GUÍA/NORMA DE SEGURIDAD DE LAS TIC

(CCN-STIC-470G/1)

MANUAL DE USUARIO PILAR
ANÁLISIS Y GESTIÓN DE RIESGOS
VERSIÓN 5.4

AGOSTO 2014

Edita:

GOBIERNO DE ESPAÑA | MINISTERIO DE LA PRESIDENCIA

© Editor y Centro Criptológico Nacional, 2014

NIPO: 002140443

Fecha de Edición: agosto de 2014

José A. Mañas ha participado en la realización y modificación del presente documento.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

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.

Agosto de 2014

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. SOBRE LA GESTIÓN DE RIESGOS 9
1.1. LECTURAS RECOMENDADAS 9
1.2. OTRA DOCUMENTACIÓN 10
2. USO TÍPICO 10
2.1. USUARIO NOVEL 10
2.2. USUARIO AVANZADO 11
2.2.1. SI DESEA VALORAR LOS ACTIVOS POR MEDIO DE DEPENDENCIAS 11
2.2.2. SI DESEA APLICAR OTRO PERFIL DE AMENAZAS (TSV) 11
2.2.3. SI DESEA MODIFICAR ALGUNA AMENAZA MANUALMENTE 11
2.2.4. SI DESEA DISPONER DE MÁS FASES 12
3. INSTALACIÓN 12
3.1. ENTORNO JAVA 12
3.2. PILAR (WINDOWS) 12
3.3. PILAR (UNIX) 13
3.4. PILAR (MAC OS X) 13
3.5. USO 13
3.6. FICHERO DE CONFIGURACIÓN 13
3.7. FICHERO DE INFORMACIÓN 14
4. EDITAR / OPCIONES 15
4.1. OPCIONES / VALORACIÓN 16
4.2. OPCIONES / PROBABILIDAD 16
4.3. OPCIONES / DEGRADACIÓN 16
4.4. OPCIONES / AMENAZAS 16
4.5. OPCIONES / GUARDAR 17
4.6. OPCIONES / FASES DEL PROYECTO 17
4.7. OPCIONES / DOMINIOS DE SEGURIDAD & FASES DEL PROYECTO 17
4.8. OPCIONES / SALVAGUARDAS NO EVALUADAS 18
4.9. OPCIONES / EXPORTAR: SALVAGUARDAS 18
4.10. OPCIONES / RIESGO RESIDUAL 18
4.11. OPCIONES / MADUREZ 19
4.12. OPCIONES / FASES ESPECIALES 19
4.13. OPCIONES / TRANSFERENCIA DE VALOR ENTRE DIMENSIONES 19
5. INFORMES 20

5.1. POR PATRÓN 20
5.2. INFORMES TEXTUALES 20
5.3. GRÁFICAS 21
5.4. BASES DE DATOS 25
6. PERÍMETROS 25
7. ACEPTAR, CANCELAR, AYUDA 27
8. PRIMERA PANTALLA 28
8.1. MODO / PRESENTACIÓN 28
8.2. MODO / TRABAJO 29
9. PANEL DE CONTROL 30
9.1. CONTROLES BÁSICOS 30
9.1.1. MENÚ PROYECTO 30
9.1.2. MENÚ FICHERO 31
9.1.3. MENÚ BASE DE DATOS 31
9.1.4. IMPORTAR O INTEGRAR 32
9.1.5. MENÚ NIVEL 33
9.1.6. MENÚ AYUDA 33
9.2. CONTROLES DEL PROYECTO 33
10. PROYECTO 34
10.1. DATOS DEL PROYECTO 34
10.2. FUENTES DE INFORMACIÓN 35
10.2.1. EDICIÓN 36
10.3. DOMINIOS DE SEGURIDAD 37
10.3.1. EDICIÓN 38
10.3.2. ELIMINACIÓN 38
10.4. SUBCONJUNTO DE DIMENSIONES 39
10.5. SUBCONJUNTO DE CRITERIOS DE VALORACIÓN 39
10.6. CUANTIFICACIÓN DEL VALOR 41
10.7. SUBCONJUNTO DE AMENAZAS 42
10.8. FASES DEL PROYECTO 43
10.8.1. COMBINACIÓN Y ELIMINACIÓN DE FASES 44
10.8.2. EDITAR UNA FASE 45
11. ANÁLISIS DE RIESGOS 45
11.1. ACTIVOS / IDENTIFICACIÓN 45

