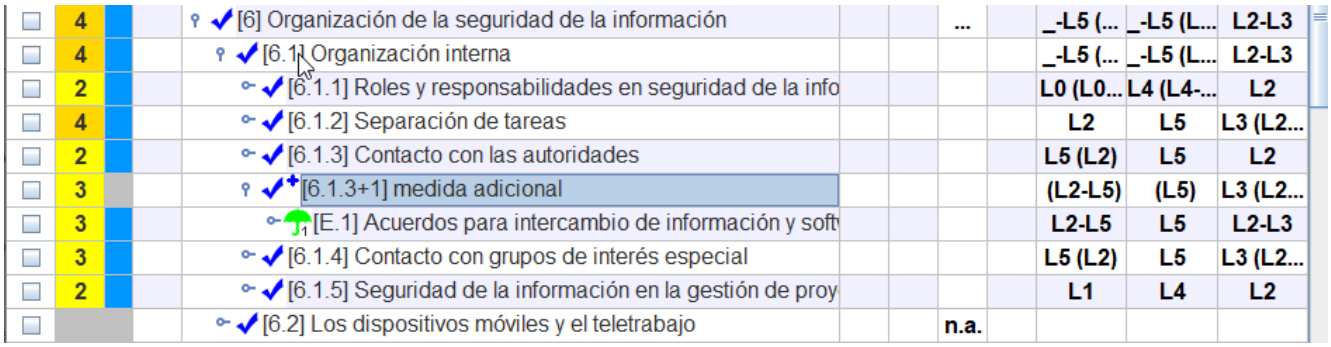
una explicación más extensa del control

safeguards (optional)

zero or more safeguards from the catalogue (either PILAR or NIST); the new control may pull-up, push-down, or just compare its valuation with that of the enumerated safeguards

description

a longer description of the control



9.10 EVL – Fase de referencia y fase objetivo

El semáforo resume en un color si la madurez del control 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)
ROJO	la madurez actual (ROJA) está muy por debajo del objetivo (VERDE)
GRIS	la salvaguarda no es aplicable

9.11 EVL - Valoración por fases

Menú superior EDITAR

buscar	busca un cierto texto en el árbol
pregunta	salta a la siguiente pregunta en el árbol

opciones	Ver *Editar / Opciones*

Menú superior EXPANDIR

controles	Expande el árbol hasta mostrar todos los controles
preguntas	Expande el árbol hasta mostrar todas las preguntas
salvaguardas	Expande el árbol hasta mostrar las salvaguardas
doble papel	Selecciona las salvaguardas que aparecen en dos o más controles
n.a.	Expande el árbol para mostrar los puntos no aplicables
{xor}	Expande el árbol para mostrar los puntos donde hay opciones alternativas; para seleccionar
perímetro	Ver *Perímetros*

Menú superior VER

madurez	madurez de las salvaguardas y de los controles
~madurez	madurez (redondeada) de las salvaguardas y de los controles
porcentaje	— porcentaje de cobertura del control (para controles) — madurez de las salvaguardas de PILAR
PILAR	porcentaje de cumplimiento de los requisitos al nivel recomendado en la fase PILAR; es decir, 100% significa que todos los requisitos se cumplen con una valoración igual o superior a la sugerida por PILAR
una línea	para entradas en el árbol que requieren más de 1 línea, muestra solo la primera
un párrafo	para entradas en el árbol que requieren más de 1 línea, muestra un párrafo

Menú superior EXPORTAR

CSV	Se copian a un fichero CSV las filas visibles
XML	Se copian los valores a un fichero XML
db	Se copian los valores a una base de datos (si está habilitado el módulo SQL)
SoA	Declaración de Aplicabilidad – informe con las medidas que aplican (o no)
informe	Se genera un informe (RTF o HTML)
< Lx	Se genera un informe con las salvaguardas que aplican pero están por debajo de un cierto umbral de madurez
< objetivo	Se genera un informe con las salvaguardas que están por debajo de la fase OBJETIVO. Ver *Salvaguardas / Fases de referencia y objetivo*

