GUÍA/NORMA DE SEGURIDAD DE LAS TIC (CCN-STIC-472D)

MANUAL DE USUARIO PILAR BASIC

VERSIÓN 5.3

NOVIEMBRE 2013

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE LA PRESIDENCIA

NIPO: 002-13-056-1

Fecha de Edición: noviembre de 2013
José A. Mañas ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

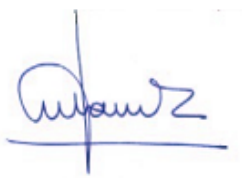
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Noviembre de 2013



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

Conceptos

1. SOBRE LA GESTIÓN DE RIESGOS

Para conocer el estado de seguridad de un sistema, necesitamos modelarlo, identificando y valorando sus activos, e identificando y valorando las amenazas sobre dichos activos. Así pues, podemos estimar el riesgo a que el sistema está sujeto.

El riesgo se puede mitigar por medio de las salvaguardas o contramedidas desplegadas para proteger el sistema. Es inusual que las salvaguardas reduzcan el riesgo a cero; es más frecuente que sigua existiendo un riesgo residual que la organización o bien pueda aceptar, o bien intente reducir más, estableciendo un plan de seguridad orientado a llevar el riesgo a niveles aceptables.

El análisis de riesgos proporciona información para las actividades de tratamiento de los riesgos. Estas actividades se ejercen una vez y otra vez, incorporando nuevos activos, nuevas amenazas, nuevas vulnerabilidades, y nuevas salvaguardas.

EAR es un conjunto de herramientas

- para realizar un análisis de riesgos, sobre las diversas dimensiones de seguridad (confidencialidad, integridad, disponibilidad,…)
- o un análisis de continuidad de operaciones, centrado en la disponibilidad del sistema, buscando reducir los tiempos de interrupción del servicio cuando sobrevienen desastres.

En cualquier caso, el análisis puede ser cualitativo o cuantitativo. PILAR implementa la metodología Magerit: [http://administracionelectronica.gob.es/].

1.1. LECTURAS RECOMENDADAS

- Magerit: versión 3,
  "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información".
  http://administracionelectronica.gob.es/
- UNE-ISO 31000:2010
  Gestión del riesgo – Principios y directrices.
- UNE-ISO/IEC Guía 73:2010
  Gestión del riesgo – Vocabulario.
- UNE-EN 31010:2011
  Gestión del riesgo – Técnicas de apreciación del riesgo.
- UNE 71504:2008
  Metodología de análisis y gestión de riesgos de los sistemas de información, AENOR.
- ISO/IEC 27005:2011
  Information technology -- Security techniques -- Information security risk management.
- NIST SP 800-39:2011
  Managing Information Security Risk: Organization, Mission, and Information System View
  http://csrc.nist.gov/publications/PubsSPs.html

- NIST SP 800-37 Rev. 1, 2010
  Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
  http://csrc.nist.gov/publications/PubsSPs.html
- NIST SP 800-30:2002
  Risk Management Guide for Information Technology Systems.
  http://csrc.nist.gov/publications/PubsSPs.html
- ISACA:2010
  The Risk IT Framework
  http://www.isaca.org/
- ISACA:2009
  The Risk IT Practitioner Guide
  http://www.isaca.org/
- AS/NZS 4360:2004
  Risk management

1.2. OTRA DOCUMENTACIÓN

- Glosario de Términos
  [http://www.pilar-tools.com/es/glossary/index.html]
- PILAR
  [http://www.pilar-tools.com/es/tools/pilar/doc.htm]

2. INSTALACIÓN

2.1. ENTORNO JAVA

Se necesita un

JRE – Entorno de ejecución Java

- visite [http://java.com]
- y siga las instrucciones
  - paso 1: descargar
  - paso 2: instalación
  - paso 3: probar

2.2. PILAR (WINDOWS)

Cuando Java esté instalado…

- ejecute `pilarbasic_<version>_<lang>.exe`
- acepte las condiciones de uso
- siga las instrucciones para instalar en el directorio que prefiera
  (varios idiomas pueden compartir el mismo directorio de instalación)
- cuando la instalación termine, habrá un archivo
  `pilarbasic.exe`
  donde haya decidido instalar el software.

Cuando el programa arranque se mostrarán los términos de la licencia.

2.3. PILAR (UNIX, LINUX, …)

Cuando Java esté instalado…

- descomprima `pilarbasic_<version>_<lang>.tar.gz` en donde considere apropiado
  (varios idiomas pueden compartir el mismo directorio de instalación)
- cuando la instalación termine, habrá un archivo
  `pilarbasic.jar`
  donde haya decidido instalar el software.

Cuando el programa arranque se mostrarán los términos de la licencia.

2.4. PILAR (MAC OS X)

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

- abra `pilarbasic_<version>_<lang>.dmg`
- ejecute la aplicación `INSTALL`, colocando los ficheros donde crea conveniente

- al terminar la instalación, debe encontrar un fichero `pilarbasic.app`

Cuando el programa arranque se mostrarán los términos de la licencia.

2.5. USO

Ejecute `pilarbasic.exe, pilarbasic.jar o pilarbasic.app`:

- le pedirá un fichero configuración:
  BASIC_ens.car

  llevándole a la "*Primera pantalla*".

El fichero .car especifica un directorio para la biblioteca. Si en ese directorio hay más de una biblioteca (fichero .pl5), PILAR le pedirá que seleccione una, y sólo una para cargar. Puede guardar varias librerías en el mismo directorio; pero sólo puede usar una en cada momento.

Vea "[http://www.pilar-tools.com/en/tools/pilar/first_time/index.html]: capturas de las primeras pantallas".

2.6. FICHERO DE CONFIGURACIÓN

PILAR incluye en la distribución algunos ficheros de configuración, en el directorio de instalación.

Se supone que la configuración por defecto será apropiada para la mayor parte de los usuarios.

Estos ficheros son texto plano, sin formato, y se pueden editar para adaptar el idioma o los directorios de trabajo.

BASIC_ens.car

2.7. FICHERO DE INFORMACIÓN

Fichero en el directorio de biblioteca, con extensión .info. Está escrito en XML y proporciona algunos valores estándar para diversos contenidos.

Por ejemplo,

PILAR / bib_ens / info_es.info

```
<?xml version="1.0" encoding="UTF-8"?>
<info>

<!--
  pares clave-valor para proyectos. ver Datos del proyecto
-->
  <model>
    <key c="desc">descripción</key>
    <key c="resp">responsable</key>
    <key c="org">organización</key>
    <key c="ver">versión</key>
    <key c="date">fecha</key>
  </model>
```

```
<!–
  pares activo-valor para activos . ver Editar un activo
-->
  <asset>
    <key c="desc">descripción</key>
    <key c="resp">responsable</key>
  </asset>
  <asset family="essential">
    <key c="owner">propietario</key>
  </asset>
  <asset family="HW, COM, SI, AUX">
    <key c="location">ubicación</key>
  </asset>
  <asset family="HW, COM, SI, AUX, L, P">
    <key c="number">cantidad</key>
  </asset>
</info>

<!–
  capas estándar. ver "Menú capas
-->
<assets>
  <layer c="B">Capa de negocio</layer>
  <layer c="IS">Servicios internos</layer>
  <layer c="E">Equipamiento
    <group c="SW">Aplicaciones</group>
    <group c="HW">Equipos</group>
    <group c="COM">Comunicaciones</group>
    <group c="AUX">Elementos auxiliares</group>
  </layer>
  <layer c="SS">Servicios subcontratados</layer>
  <layer c="L">Instalaciones</layer>
  <layer c="P">Personal</layer>
</assets>
```

3. EDITAR / OPCIONES

El comportamiento de PILAR puede ser ajustado con varias opciones:

- *Opciones / Madurez*
- *Opciones / Fases especiales*

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

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

3.1. 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

3.2. 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.

4. INFORMES

4.1. 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. Para ello, se copia la información en RTF, sin modificar, salvo una serie de marcadores que siguen esta sintaxis:

<pilar> orden(es) </pilar>

El marcador se reemplaza por el contenido ordenado.

El formato se describe en

[http://www.pilar-tools.com/es/tools/pilar/doc.htm]

4.2. 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.

Modelo de valor

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

Evaluación de las salvaguardas

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

Perfil de seguridad

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

4.3. GRÁFICAS

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. Sólo mostrará el primer nivel.

Para ajustar el nivel de despliegue del árbol.

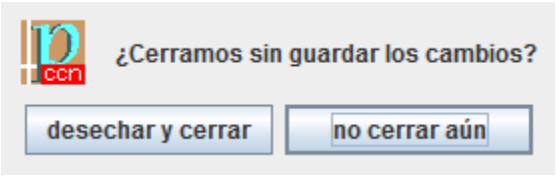
Pantallas

5. ACEPTAR, CANCELAR, AYUDA

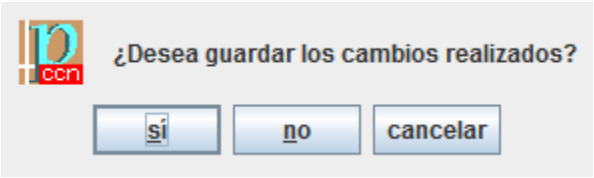
La mayoría de las pantallas incluyen los siguientes botones:

	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:



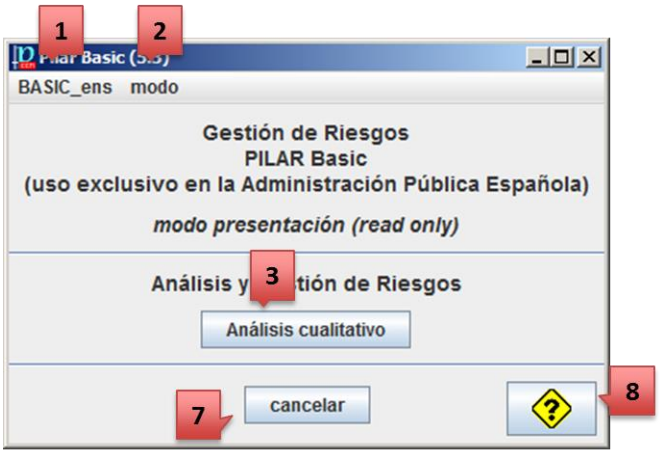
donde puede elegir

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. PRIMERA PANTALLA

Para empezar rápidamente
Para ver un análisis de riesgos (sólo lectura): • **modo / presentación** • **análisis cualitativo [3]** Para trabajar en un proyecto nuevo o ya existente: • **modo / trabajo** • vaya al directorio donde guardó la licencia (fichero .lic) y selecciónela • **análisis cualitativo**

6.1. MODO / PRESENTACIÓN



1	Selecciona un fichero de configuración. Ver "*Fichero de configuración*".
2	Modo de presentación: sólo se permite navegar por el proyecto, sin hacer cambios. *Modo / trabajo*: permite modificar el proyecto. Se requiere una licencia.
3	Inicia un análisis cualitativo: confidencialidad, integridad, disponibilidad, etc.
7	Cancelar
8	Ayuda en línea

6.2. MODO / TRABAJO

1	Selecciona una licencia
2	Presenta la licencia, incluyendo la fecha de expiración, si la hubiera. Haga clic-clic para seleccionar una licencia.
3	Protege el proyecto impidiendo modificaciones.

7. PANEL DE CONTROL

7.1. CONTROLES BÁSICOS

1	Ver *Menú proyecto*
2	**Preferencias:** tipo y tamaño de letra. **Opciones:** Ver *Editar / Opciones*
3	Ver *Menú ayuda*
	Crea un nuevo proyecto, vacío.
	Selecciona un proyecto de un fichero (.mgr)
	Guarda el proyecto en su fichero o en su base de datos.