11.1.1. MENÚ CAPAS ... 47
11.1.2. MENÚ ACTIVOS ... 49
11.1.3. ACTIVO: ¿ES OBJETO DE AMENAZAS? ... 52
11.1.4. ACTIVO: ¿ES VISIBLE? ... 53
11.1.5. ACTIVO: ¿EXISTE? ... 53
11.1.6. ACTIVO: ¿ESTÁ DISPONIBLE? ... 53
11.1.7. MENÚ ESTADÍSTICAS ... 53
11.1.8. OPERACIONES SOBRE UN ACTIVO ... 54
11.2. ACTIVOS / EDITAR UN ACTIVO ... 55
11.3. ACTIVOS / CLASES DE ACTIVOS ... 57
11.4. ACTIVOS / NOMBRES CPE ... 59
11.5. ACTIVOS / DEPENDENCIAS ... 61
11.5.1. MAPA DE DEPENDENCIAS ENTRE CAPAS ... 65
11.5.2. GRAFO DE DEPENDENCIAS ENTRE ACTIVOS ... 66
11.5.3. BUSES: DEPENDENCIAS ENTRE ACTIVOS ... 67
11.5.4. BLOQUES: DEPENDENCIAS ENTRE ACTIVOS ... 68
11.5.5. MAPA DE DEPENDENCIAS ENTRE ACTIVOS ... 69
11.5.6. DEPENDENCIAS POR DIMENSIÓN DE SEGURIDAD ... 71
11.6. ACTIVOS / VALORACIÓN ... 73
11.6.1. VALORACIÓN DE LOS DOMINIOS DE SEGURIDAD ... 73
11.6.2. VALORACIÓN ACTIVO POR ACTIVO ... 75
11.6.3. VALORACIÓN CUALITATIVA ... 79
11.6.4. VALORACIÓN CUANTITATIVA ... 80
11.6.5. ANULACIÓN DE UNA VALORACIÓN ... 81
11.6.6. VALORACIÓN DE LA DISPONIBILIDAD ... 82
11.7. AMENAZAS ... 83
11.7.1. FACTORES AGRAVANTES | ATENUANTES ... 83
11.7.2. IDENTIFICACIÓN ... 85
11.7.3. VALORACIÓN ... 88
11.7.4. TSV – THREAT STANDARD VALUES ... 91
11.7.5. VULNERABILIDADES TÉCNICAS (CVE) ... 92
11.8. SALVAGUARDAS ... 95
11.8.1. ASPECTO ... 95
11.8.2. TIPO DE PROTECCIÓN ... 95

11.8.3. PESO RELATIVO ... 95
11.8.4. INFORMACIÓN ADICIONAL ... 96
11.8.5. EN EL ÁRBOL DE SALVAGUARDAS ... 96
11.8.6. IDENTIFICACIÓN ... 97
11.8.6.1. MENÚS BARRA SUPERIOR ... 97
11.8.6.2. PANTALLA PRINCIPAL, CUERPO ... 98
11.8.6.3. BARRA INFERIOR DE HERRAMIENTAS ... 100
11.8.6.4. SÓLO SI … ... 101
11.8.6.5. SOA – DECLARACIÓN DE APLICABILIDAD ... 101
11.8.7. VALORACIÓN POR DOMINIOS ... 102
11.8.7.1. BARRA SUPERIOR - MENÚS ... 103
11.8.7.2. PANTALLA PRINCIPAL – CUERPO ... 104
11.8.7.3. BARRA INFERIOR DE HERRAMIENTAS ... 106
11.8.8. VALORACIÓN POR ACTIVOS ... 107
11.8.9. FASE DE REFERENCIA Y FASE OBJETIVO ... 108
11.8.10. VALORACIÓN DE LA MADUREZ DE LAS SALVAGUARDAS ... 109
11.8.11. OPERACIONES ... 110
11.8.12. OPERACIÓN SUGERENCIA ... 111
11.8.13. BUSCAR ... 111
11.8.14. NORMATIVA DE SEGURIDAD ... 112
11.8.15. PROCEDIMIENTOS OPERATIVOS DE SEGURIDAD ... 112
11.9. IMPACTO Y RIESGO ... 112
11.9.1. NIVELES DE CRITICIDAD – CÓDIGO DE COLORES ... 112
11.9.2. IMPACTO ACUMULADO ... 113
11.9.2.1. VISTA ALTERNATIVA ... 115
11.9.3. RIESGO ACUMULADO ... 116
11.9.3.1. VISTA ALTERNATIVA ... 118
11.9.4. TABLA DE IMPACTO Y RIESGO ACUMULADO ... 119
11.9.4.1. RESUMEN DE IMPACTO ... 122
11.9.4.2. RESUMEN DE RIESGO ... 122
11.9.5. IMPACTO REPERCUTIDO ... 123
11.9.5.1. VISTA ALTERNATIVA ... 126
11.9.6. RIESGO REPERCUTIDO ... 126
11.9.6.1. VISTA ALTERNATIVA ... 130