Menú superior IMPORTAR

de CSV	lee los valores de madurez de un fichero CSV
de XML	lee los valores de madurez de un fichero XML
importar (mgr)	
importar (db)	

Menú superior SELECCIONAR

borrar	Borra la selección actual
nivel 1	Selecciona los controles en nivel 1 del árbol.
nivel 2	Selecciona los controles en nivel 2 del árbol.
nivel 3	Selecciona los controles en nivel 3 del árbol.
situación actual	Selecciona controles y preguntas visibles en este momento
obligatorio	Selecciona los controles obligatorios
fases	Permite seleccionar las fases del proyecto que queremos que aparezcan en graficas e informes

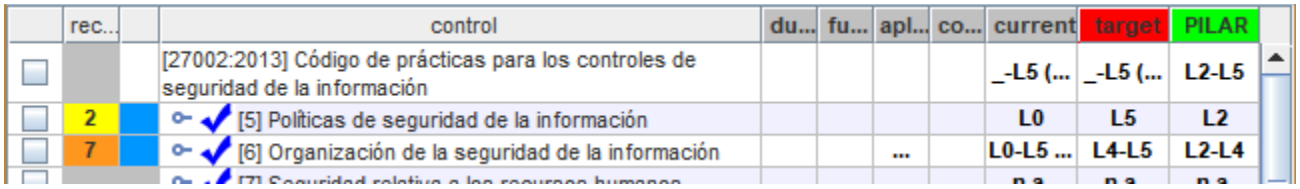
Menú superior GRÁFICA

dibuja	Dibujo con la selección de controles y fases

Bandas superiores

dominio de seguridad	Pueden haber diferentes valores en diferentes dominios. Haga clic para seleccionar el dominio en el que vamos a trabajar.
solo si …	Haga clic para seleccionar un subconjunto de controles basado en algunos atributos de los mismos. PILAR recortará el árbol para mostrar solo los que cumplan los criterios Se pueden usar diferentes criterios • controles que aplican; o que no • fuentes de información • nivel de aplicabilidad

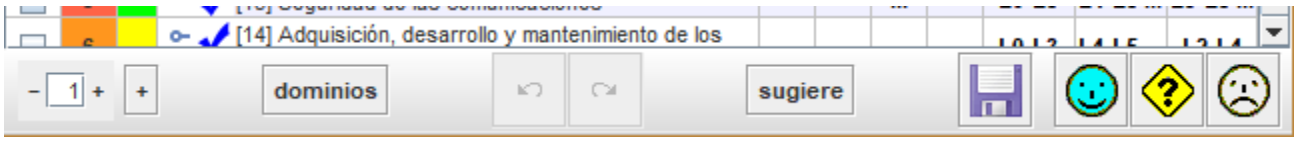
Columnas en la tabla



1	**selección**	Selecciona líneas para aparecer en las gráficas
2	**recomendación**	Es una valoración en el rango [nada .. 10] estimada por PILAR teniendo en cuenta el tipo de activos y su valoración en cada dimensión. La celda queda gris si PILAR no ve ningún motivo para poner esta protección. (o) – significa que PILAR opina que es excesiva ("overkill") (u) – significa que PILAR opina que es insuficiente ("underkill"). Haga clic con el botón derecho y aparecerá una nueva ventana con un resumen de las razones que han llevado a PILAR a su recomendación; es decir, los activos y dimensiones que protege.
3	**semáforo**	Compara la valoración en la fase de referencia (ROJA) con la valoración en la fase objetivo (VERDE): ROJO el valor en la fase de referencia está muy lejos del valor objetivo AMARILLO el valor en la fase de referencia es inferior, pero cercano, al valor objetivo VERDE el valor en la fase de referencia es igual al objetivo AZUL el valor en la fase de referencia es mayor que el objetivo Vea "*EVL / Fases de referencia y objetivo*
4	**árbol de controles**	. Presenta de forma jerárquica los controles y preguntas en el perfil, y su conexión a salvaguardas de PILAR. Haga clic-clic para colapsar / expandir el árbol. Clic con el botón derecho para acceder al menú del árbol.
5	**dudas**	Haga clic para marcar / desmarcar la caja. La marca se usa, típicamente, para recordar que hay asuntos pendientes de una respuesta. La marca "mancha" todo el árbol, desde donde se pone hasta la raíz, para que sea evidente que hay algo pendiente.
6	**fuentes**	Haga clic para asociar fuentes de información a la salvaguarda (la marcada y sus descendientes).
7	**aplica**	Haga clic para conmutar. Ver *EVL / Aplicabilidad*