7.1.1. MENÚ PROYECTO

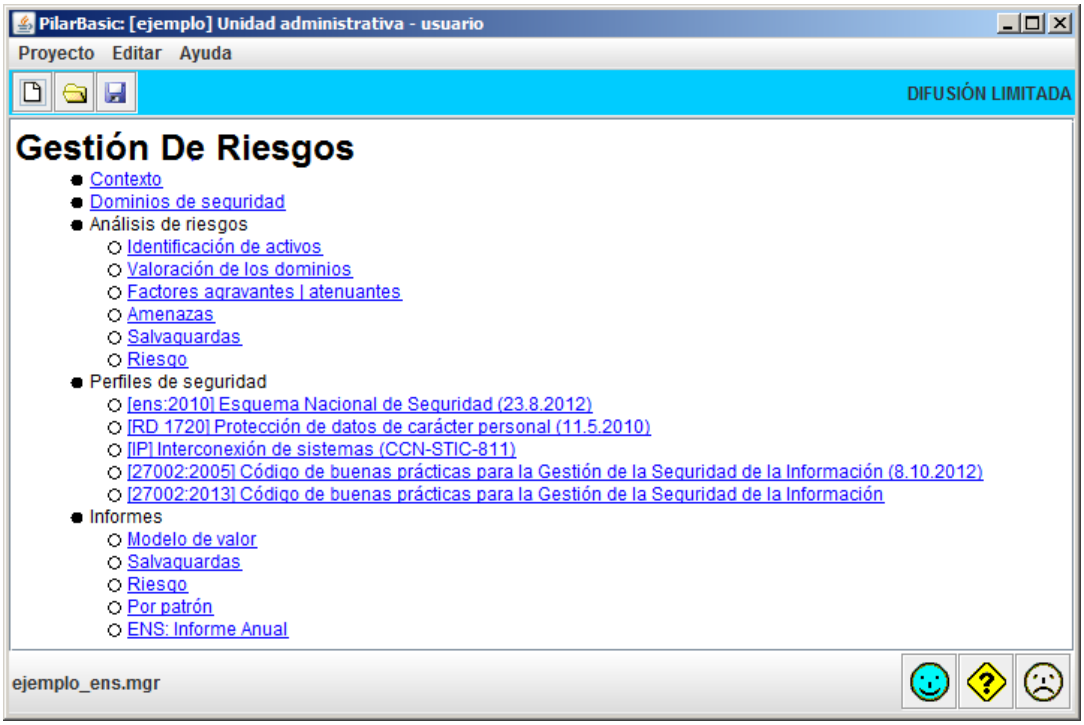
1 **Manú proyecto**	
Nuevo	Crea un nuevo proyecto, vacío
Abrir	Selecciona un proyecto existente para trabajar
Recientes	Recarga proyectos abiertos recientemente
Guardar	Guarda el proyecto en su fichero o en su base de datos
Guardar como	Guarda el fichero, seleccionando el nombre y la contraseña
Guardar y cerrar	Guarda el proyecto y termina
Cancelar y cerrar	Termina sin guardar los datos

7.1.2. MENÚ AYUDA

3 **Menú 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

7.2. CONTROLES DEL PROYECTO



La barra inferior presenta el nombre del fichero.

El árbol en el interior presenta las actividades. Haga clic para saltar a la actividad correspondiente.

- *Contexto*
- *Dominios de seguridad*
- Análisis de riesgos
  - *Identificación de activos* Identificación de activos]]
  - *Valoración de los dominios*
  - *Factores agravantes | atenuantes*
  - *Amenazas*
  - *Salvaguardas*
  - *Riesgo*
- *EVL – Perfiles de seguridad*
- Informes
  - *Modelo de valor*
  - *Salvaguardas*
  - *Riesgo*
  - *Por patrón*

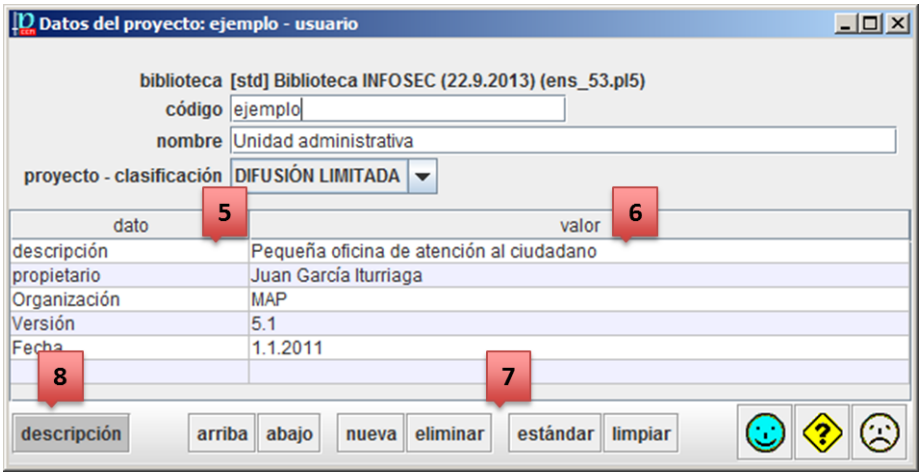
8. PROYECTO

8.1. DATOS DEL PROYECTO

Para empezar rápidamente
Seleccione un código y un nombre descriptivo. Seleccione **ESTÁNDAR** y agregue una cierta información descriptiva. Seleccione **OK** para continuar.

1	La biblioteca. Se selecciona al arrancar. Ver "*Fichero de configuración*".
2	Código del proyecto. Debería ser único.
3	El nombre del proyecto. Una descripción sucinta.
4	La marca de clasificación, por defecto, de los informes.

Se puede añadir información administrativa: pares clave-valor.

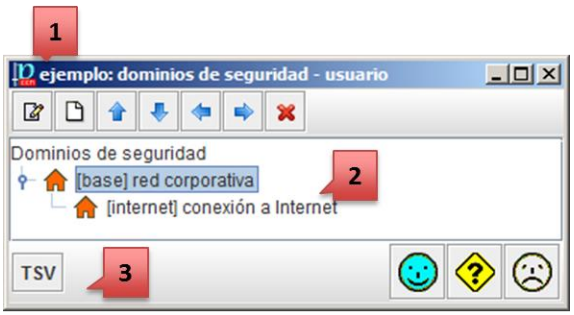


5	Claves para las parejas clave-valor. Haga clic para editar.
6	Valores para las parejas clave-valor. Haga clic para editar.
7	Operaciones sobre las parejas clave-valor. Seleccione una fila y haga clic en la operación deseada.
8	Descripción extensa del proyecto. La descripción puede incluir hiperenlaces (URLs). Para ir a la página enlazada, CLIC con el botón derecho, y después
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. Ver "*fichero de información*".
limpiar	Elimina las filas sin valor.

8.2. 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.



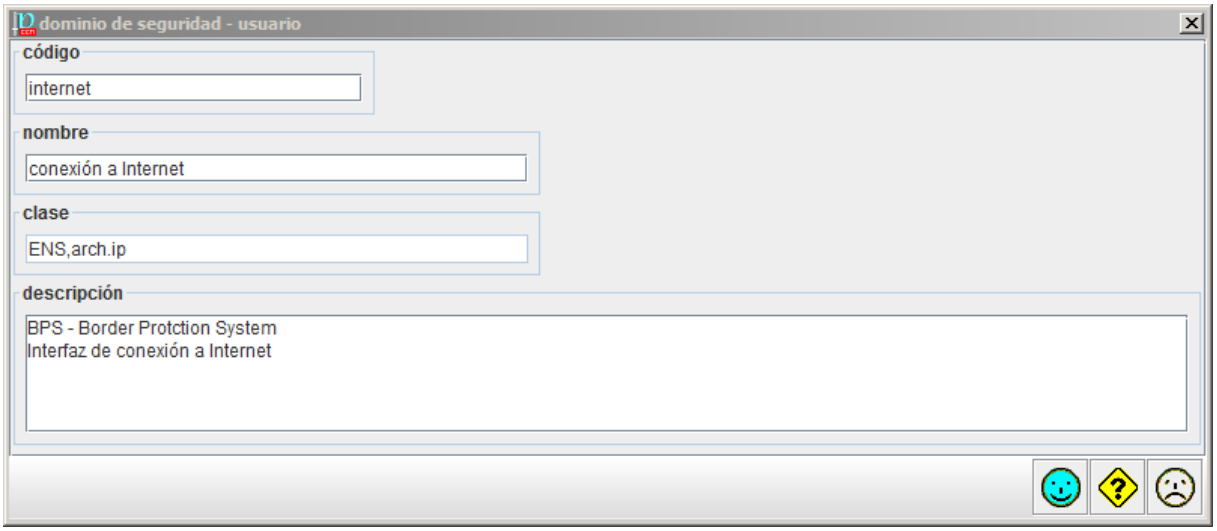
1	operaciones con dominios de seguridad
	seleccione un dominio en [2] y haga clic para editarlo
	seleccione un dominio en [2] y haga clic para añadir otro dominio dentro de él
	seleccione un dominio en [2] y haga clic para moverlo hacia arriba también: MAYÚSCULAS + FLECHA_ARRIBA
	seleccione un dominio en [2] y haga clic para moverlo hacia abajo también: MAYÚSCULAS + FLECHA_ABAJO
	seleccione un dominio en [2] y haga clic para moverlo a la izquierda también: MAYÚSCULAS + FLECHA_IZQUIERDA
	seleccione un dominio en [2] y haga clic para moverlo hacia la derecha también: MAYÚSCULAS + FLECHA_DERECHA
	seleccione un dominio en [2] y haga clic para eliminarlo también: DELETE
2	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
3	para cargar perfiles de amenazas Ver "*Threat Standard Values*

8.2.1. EDICIÓN

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

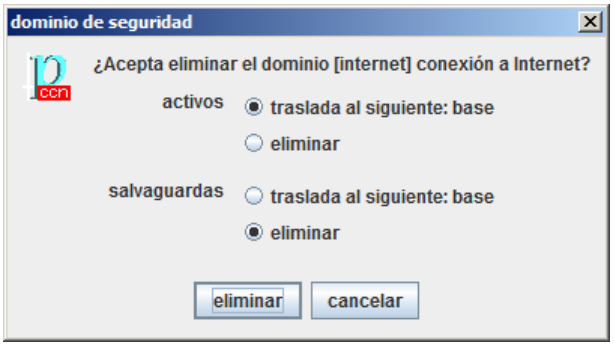
- el código, que debe ser único
- el nombre del dominio
- la clase del dominio; se puede marcar un dominio
  - ENS – sistema adscrito al perfil ENS
  - IP – punto de interconexión, perfil IP (CCN-STIC 811)
- una descripción más extensa

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



8.2.2. ELIMINACIÓN

Cuando vaya a eliminar un dominio, PILAR le preguntará qué desea hacer con los datos asociados a ese dominio. Concretamente, debe usted 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:



9. ANÁLISIS DE RIESGOS

9.1. 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

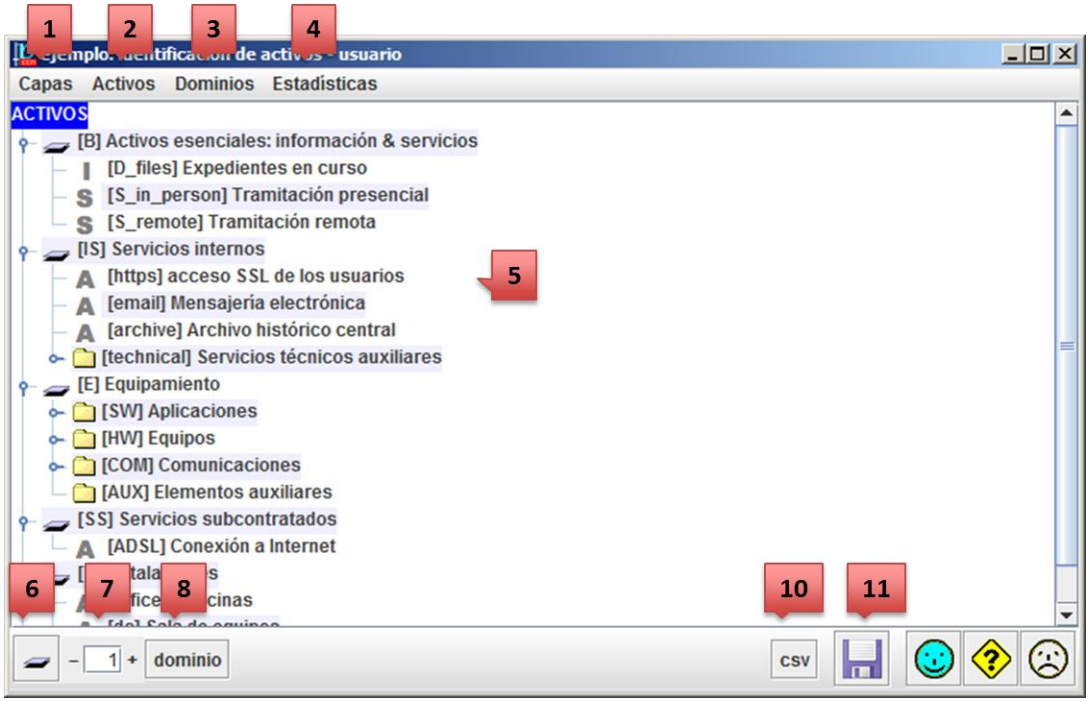
Estos son esenciales para el análisis de riesgos: los activos de verdad.

Para mover un capa, 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



1	capas	Ver "*Menú capas*".
2	activos	Ver "*Menú activos*".
3	dominios	Para editar los dominios de seguridad. Ver "*Dominios de seguridad*".
4	estadísticas	Ver "*Menú estadísticas*".
5		Los activos, organizados por capas (como volúmenes) y grupos (como directorios). Puede expandir / colapsar el árbol. Haga clic-clic para editar un activo. Ver "*Editar un activo*". Haga clic con el botón derecho para operar sobre un activo. Ver "*Operaciones sobre un activo*"-
6		Haga clic para colapsar el árbol al primer nivel.
7		Para seleccionar el nivel de expansión del árbol.
8	dominio	Haga clic y seleccione un dominio. PILAR selecciona los activos en dicho dominio.
10	csv	Exporta los datos a un fichero CSV (comma-separated values).

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

9.1.1. MENÚ CAPAS

1 **Menú capas**	
capas estándar	Incorpora las capas definidas en la biblioteca. Ver "*fichero de información*".
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 (ver *fichero de información*

- 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

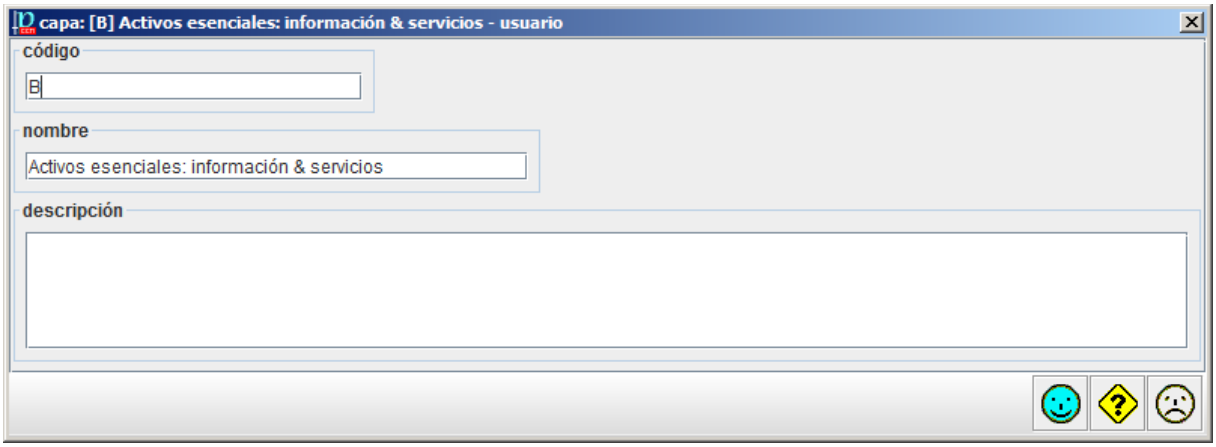
o

- 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.

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

9.1.2. MENÚ ACTIVOS

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*".
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.
ordenar	Los activos seleccionados se ordenan alfabéticamente, por código.

/ [a..z] …	
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.
tiene amenazas	El activo puede marcarse como que está libre de amenazas, o que puede tenerlas.
visible	Puede ocultar el activo: no aparecerá en las ventanas.
existe	Puede activar o inhibir un activo. Si no existe, se ignora a efectos del análisis de riesgos.
disponible	Puede detener (o volver a arrancar) un activo. Sólo afecta a su disponibilidad.

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

9.1.3. ACTIVO: ¿ES OBJETO DE AMENAZAS?

Los activos normalmente están sujetos a amenazas. Cuando se indica que un activo no tiene amenazas, las propuestas del perfil de amenazas se ignoran.

Para indicar si un activo está sujeto a amenazas o no

- seleccionar un activo
- menú activos / tiene amenazas / …

o

- seleccionar un activo
- botón derecho / tiene amenazas / …

9.1.4. ACTIVO: ¿ES VISIBLE?

Cuando un activo no es visible, no se muestra en las pantallas, ni en los reportes.

Para indicar si un activo debe estar visible o no

- seleccionar un activo
- menú activos / visible / …

o

- seleccionar un activo
- botón derecho / visible / …

9.1.5. ACTIVO: ¿EXISTE?

Cuando un activo no existe, es como si no existiera, ni tiene valor, ni lo propaga, ni tiene amenazas, ni riesgo, ni necesita salvaguardas.

Para indicar si un activo existe o no

- seleccionar un activo
- menú activos / existe / …

o

- seleccionar un activo
- botón derecho / existe / …

9.1.6. ACTIVO: ¿ESTÁ DISPONIBLE?

Cuando un activo no está disponible, estarán indisponibles también aquellos que dependen críticamente de él; es decir, sus superiores en el árbol de dependencias, excepto los que tengan opciones alternativas (OR).

Para indicar si un activo está disponible o no

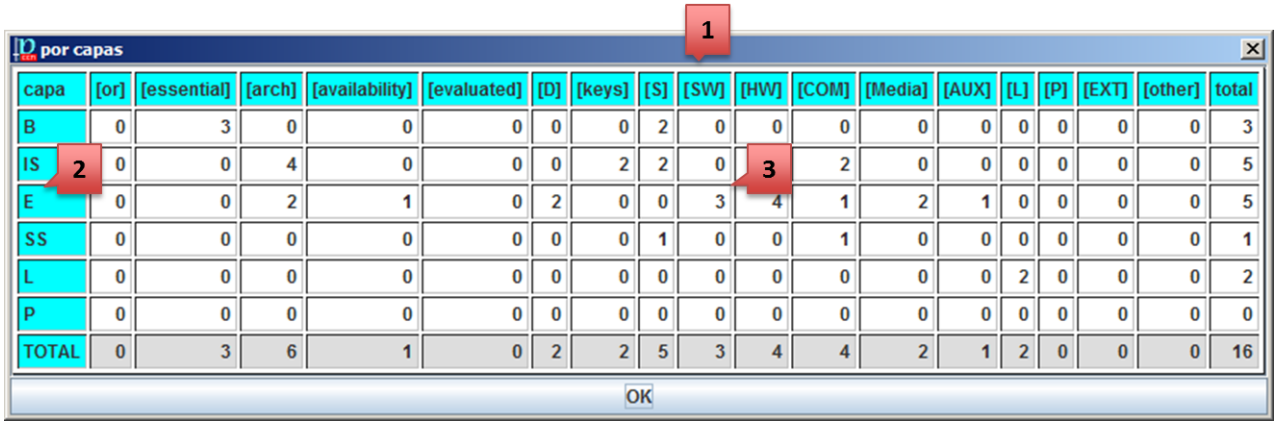
- seleccionar un activo
- menú activos / disponible / …

o

- seleccionar un activo
- botón derecho / disponible / …

9.1.7. 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	4	0	0	0	2	2	0	3	2	0	0	0	0	0	0	5
E	0	0	2	1	0	2	0	0	3	4	1	2	1	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	6	1	0	2	2	5	3	4	4	2	1	2	0	0	0	16

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.

9.1.8. 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, sólo que ahora se aplican sobre el activo bajo el ratón.

Para mover un activo de un sitio a otro

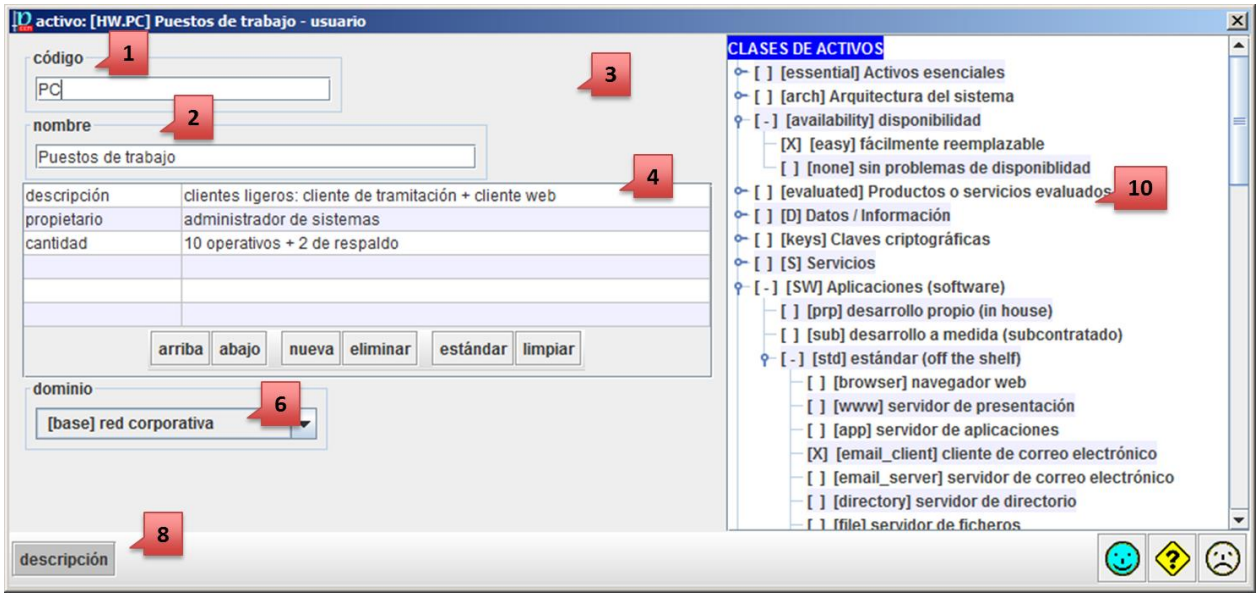
— marcar y dejar caer (drag & drop)

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

9.2. 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.



1	El código, que debe ser único
2	Una descripción sucinta: en una línea
3	Pares clave-valor para describir el activo. Sólo es a efectos informativos. Haga clic en la clave para editarla.