11.9.7. TABLA DE IMPACTO Y RIESGO REPERCUTIDO 130
11.9.7.1. RESUMEN DE IMPACTO 134
11.9.7.2. RESUMEN DE RIESGO 134
12. PROTECCIONES ADICIONALES 135
12.1. EN EL ÁRBOL KB 135
12.2. VALORACIÓN DEL ÁRBOL KB 136
12.3. PROTECCIONES PARA UN ACTIVO 139
13. PERFILES DE SEGURIDAD 140
13.1. EVL – CONTROLES OBLIGATORIOS 143
13.2. EVL – APLICABILIDAD 143
13.3. EVL – IDENTIFICACIÓN 144
13.4. EVL – VALORACIÓN 147
13.5. EVL – FASE DE REFERENCIA Y FASE OBJETIVO 148
13.6. EVL - VALORACIÓN POR FASES 148
13.7. EVL - VALORACIÓN POR DOMINIOS DE SEGURIDAD 152

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 siga 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. USO TÍPICO

2.1. USUARIO NOVEL

1. Instale y arranque la aplicación: ver "*Instalación*".
2. Ver "*Primera pantalla*
3. Elija análisis de riesgos / análisis cualitativo
4. Cree un proyecto nuevo
5. PILAR estándar: En *Editar / Opciones* seleccione
   - valoración de los dominios: ON
   - amenazas: automáticas
6. *Identifique activos*, al menos
   - alguna información esencial
   - algún servicio esencial
   - algún equipamiento
7. Valore los activos: *Valoración por dominios*
8. Identifique las salvaguardas útiles para su sistema: *Identificación de salvaguardas*
9. Evalúe las salvaguardas identificadas: *Valoración de salvaguardas por dominios*
10. Examine el *Riesgo repercutido*
11. Repita los pasos 8, 9 y 10 hasta estar satisfecho
12. Verifique que se satisfacen los perfiles de seguridad que le interesan
13. Repita los pasos 8, 9, 10 y 11 hasta estar satisfecho

2.2. USUARIO AVANZADO

2.2.1. SI DESEA VALORAR LOS ACTIVOS POR MEDIO DE DEPENDENCIAS

La valoración por dependencias se selecciona en

editar / opciones / valoración / activos + dependencias

Este modo permite transferir el valor (o consecuencias de los incidentes) entre activos; típicamente, desde los activos esenciales hacia los demás activos del sistema.

Es un método muy laborioso, pero permite precisar en qué activos reside el valor del sistema. Es decir, de qué activos depende la protección del valor.

2.2.2. SI DESEA APLICAR OTRO PERFIL DE AMENAZAS (TSV)

Los perfiles de amenazas indican qué amenazas se pueden dar sobre cada clase de activos, determinando su probabilidad y sus consecuencias en cada dimensión de seguridad.

Se define un perfil para todo el sistema, y se puede emplear un perfil más preciso en cada dominio de seguridad.

La selección de perfiles TSV se realiza desde la pantalla de edición de dominios de seguridad.

proyecto / dominios de seguridad

2.2.3. SI DESEA MODIFICAR ALGUNA AMENAZA MANUALMENTE

En

editar / opciones / amenazas

puede elegir entre modo manual (usted elige y valora cada amenaza), modo automático (PILAR aplica el TSV indicado para el dominio, o en su defecto, el perfil del proyecto), o modo mixto (PILAR funciona automáticamente, salvo para las amenazas que se marquen como manuales).

En

análisis de riesgos / amenazas / valoración

puede marcar como manuales amenazas concretas sobre un activo concreto, o todas las amenazas sobre un cierto activo.

En

análisis de riesgos / impacto y riesgo / valores acumulados / tabla

puede marcar líneas, y por medio de

gestionar / descartar los seleccionados

o

gestionar / retener los seleccionados

pasamos a modo manual las amenazas que se descartan.