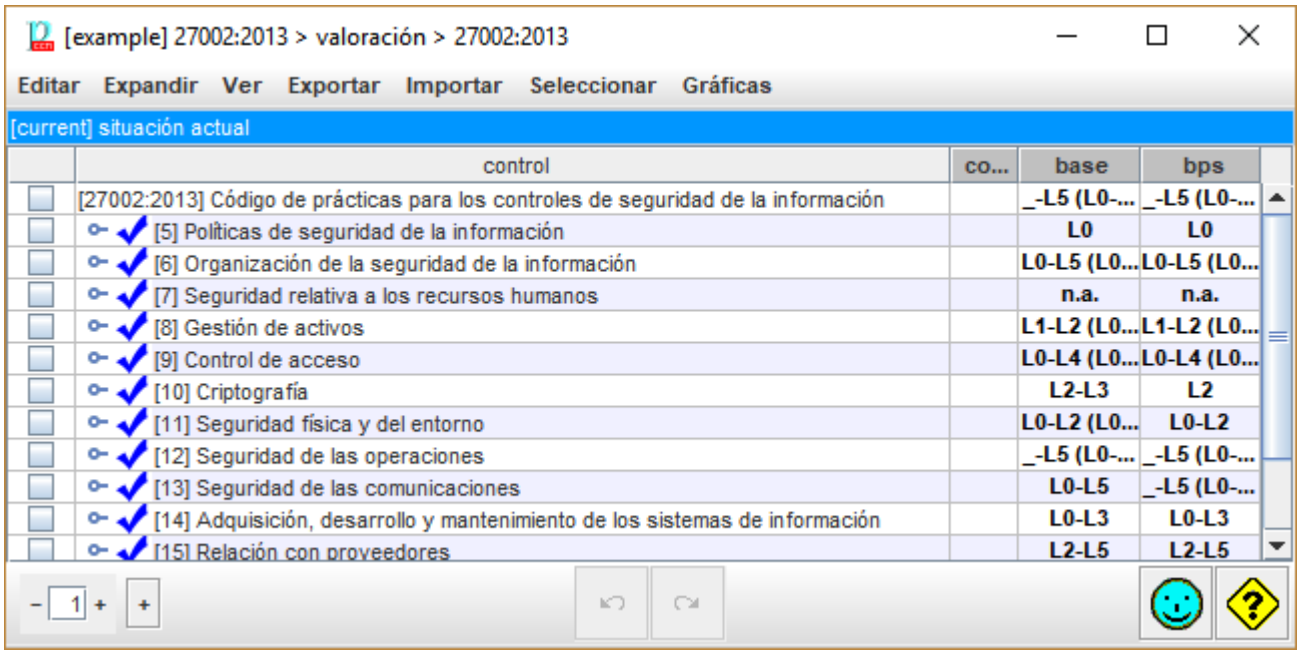
8	**comentario**	Haga clic para asociar un comentario a la salvaguarda.
9 …		Fases del proyecto. Haga clic con el botón izquierdo para marcar la fase roja (referencia). Haga clic con el botón derecho para marcar la fase verde (objetivo). • Vea "*EVL / Fases de referencia y objetivo* • Ver "*EVL / Valoración*

Barra inferior



	Controla el despliegue del árbol .
	Modifica el comportamiento del *spinner*. Si se selecciona, el árbol se despliega incluyendo las salvaguardas asociadas a cada control.
dominios	Ver *EVL / dominio*
	Revierte los últimos cambios
	Rehace los últimos cambios revertidos
sugiere	
	Guarda el proyecto en su fichero o en su base de datos.