	Haga clic en el valor para editarlo.
4	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 en [10]. Ver "*fichero de información* — limpiar – elimina las líneas sin valor
6	Selecciona el dominio de seguridad al que pertenece el activo.
8	Una descripción más extensa. La descripción puede contener hiperenlaces (URLs). Para ir a la página enlazada, haga clic con el botón derecho y después
10	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 [X] significa que esa clase sí está asociada al activo [-] significa que alguna subclase de ésta está asociada al activo Algunas clases vienen marcadas (*). Eso significa que para ellas hay medidas adicionales de protección (KBs)

9.3. ACTIVOS / VALORACIÓN

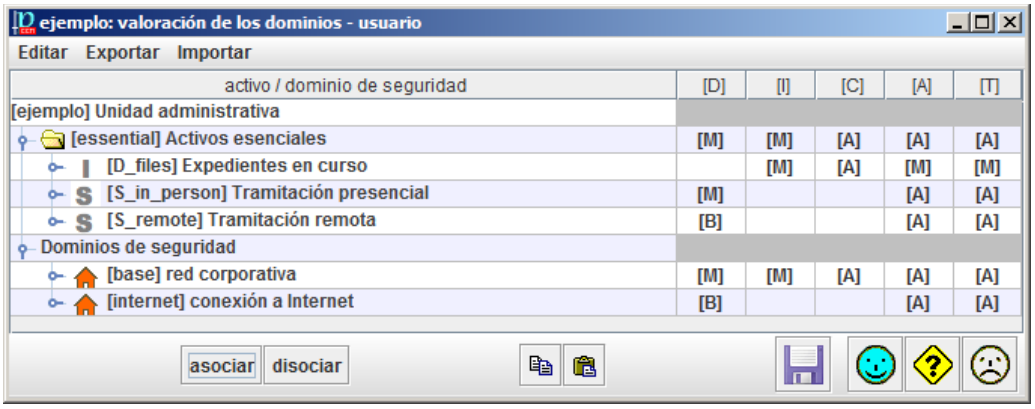
Se hace una valoración "rápida y aproximada" común para todos los activos en el dominio. Es más rápido que la valoración por dependencias. Usando este método, todos los activos en el dominio reciben los mismos valores.

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.

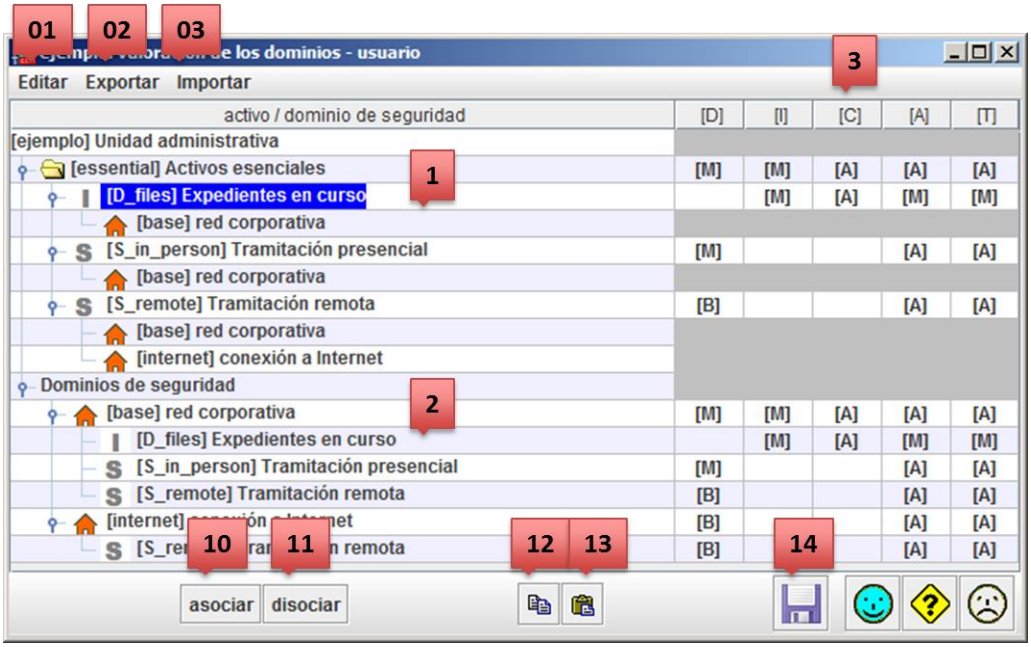
Supongamos que tenemos 2 dominios de seguridad

— [base] Seguridad corporativa

— [internet] Conexión a Internet



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



01	editar	Ver copiar [12] y pegar [13] a continuación
02	exportar	A un fichero XML
03	importar	De un fichero XML.
1	activos	Activos esenciales
2	dominios	Dominios de seguridad
3	dimensiones	Tantas columnas como dimensiones de seguridad.

4	valor de los activos	Para cada activo esencial y cada dimensión de seguridad, el valor.
5	valor de los dominios	Para cada dominio de seguridad, el valor heredado de los activos esenciales que tiene asociados
10	asociar	Seleccione un activo en [1] y un dominio en [2]. Haga clic en ASOCIAR para asociar el activo al dominio. Los activos siempre están asociados a su dominio. Usted sólo puede asociarlos a alguno más.
11	disociar	Seleccione un activo en [1] y un dominio en [2]. Haga clic en DISOCIAR para disociar el activo del dominio. Un activo nunca puede disociarse de su propio dominio.
12		Seleccione una o más celdas. Copie lo valores para pegarlos más tarde.
13		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.
14		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

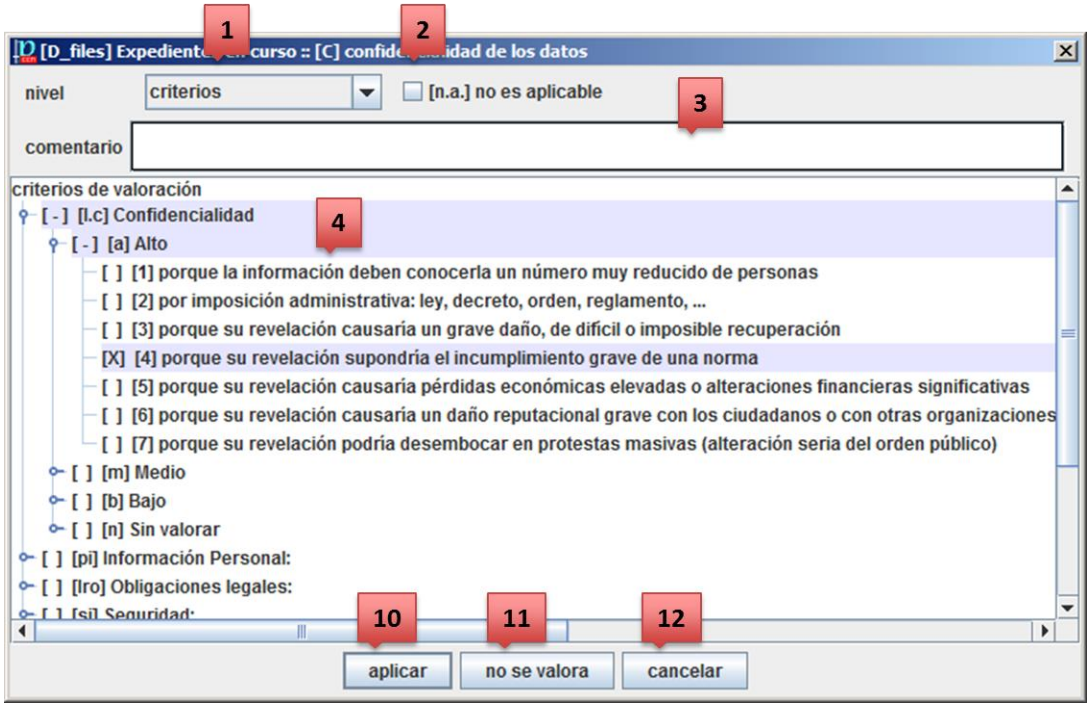
Para disociar un activo de un dominio

- seleccione el activo
- seleccione el dominio
- clic DISOCIAR

9.3.1. VALORACIÓN CUALITATIVA

Para asignar un valor a un activo

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

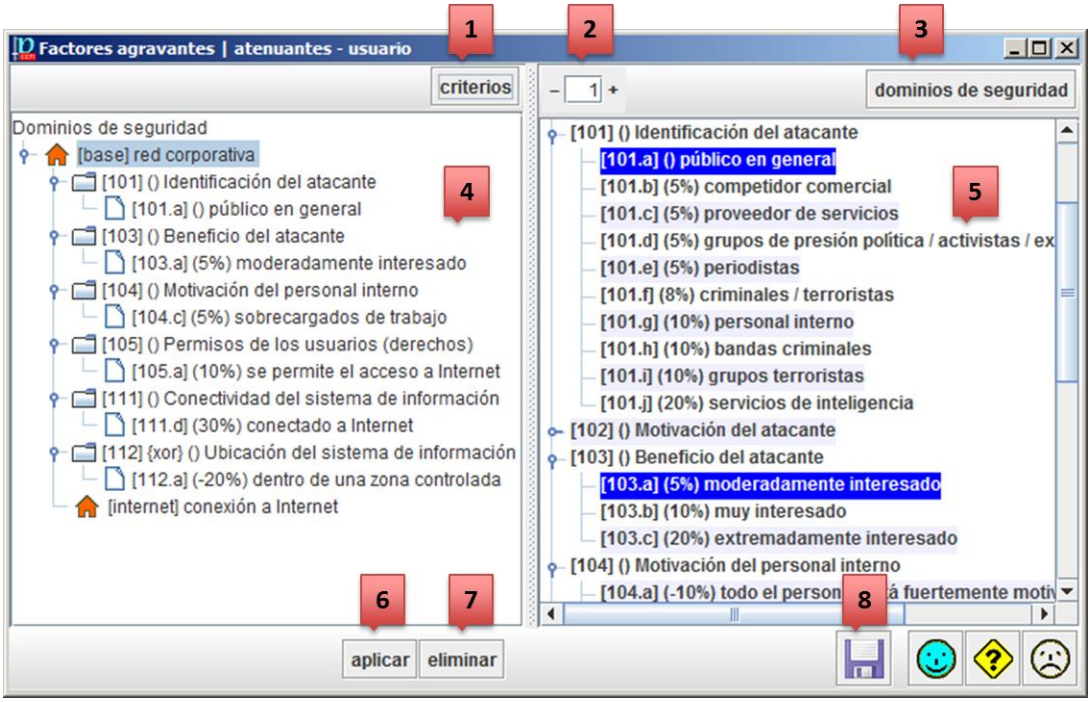


1	Si selecciona “CRITERIOS”, el valor lo decide la marca de mayor valor de los criterios marcados en [4]. Si selecciona un nivel, este será el asignado al activo, independientemente de los criterios marcados.
2	Se marca N.A. cuando esa dimensión no tiene relevancia ni para ese activo ni propaga su valor a los activos de los que depende.
3	Un comentario para explicar el por qué de la valoración
4	Criterios para valorar un activo
10	Aplica el valor y cierra la ventana
11	Elimina el valor del activo y cierra la ventana
12	Cierra la ventana sin modificar la valoración del activo

9.4. AMENAZAS

9.4.1. 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.