2.2.4. SI DESEA DISPONER DE MÁS FASES

Las fases permiten establecer una valoración del conjunto de salvaguardas. Una foto. Pueden usarse para recoger el progreso del plan de seguridad

día 0 -> a los 3 meses -> al cabo del primer año -> al cabo del segundo año -> al final

para anualizar el estado de seguridad

2010 -> 2011 -> 2012 -> 2013 -> 2014

para experimentar con variantes

actual -> test -> objetivo

Se pueden insertar o eliminar fases en

proyecto / fases del proyecto

3. INSTALACIÓN

3.1. 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

3.2. PILAR (WINDOWS)

Puede instalar PILAR como administrador o como usuario normal. Los archivos se pueden instalar en cualquier lugar. Si tiene privilegios de administrador, los archivos pueden entrar en "Archivos de programa" para todo el mundo, y el registro puede tener un número de entradas para asociar PILAR a ficheros con extensión .mgr.

Cuando Java esté instalado…

- ejecute `pilar_<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
  `pilar.exe`
  donde haya decidido instalar el software.

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

3.3. PILAR (UNIX)

Cuando Java esté instalado…

- ejecute `pilar_linux_<version>_<lang>.jar`
  e instale la aplicación y la librería en donde considere apropiado
  (varios idiomas pueden compartir el mismo directorio de instalación)
- cuando la instalación termine, habrá un archivo
  `pilar.jar`
  donde haya decidido instalar el software.

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

3.4. PILAR (MAC OS X)

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

- ejecute `pilar_mac_<version>_<lang>.jar`
  e instale la aplicación y la librería en donde considere apropiado
  (varios idiomas pueden compartir el mismo directorio de instalación)
- al terminar la instalación, debe encontrar un fichero
  `pilar.app`

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

3.5. USO

Ejecute `pilar`:

- le pedirá un fichero configuración:
  STIC_es.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".

3.6. 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.

STIC_ens.car

Se recomienda estudiar el documento "Personalización" en la documentación de PILAR. [http://www.pilar-tools.com/es/tools/pilar/doc.htm]