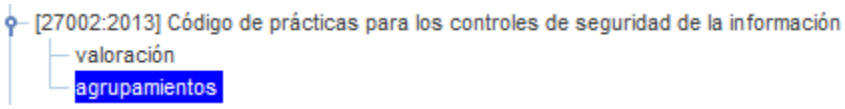
9.12 EVL - Valoración por dominios de seguridad



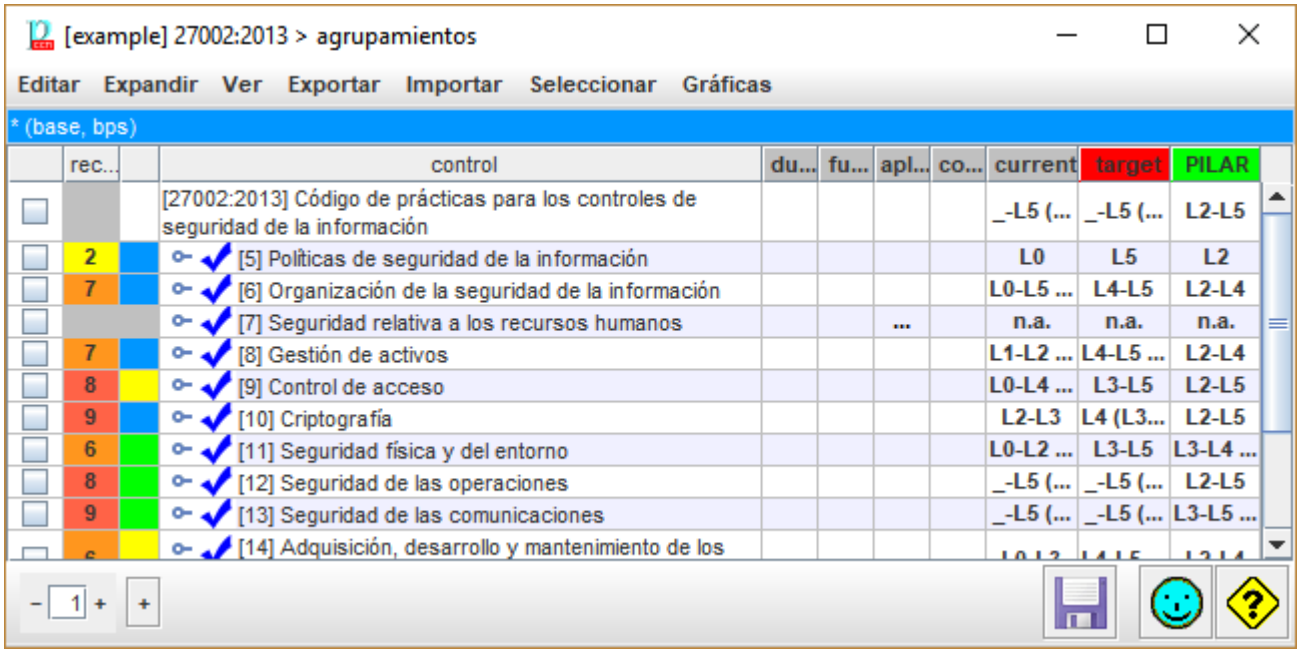
9.13 Grupos de dominios de seguridad

La valoración por dominios de seguridad es buena para los detalles; pero dificulta una visión global del sistema.