1	criterios	Seleccione un dominio de seguridad en [4]. Haga clic en CRITERIOS. PILAR presenta en [5] los criterios que se aplican en el dominio seleccionado.
2	– 1 +	Controla el despliegue del árbol de criterios.
3	dominios	Seleccione un criterio en [5]. Haga clic en DOMINIOS DE SEGURIDAD. PILAR selecciona en [4] los dominios a los que se aplica el criterio.
4		Dominios de seguridad
5		Criterios
6	aplicar	Seleccione uno o más dominios de seguridad a la izquierda ([4]). Seleccione uno o más dominios de seguridad a la derecha ([5]). Haga clic en APLICAR. PILAR aplica los criterios seleccionados a los dominios seleccionados.
7	eliminar	Seleccione uno o más dominios de seguridad a la izquierda ([4]). Seleccione uno o más dominios de seguridad a la derecha ([5]). Haga clic en ELIMINAR. PILAR retira los criterios seleccionados de los dominios seleccionados.
8		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

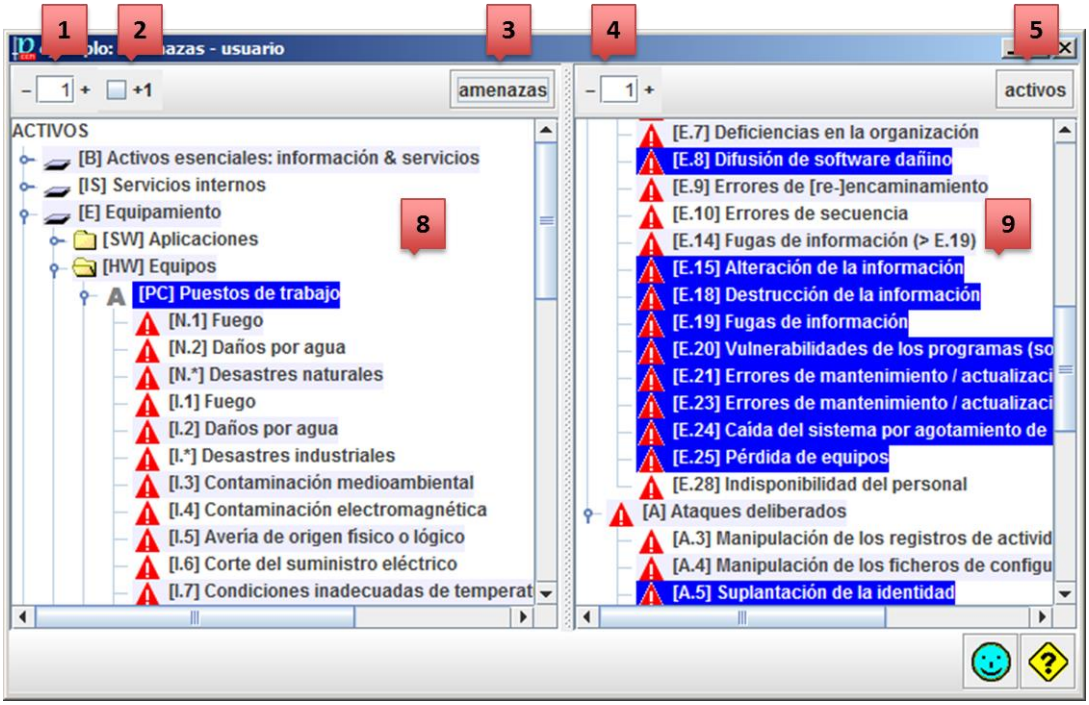
- seleccione el dominio (izquierda)
- clic CRITERIOS (panel izquierdo, barra superior)

Para descubrir a qué dominios aplica una cierta vulnerabilidad

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

9.4.2. IDENTIFICACIÓN

PILAR aplica automáticamente los valores del *fichero TSV*



1	− 1 +	Controla el despliegue del árbol de activos.
2	+1	Ajusta el efecto de [2]. Si se marca [+1], PILAR muestra también las amenazas asociadas a cada activo.

3	amenazas	— Seleccione uno o más activos a la izquierda ([8]). — Haga clic en AMENAZAS. PILAR selecciona a la derecha ([9]) las amenazas asociadas a los activos seleccionados.
4	- 1 +	Controla el despliegue del árbol de amenazas.
5	activos	— Seleccione una o más amenazas a la derecha ([9]). — Haga clic en ACTIVOS. PILAR selecciona a la izquierda los activos sujetos a dichas amenazas.
8		Activos
9		Amenazas

¿Qué amenazas afectan a un activo?

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

¿Qué activos están afectados por una amenaza?

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

9.4.3. TSV – THREAT STANDARD VALUES

Los ficheros TSV se explican en

[http://www.pilar-tools.com/es/tools/pilar/doc.htm]

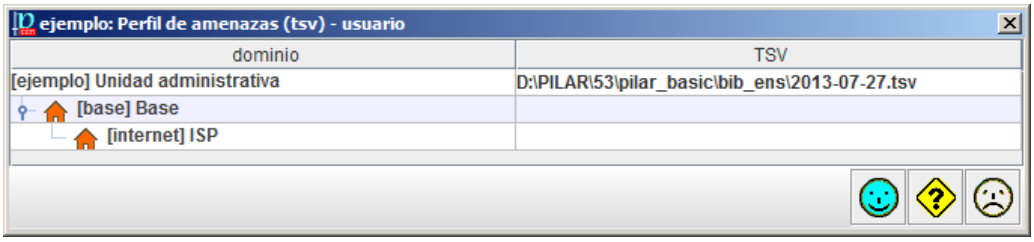
aunque también puede abrir el fichero con un editor XML

bib_ens / threats.tsv

threats.tsv	**significado**
<?xml version="1.0" encoding="UTF-8" ?> <threat-standard-values> <family F="HW"> <threat Z="E.2" f="1.0" s="6h"> <set D="D" deg="0.2"/> <set D="I" deg="0.2"/> <set D="C" deg="0.2"/> </threat> <threat Z="E.23" f="1.0" s="1d"> <set D="D" deg="0.1"/> </threat> <threat Z="E.24" f="10.0" s="30m"> <set D="D" deg="0.5"/> </threat>	formato: XML para cada activo de clase HW … aplica la amenaza E.2 con frecuencia 1.0 aplicar a la dimensión D, degradación 20% … y así sucesivamente … las dimensiones de seguridad son: D de disponibilidad I de integridad C de confidencialidad A de autenticidad T de trazabilidad

<threat Z="E.25" f="1.0" s="2d"> <set D="D" deg="1.0"/> <set D="C" deg="0.5"/> </threat> <threat Z="A.6" f="1.0"> <set D="I" deg="0.1"/> <set D="C" deg="0.5"/> </threat>	

Cuando PILAR va a cargar perfiles:



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.

9.5. SALVAGUARDAS

9.5.1. ASPECTO

Aspecto que trata la salvaguardas

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

9.5.2. 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

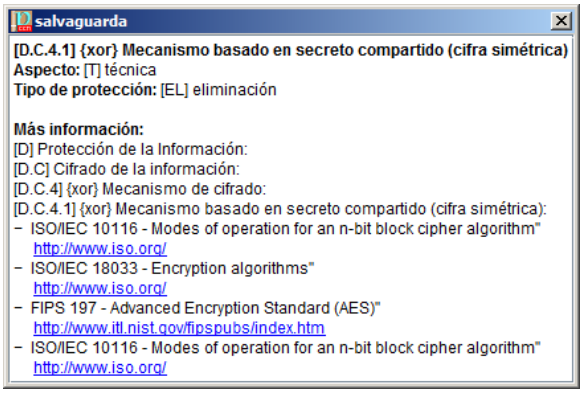
— cert – certificación o acreditación

9.5.3. PESO RELATIVO

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

9.5.4. INFORMACIÓN ADICIONAL

Una ventana separada presenta información adicional relativa a la salvaguarda



9.5.5. EN EL ÁRBOL DE SALVAGUARDAS

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

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

más información

presenta información adicional sobre la salvaguarda.

Ver "*Salvaguardas / Información adicional*".

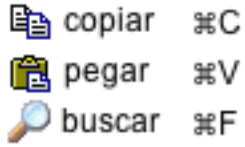
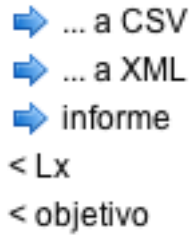
9.5.6. VALORACIÓN POR DOMINIOS

Para empezar rápidamente

- Sitúese en la celda que está en la fila **SALVAGUARDAS**, y en la columna de la fase **ACTUAL.**
- Selecciónela.
- Vaya al **combo** inferior en el centro, y seleccione el nivel de madurez que considere que en líneas generales define su sistema.
- Clic en **APLICAR** (abajo en el centro).

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.
- Vaya al **combo** inferior en el centro, y seleccione el nivel de madurez al que aspira llegar.
- Clic en **APLICAR** (abajo en el centro).

01	editar 	copiar se copia al portapapeles el valor de las celdas de madurez seleccionadas en [12] pegar se pegan en las celdas los valores copiados previamente buscar Ver "*Salvaguardas / Buscar*
02	exportar 	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*
03	importar	Lee los niveles de madures de un fichero, CSV o XML.
04	estadísticas	Genera una tabla resumen con al número de salvaguardas evaluadas en cada dominio de seguridad.
1	dominio de seguridad	Pueden haber diferentes salvaguardas en diferentes dominios. Haga clic para seleccionar el dominio en el que vamos a trabajar.
3	aspecto	Ver "*Salvaguardas / Aspecto*".
4	tdp	Ver "*Salvaguardas / Tipo de protección*".
5		Árbol de salvaguardas. Haga clic-clic para colapsar / expandir el árbol. Clic con el botón derecho para acceder a *Salvaguardas / tree*
6	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	comentario	Haga clic para asociar un comentario a la salvaguarda.
9	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.
10	semáforo	Ver "*Salvaguardas / Fases de referencia y objetivo*".
11		Fases del proyecto
12		Ver "*Salvaguardas / Valoración de la madurez*".

14		Controla el despliegue del árbol de salvaguardas.
16		Revierte los últimos cambios
17		Rehace los últimos cambios revertidos
18		Con el combo puede elegir una madurez para las *Salvaguardas / Valoración / Operaciones*
19	operación	Ver "*Salvaguardas / Valoración / Operaciones*".
20	sugiere	Ver "*Salvaguardas / Sugiere*".
21		Ver "*Salvaguardas / Buscar*".
22	>>	Ver "*Salvaguardas / Buscar*".
23		Guarda el proyecto en su fichero o en su base de datos.

9.5.7. FASE DE REFERENCIA Y FASE OBJETIVO

El semáforo [10] 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

9.5.8. VALORACIÓN DE LA MADUREZ DE LAS SALVAGUARDAS

Las celdas en la sección [12] 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 reutiliza el valor de la fase. Si después de esa búsqueda sigue sin valor, se usa el valor "L0".

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 el combo [18] y use alguna de las operaciones en "*Salvaguardas / Valoración / Operaciones*
- puede usar las operaciones copiar y pegar del menú EDITAR ([01]) para trasladar el valor de unas celdas a otras

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.

9.5.9. 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

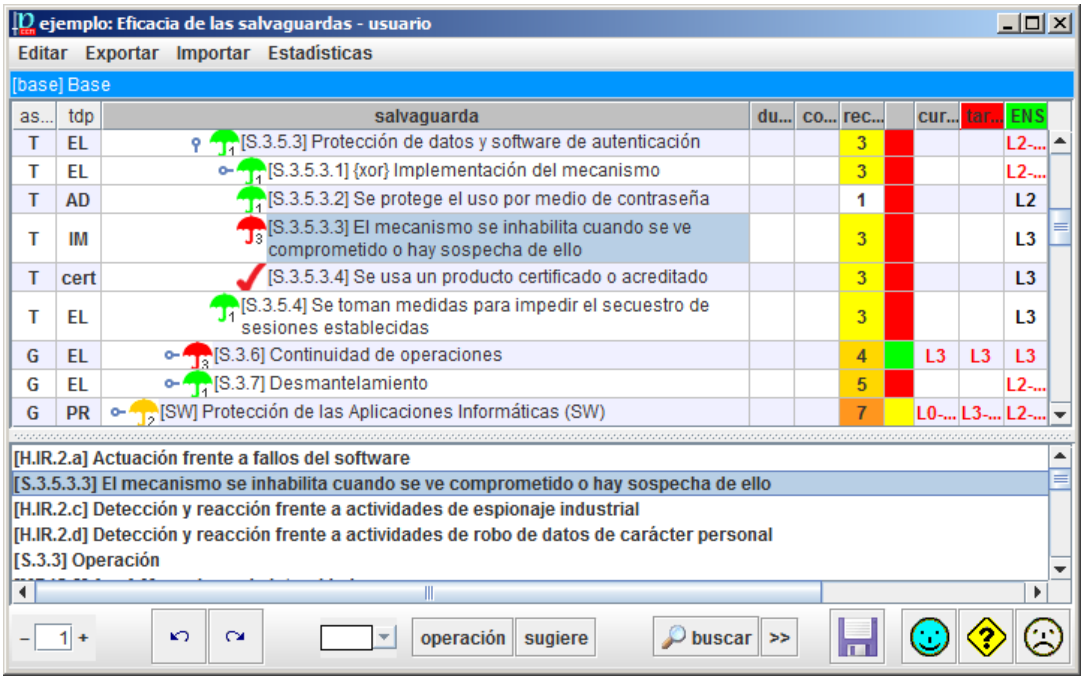
teniendo en cuenta la recomendación, PILAR sugiere unos valores de madurez que considera mínimos para satisfacer las necesidades del sistema. Meramente heurístico, con ánimo de marcar una referencia por debajo de la cual no se debería operar el sistema

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

9.5.10.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 a parte inferior y PILAR se la presentará en su contexto en la parte superior.



9.5.11.BUSCAR

PILAR puede buscar entre las salvaguardas con ciertos criterios:

CAMBIOS

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

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)

>>

busca la siguiente salvaguarda que cumple el criterio de búsqueda

9.6. IMPACTO Y RIESGO

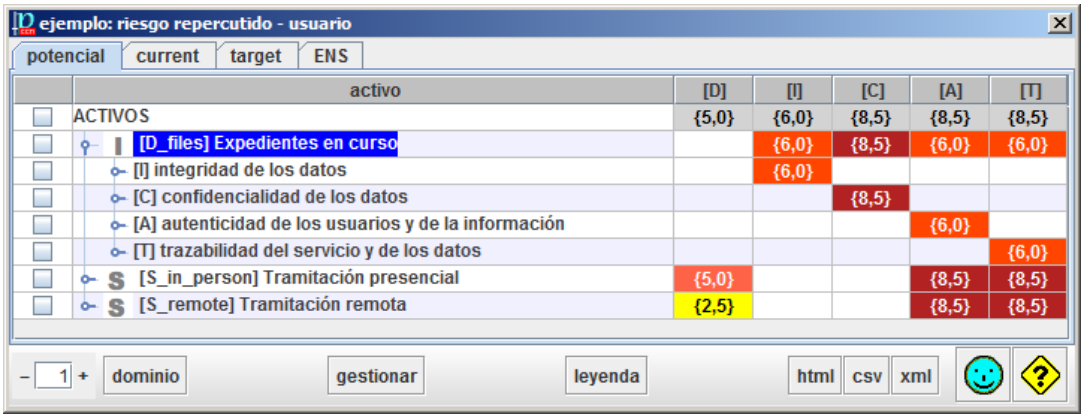
9.6.1. NIVELES DE CRITICIDAD – CÓDIGO DE COLORES

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

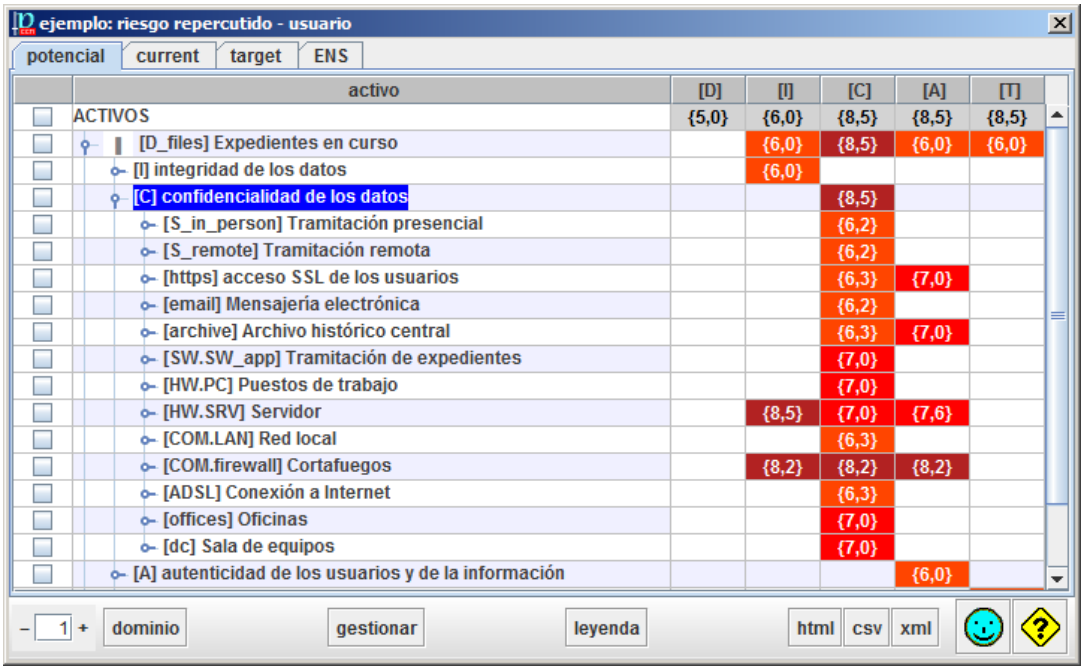
9.6.2. RIESGO REPERCUTIDO

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

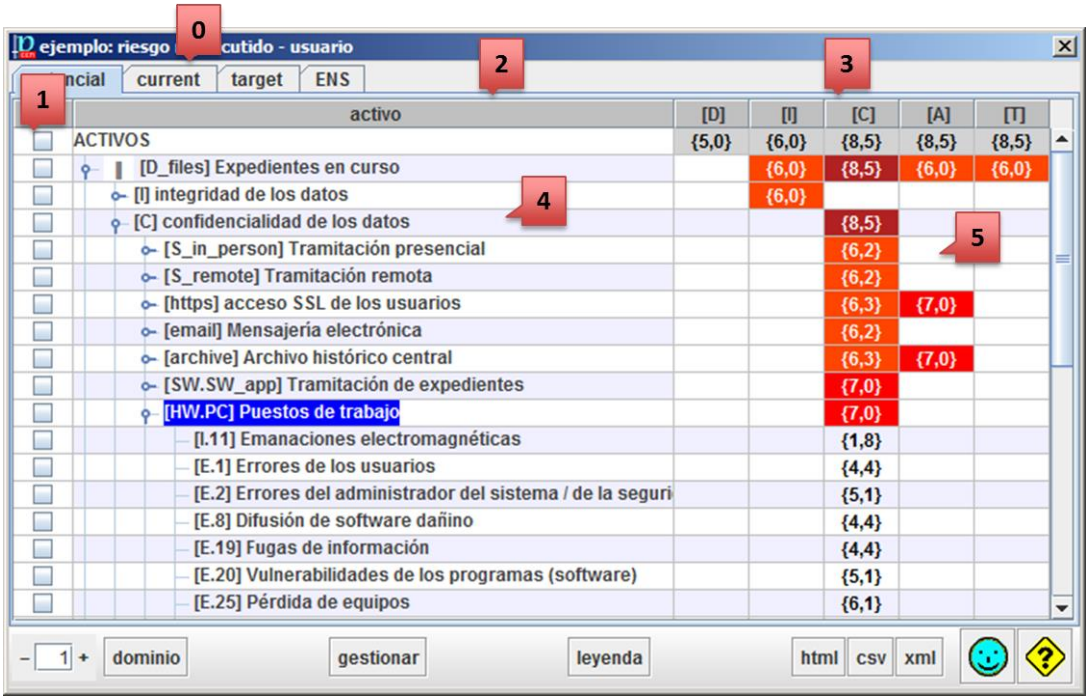
Puede expandir el árbol para segregar cada dimensión:



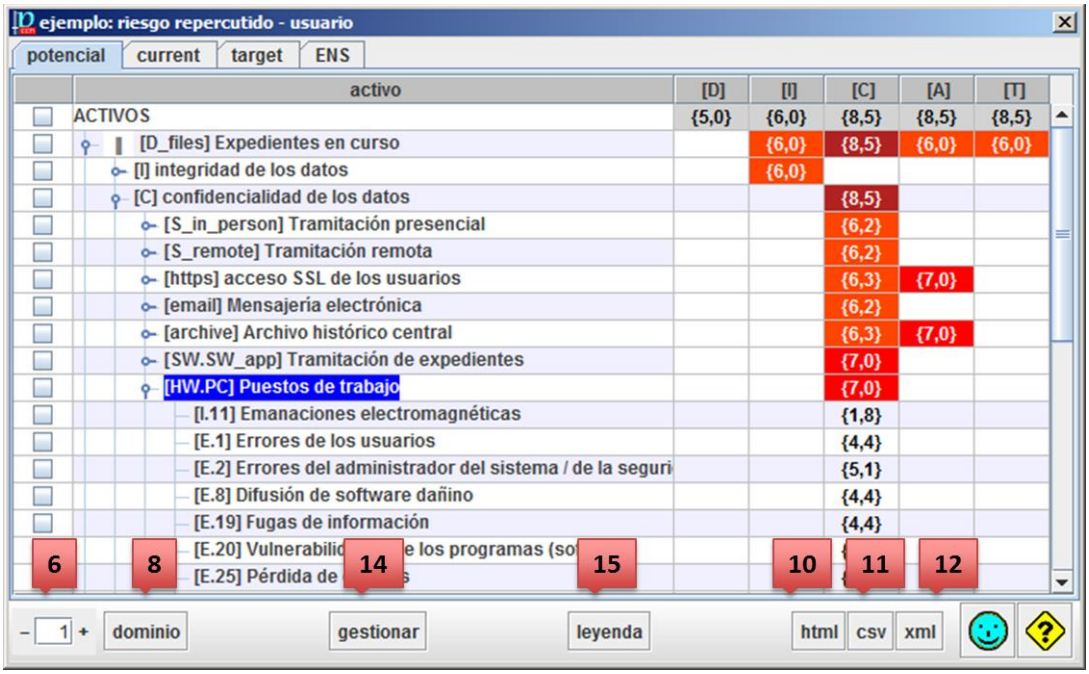
Puede seguir expandiendo el árbol para ver cómo es afectada cada dimensión en los activos de los que depende:



Y puede llegar a amenazas concretas:



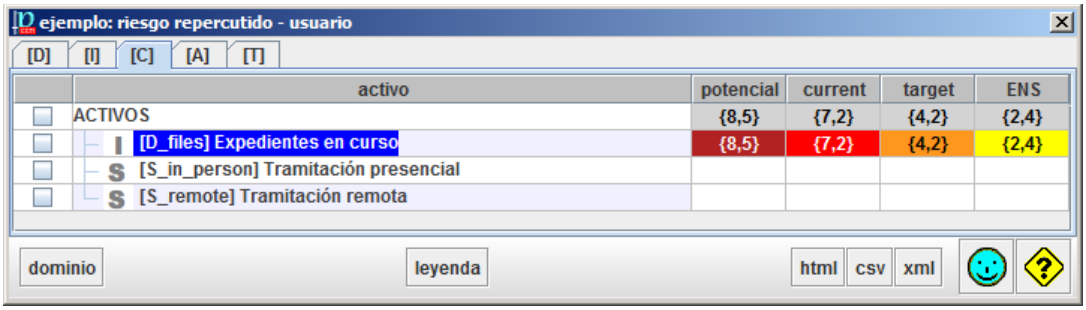
0	pestañas	Una por fase del proyecto. Haga clic para cambiar. La pseudo-fase POTENCIAL muestra el riesgo potencial (sin salvaguarda alguna).
1	selección	Haga clic en las cajitas para seleccionar / deseleccionar. Haga MAYÚSCULAS+clic para seleccionar un rango. Haga clic en la cabecera de la columna para eliminar la selección actual. La selección determina a qué filas se aplica GESTIONAR ([14]).
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.
4		Árbol de activos y amenazas. nivel 1: activos con valor propio: riesgo repercutido nivel 2: desglose por dimensión: riesgo repercutido nivel 3: activos de los que depende: riesgo acumulado nivel 4: amenazas: riesgo acumulado
5		Valores de riesgo



6	− 1 +	Para controlar el despliegue del árbol
8	dominio	Seleccione un dominio de seguridad. PILAR seleccionará los activos ([4]) en ese dominio.
10	html	Exporta los datos a un fichero HTML
11	csv	Exporta los datos a un fichero CSV
12	xml	Exporta los datos a un fichero XML
14	gestionar	Para las filas seleccionadas ([1]), PILAR recolecta los riesgos asociados y salta a la ventana de *valoración de salvaguardas*, teniendo en cuenta sólo dichos riesgos.
15	leyenda	Ver *Riesgos / Niveles de criticidad / código de colores*

Vista alternativa

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

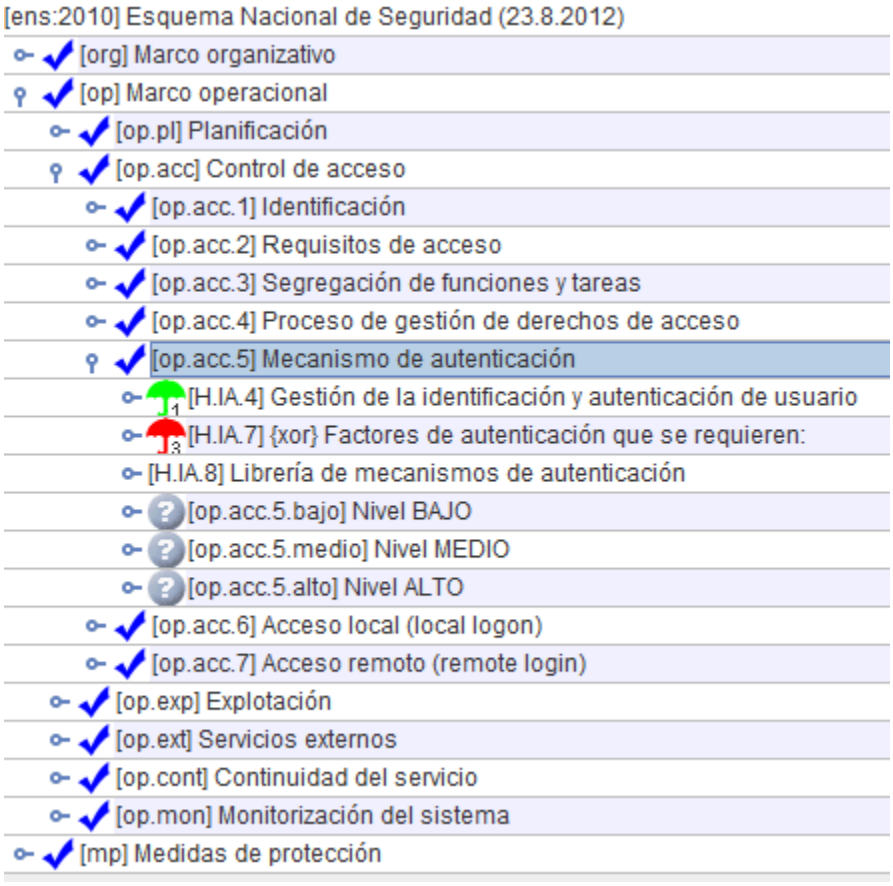

ejemplo: riesgo repercutido - usuario
[D]
[I]
[C]
[A]
[T]
activo
potencial
current
target
ENS
ACTIVOS
{8,5}
{7,2}
{4,2}
{2,4}
[D_files] Expedientes en curso
{8,5}
{7,2}
{4,2}
{2,4}
[S_in_person] Tramitación presencial
[S_remote] Tramitación remota
dominio
leyenda
html
csv
xml

10. PERFILES DE SEGURIDAD

Podemos ver la posición de seguridad del sistema desde el punto de vista de un perfil dado.

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



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

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

10.1. 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:

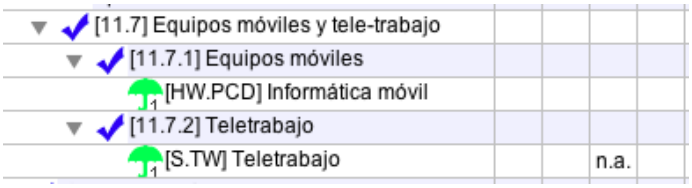
[M] Medidas de seguridad de nivel medio			...		12%	41%	95%
[95] Responsable de seguridad			M		10%	10%	95%
[96] Auditoría			M		0%	21%	94%
[97] Gestión de soportes y documentos			M		5%	47%	95%
[98] Identificación y autenticación			M		10%	90%	95%
[99] Control de acceso físico			n.a.				
[100] Registro de 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.

10.2. 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.

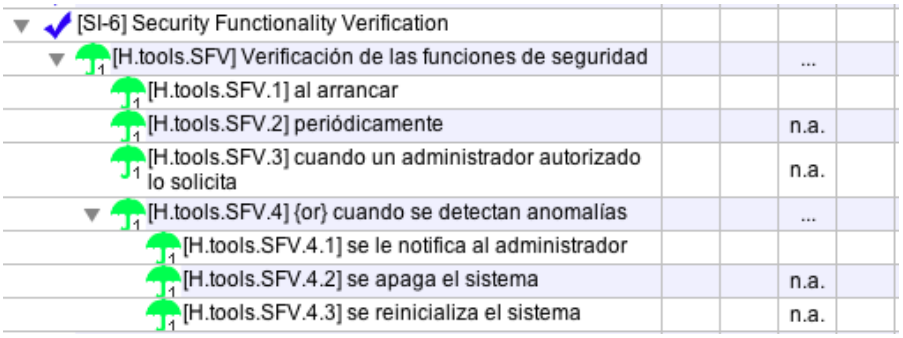
Por ejemplo, si tenemos equipos móviles, pero no tele-trabajo:

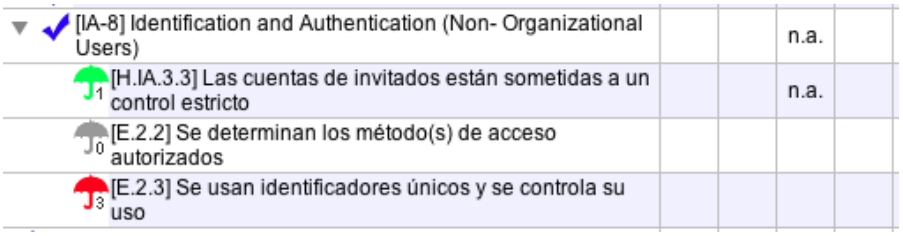


“n.a”. significa que la fila no aplica. Cuando aparecen puntos suspensivos, es porque hay algo que no aplica anidado.

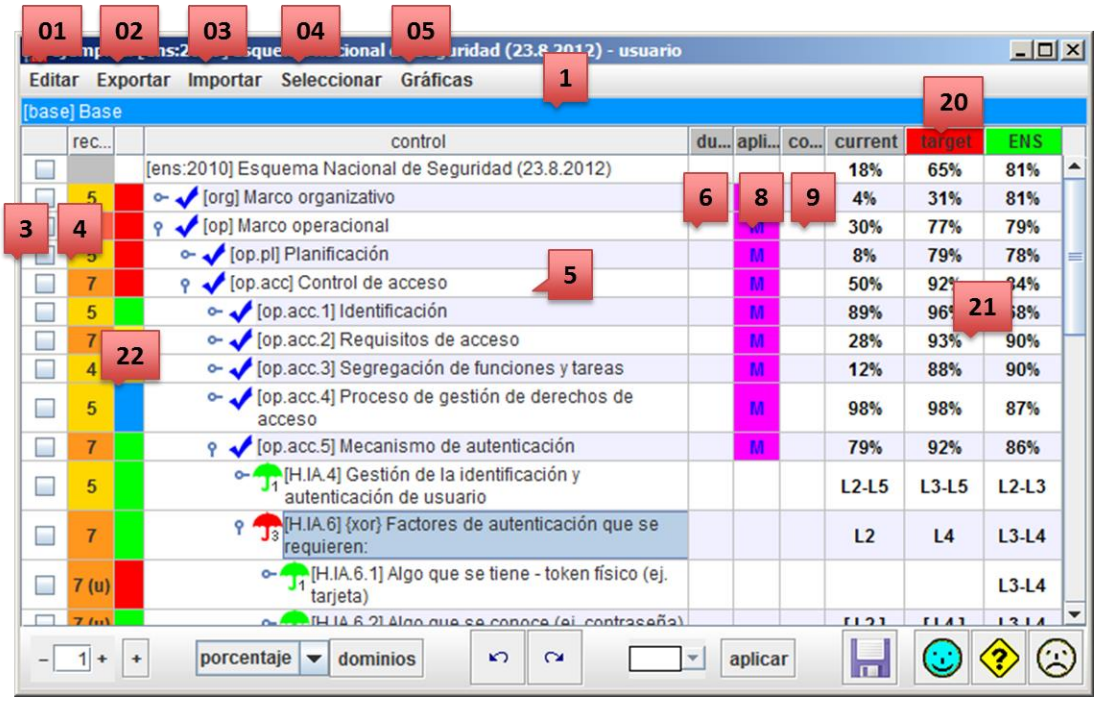
Si selecciona un control y hace clic en “n.a.”, todo lo que hay debajo pasa a “n.a.”.