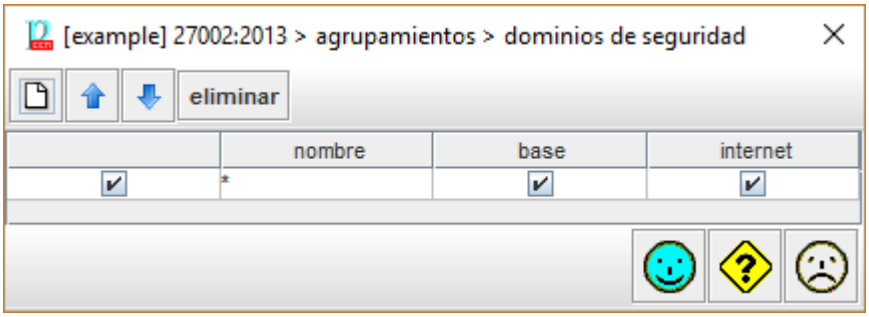
Para tener una visión global, vamos a “agrupamientos”:



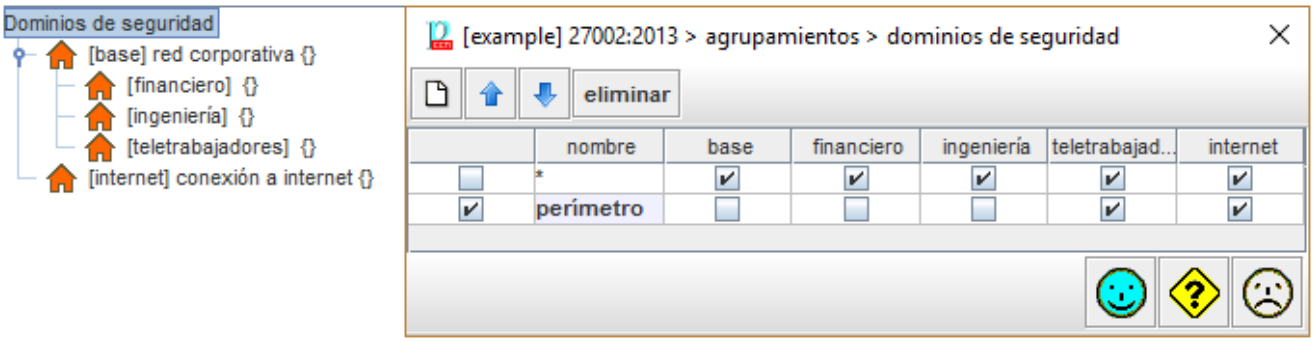
La pantalla de agrupamientos es bastante similar a la de valoración, pero solo permite leer datos:



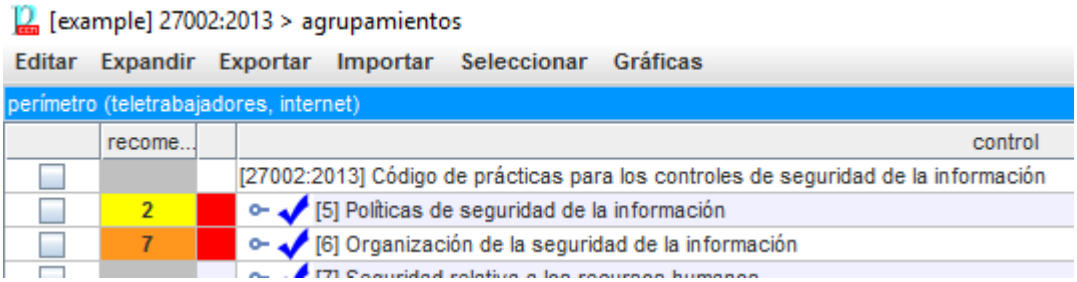
En la banda azul superior, el usuario puede editar y seleccionar agrupamientos. Por defecto, siempre hay un grupo que incluye todos los dominios



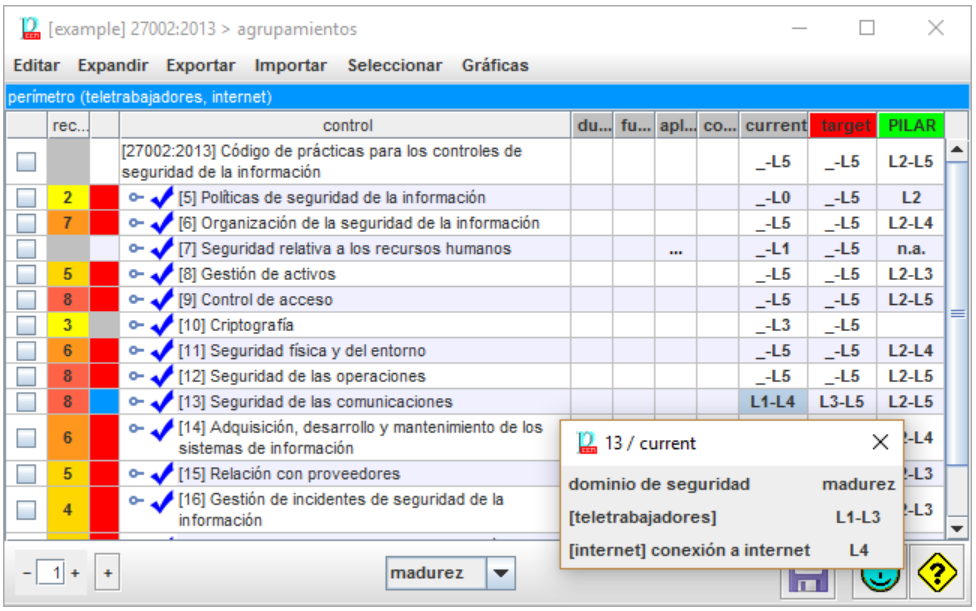
Ese grupo no admite modificaciones. El interés real está en los grupos definidos por el usuario cuando tiene múltiples dominios:



Ahora los usuarios pueden seleccionar sus grupos



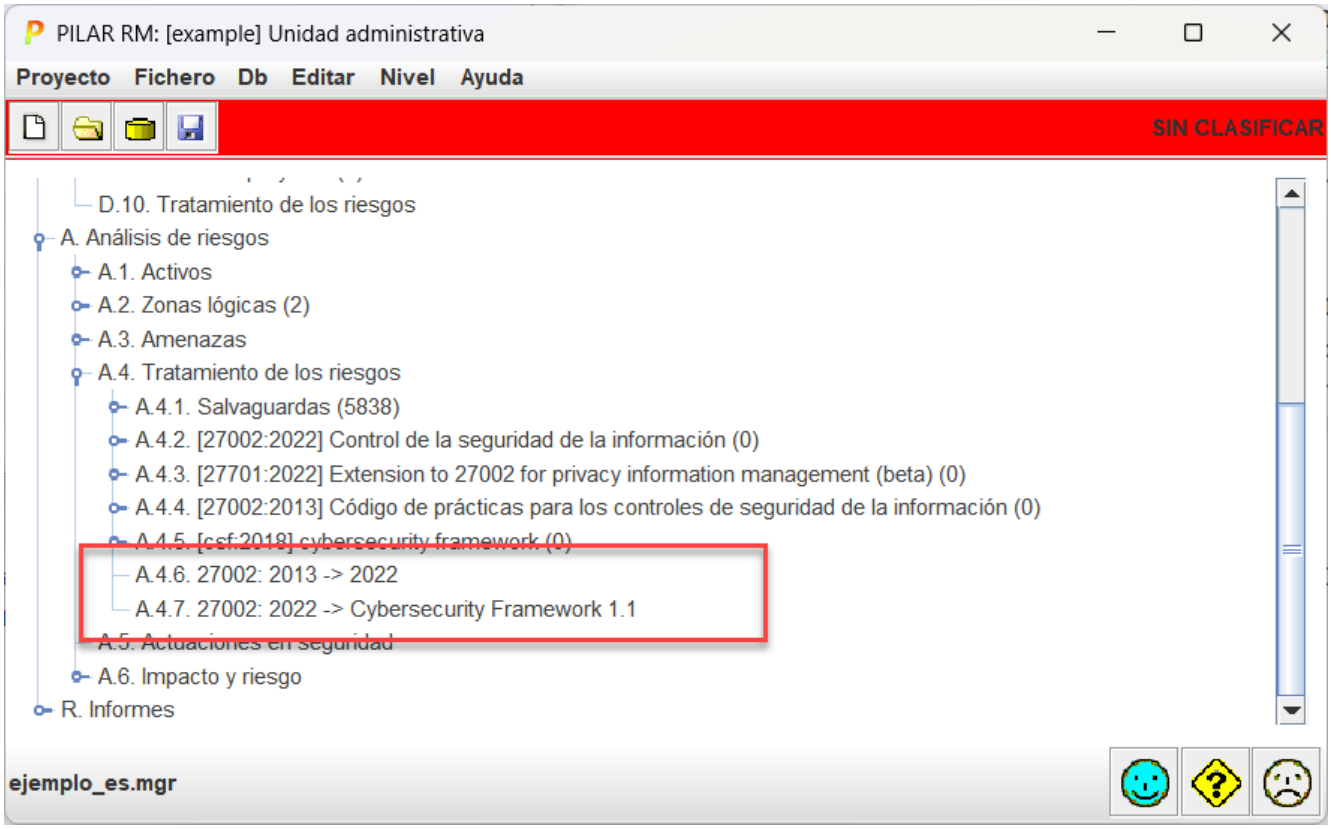
En las columnas para madurez, dudas, etc., el usuario recibe un resumen del valor correspondiente en cada dominio. Por ejemplo:



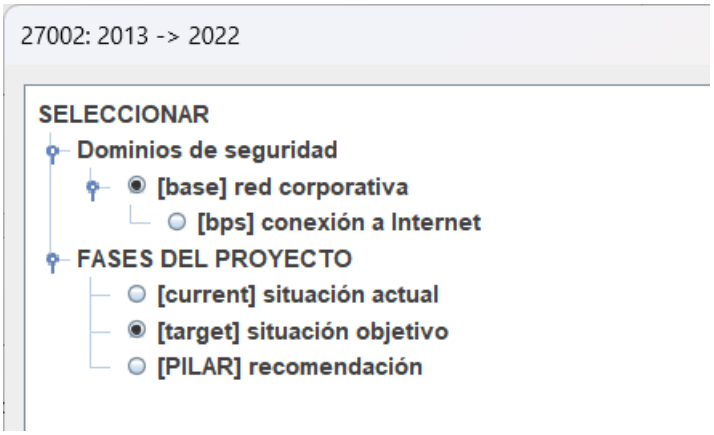
9.14 EVL-EVL (Mapping)

PILAR alinea los controles de un perfil de seguridad con los controles de otro perfil de seguridad. Esta funcionalidad es útil, por ejemplo, para estimar los valores ISO 27002:2022 a partir de los valores ISO 27001:2015 ya conocidos.