Podemos tener múltiples combinaciones de controles y salvaguardas que aplican o que no. Por ejemplo:





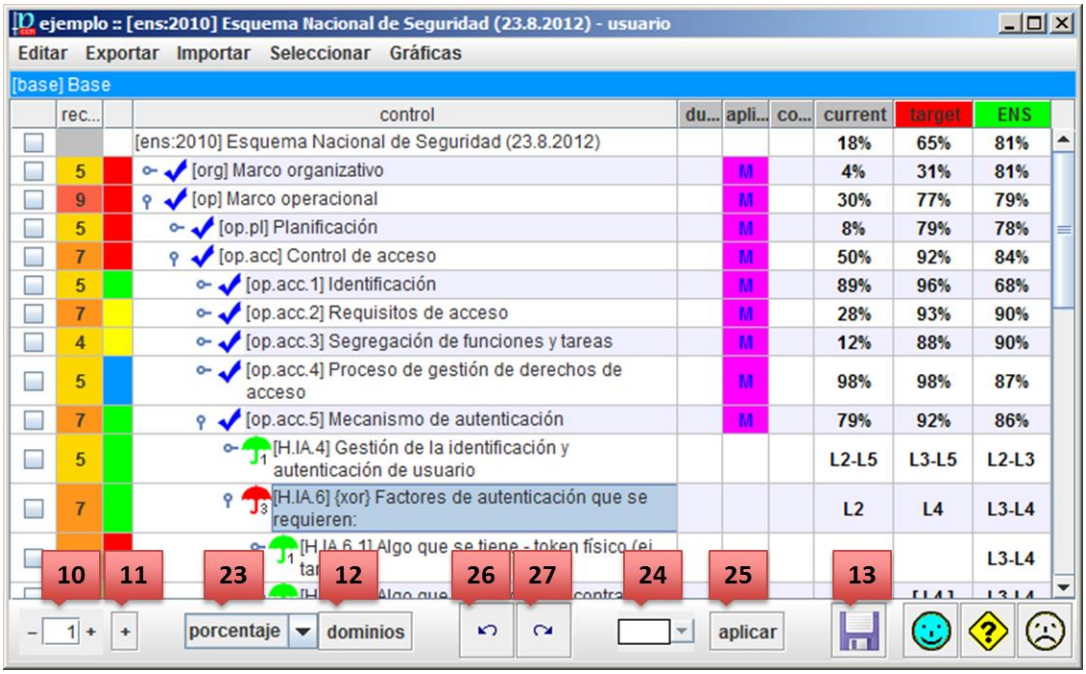
10.3. EVL – VALORACIÓN POR FASES



01	editar	buscar busca un cierto texto en el árbol [5] pregunta salta a la siguiente pregunta en el árbol [5]
02	exportar	CSV Las filas desplegadas se copian a un fichero CSV XML Los datos se copian a un fichero XML INFORME Se genera un informe RTF o HTML SoA Se genera un informe "Declaración de Aplicabilidad)
03	importar	Carga los valores de un fichero CSV o XML
04	seleccionar	borrar Borra la selección actual en [3] "nivel: #" Selecciona las filas visibles y a la profundidad indicada en [3] situación actual Selecciona controles y preguntas visibles en este momento fases del proyecto

		Permite seleccionar las fases del proyecto que queremos que aparezcan en graficas e informes
05	gráficas	dibuja los valores de las filas seleccionadas ([3]) y fases seleccionadas ([05])
1	dominio de seguridad	Pueden haber diferentes valores en diferentes dominios. Haga clic para seleccionar el dominio en el que vamos a trabajar.
3	selección	Selecciona líneas para aparecer en las gráficas
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 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.
5		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 a *EVL / tree*
6	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	aplica	Ver *EVL / Aplicabilidad*
9	comentario	Haga clic para asociar un comentario a la salvaguarda.
20		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*
21		Ver "*EVL / Valoración*"

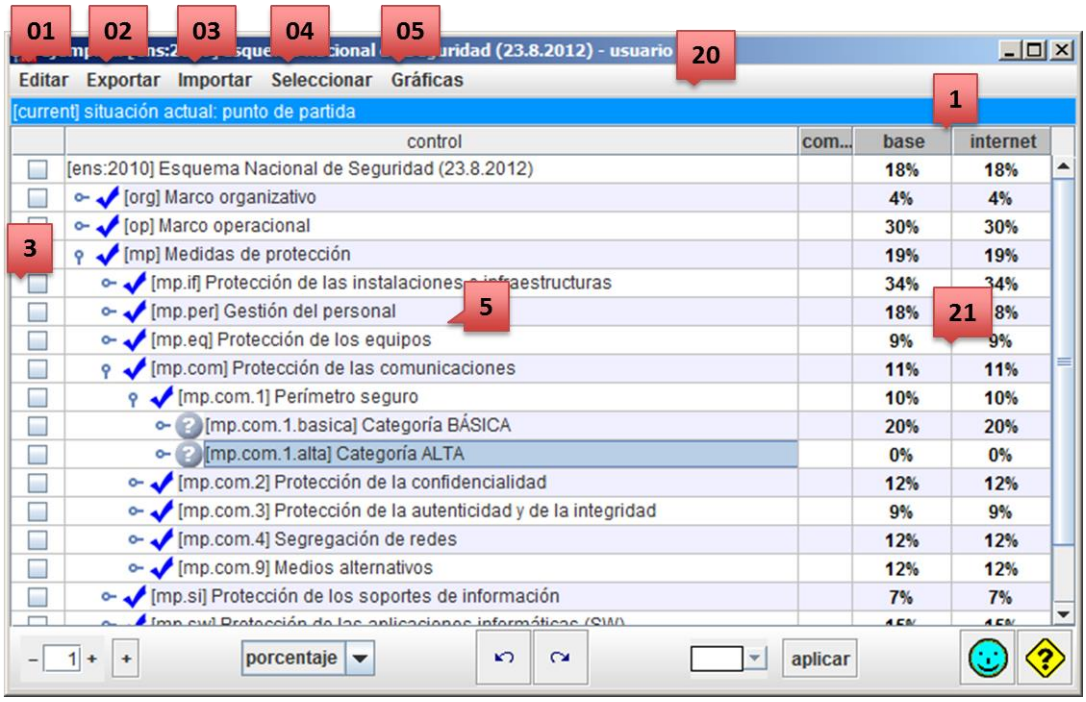
22	semáforo	Compara la valoración en la fase de referencia (ROJA) con la valoración en la fase objetivo (VERDE): ROJO el valor en la fase de referencia está muy lejos del valor objetivo AMARILLO el valor en la fase de referencia es inferior, pero cercano, al valor objetivo VERDE el valor en la fase de 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*



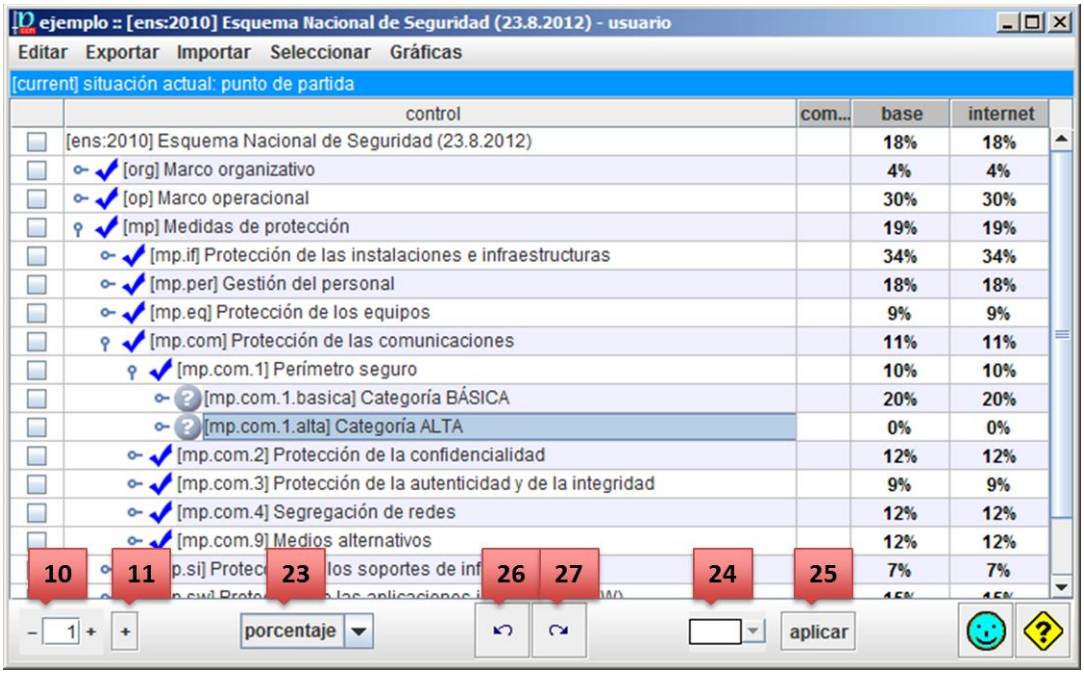
10	– 1 +	Controla el despliegue del árbol [5].
11	+	Modifica el comportamiento de [10]. Si se selecciona, el árbol se despliega incluyendo las salvaguardas asociadas a cada control.
12	dominios	Ver *EVL / dominio*
13		Guarda el proyecto en su fichero o en su base de datos.

23	porcentaje madurez PILAR	Controla cómo se presenta el valor en la zona [21] **porcentaje** — porcentaje de cobertura del control (para controles) — madurez de las salvaguardas de PILAR **madurez** — madurez de las salvaguardas y de los controles **cobertura** de **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
24		Con el combo puede seleccionar un valor para ser usado en APLICAR ([25]).
25	aplicar	— Seleccione una o más celdas en [21] — Seleccione un valor en [24] — Haga clic en APLICAR
26		Revierte los últimos cambios
27		Rehace los últimos cambios revertidos

10.4. EVL - VISTA POR DOMINIOS DE SEGURIDAD



01	editar	buscar busca un cierto texto en el árbol [5] pregunta salta a la siguiente pregunta en el árbol [5]
02	exportar	CSV Las filas desplegadas se copian a un fichero CSV XML Los datos se copian a un fichero XML INFORME Se genera un informe RTF o HTML SoA Se genera un informe "Declaración de Aplicabilidad)
03	importar	Carga los valores de un fichero CSV o XML
04	seleccionar	borrar Borra la selección actual en [3] "nivel: #" Selecciona las filas visibles y a la profundidad indicada en [3] situación actual Selecciona controles y preguntas visibles en este momento dominios de seguridad Permite seleccionar os dominios de seguridad que queremos que aparezcan en graficas e informes
05	gráficas	dibuja los valores de las filas seleccionadas ([3]) y dominios seleccionados ([05])
1	dominios de seguridad	Una columna para cada dominio de seguridad
3	selección	Selecciona líneas para aparecer en las gráficas
5		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 a *EVL / tree*
20		Fases del proyecto. Clic para cambiar.
21		Ver "*EVL / Valoración*"



10	− 1 +	Controla el despliegue del árbol [5].
11	+	Modifica el comportamiento de [10]. Si se selecciona, el árbol se despliega incluyendo las salvaguardas asociadas a cada control.
23	porcentaje madurez PILAR	Controla cómo se presenta el valor en la zona [21] **porcentaje** — porcentaje de cobertura del control (para controles) — madurez de las salvaguardas de PILAR **madurez** — madurez de las salvaguardas y de los controles **cobertura** de **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
24	L3	Con el combo puede seleccionar un valor para ser usado en APLICAR ([25]).
25	aplicar	— Seleccione una o más celdas en [21] — Seleccione un valor en [24] — Haga clic en APLICAR
26	↶	Revierte los últimos cambios
27	↷	Rehace los últimos cambios revertidos

10.5. EVL – VALORACIÓN

[SC] System and Communications Protection					30%	63%	84%
[SC-1] System and Communications Protection Policy and Procedures					24%	79%	90%
[SC-2] Application Partitioning					50%	60%	93%
[H.IA.4.2] Hay cuentas específicas para administradores de seguridad							L4
[H.AC.8.7] Se separan las responsabilidades de administración y operación					L5	L3	L3
[H.AC.4.4] Se establecen menús específicos para controlar los accesos a las funciones de las aplicaciones					L2	L3	L4

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

La valoración se aplica a las salvaguardas más detalladas, sin posterior refinamiento. Si aplica una valoración a una salvaguarda o a un control con hijos, PILAR aplica el valor a todos los descendientes.

PILAR puede presentar el valor de los controles de diferentes maneras:

porcentaje PILAR estima un porcentaje de cobertura derivado de los niveles de madurez de las salvaguardas que despiezan el control.

madurez PILAR presenta el rango de madurez (min-max) de las salvaguardas que despiezan el control.

ENS PILAR compara la madurez declarada con la madurez de la fase ENS. Si la valoración de la fase es superior o igual a la recomendada por PILAR, se presenta un valor del 100%. Si es inferior, el porcentaje disminuye en proporción.

En las celdas de valoración, también puede seleccionar

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, 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.

10.6. EVL – FASE DE REFERENCIA Y FASE OBJETIVO

El semáforo [22] 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