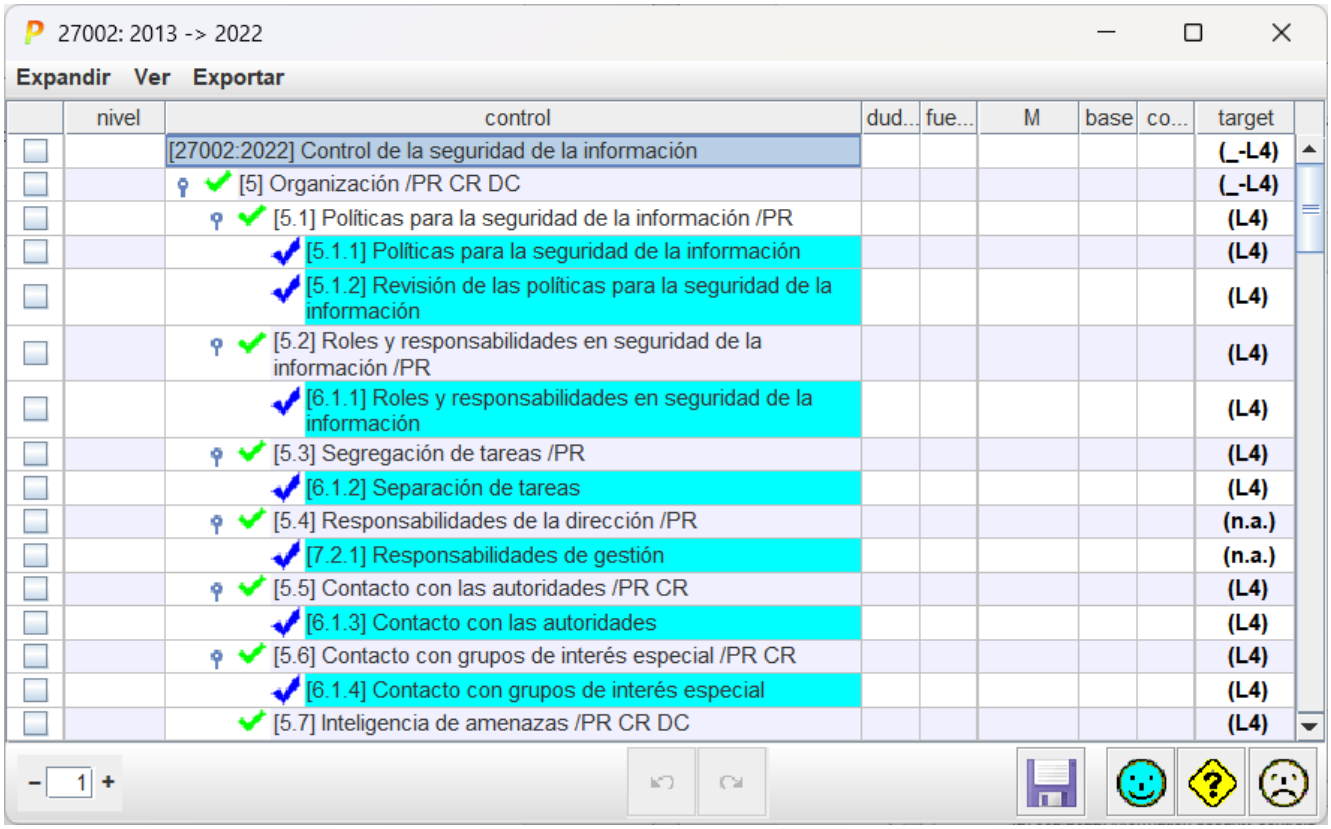
Puede haber varias asociaciones disponibles en su instalación. Por ejemplo:



Cuando hace clic en una asociación, debe seleccionar un dominio de seguridad y una fase para traducir los valores del evl izquierdo al evl derecho.



Y entonces aparece un panel para transferir valores:



Las filas presentadas como letras negras sobre fondo cian son valoraciones del EVL origen (antiguo).

Las filas negras sobre blanco son la valoración del EVL destino (nuevo).

Los valores entre paréntesis muestran la valoración de las salvaguardas asociadas.

Puede establecer niveles de madurez y comentarios sobre el (nuevo) EVL. La propagación de estos valores a las salvaguardas depende de la configuración de propagación para el perfil correspondiente.

Puede pedirle a PILAR que sugiera un valor para el destino teniendo en cuenta la fuente.