3.7. 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,

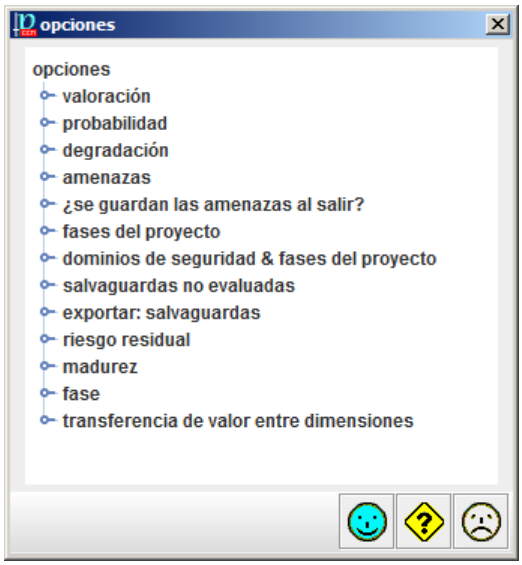
PILAR / bib_es / info_es.info

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

<!—
 pares clave-valor para projectos. 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>
```

4. EDITAR / OPCIONES

El comportamiento de PILAR puede ser ajustado con varias opciones:



- *Opciones / Valoración*
- *Opciones / Probabilidad*
- *Opciones / Degradación*
- *Opciones / Amenazas*
- *Opciones / Guardar*
- *Opciones / Fases del proyecto*
- *Opciones / Dominios y fases*
- *Opciones / Salvaguardas no evaluadas*
- *Opciones / Exportar: salvaguardas*
- *Opciones / Riesgo residual*
- *Opciones / Madurez*
- *Opciones / Fases especiales*
- *Opciones / Transferencia de valor entre dimensiones*

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.

4.1. 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.

4.2. 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

4.3. OPCIONES / DEGRADACIÓN

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%

4.4. 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

4.5. 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.

4.6. OPCIONES / FASES DEL PROYECTO

Cómo se relacionan unas fases con otras.

fases del proyecto / conectadas

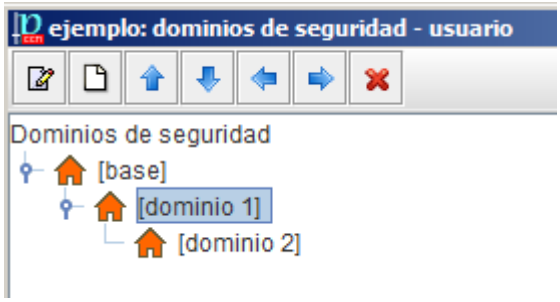
si una salvaguarda no está evaluada en una fase, hereda el valor de la fase anterior

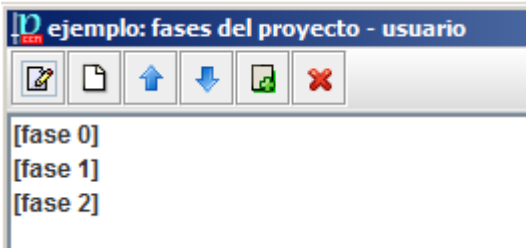
fases del proyecto / independientes

cada fase es independiente, sin heredar nada de otras fases

4.7. 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	7°	4°	**1°**	**3°**	**2°**	**1°**
dominio 1	8°	5°	**2°**	6°	5°	4°
base	9º	6°	**3º**	9°	8°	7°

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	7°	4°	**1°**	**3°**	**2°**	**1°**
dominio 1	8°	5°	**2°**	6°	5°	4°
base	9º	6°	**3º**	9°	8°	7°

4.8. OPCIONES / SALVAGUARDAS NO EVALUADAS

Si una salvaguarda no está evaluada, PILAR usa el valor determinado por esta opción

salvaguardas no evaluadas / ignorar (= n.a.)

es como si la salvaguarda fuera irrelevante en este dominio

salvaguardas no evaluadas / inexistente (= L0)

es como si la salvaguarda fuera necesaria, pero no existe (este es el comportamiento de PILAR en versiones anteriores a 4.4)

4.9. 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)

sólo imprime los valores explícitos

4.10. 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.

4.11. 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

4.12. 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, ENS. Estas fases no se pueden editar; usted simplemente puede verlas y usarlas como sugerencia de la madurez adecuada para cada salvaguarda.

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

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

5. INFORMES

5.1. 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]

5.2. 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 (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.

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.

Normativa de seguridad

El informe muestra la madurez de las normas *(security policies)* de seguridad fase por fase.

Procedimientos de seguridad

El informe muestra la madurez de los procedimientos de seguridad fase por fase.

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

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

Protecciones adicionales

Se presenta la evaluación de las protecciones adicionales para ciertas clases de activos.

5.3. 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. Sólo 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. Sólo 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. Sólo 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. Sólo 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 sólo está disponible en análisis cuantitativo.

5.4. BASES DE DATOS

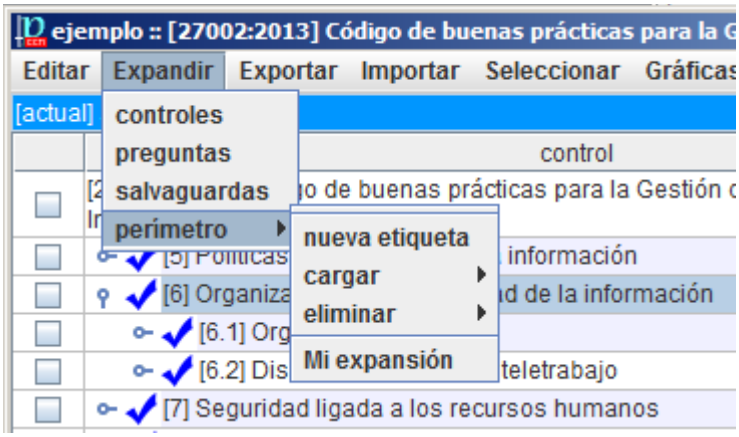
La información para usar PILAR con bases de datos está disponible en

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

6. 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`

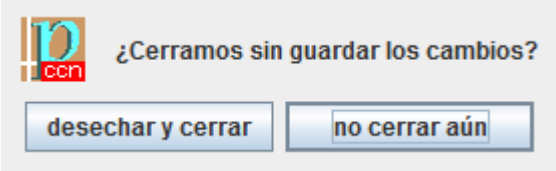
Pantallas

7. ACEPTAR, CANCELAR, AYUDA

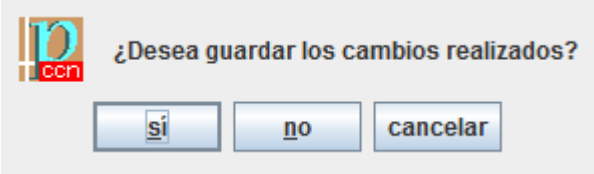
La mayoría de las pantallas incluyen los siguientes botones:

	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
Sí	se guardan los cambios y se cierra la ventana

8. PRIMERA PANTALLA

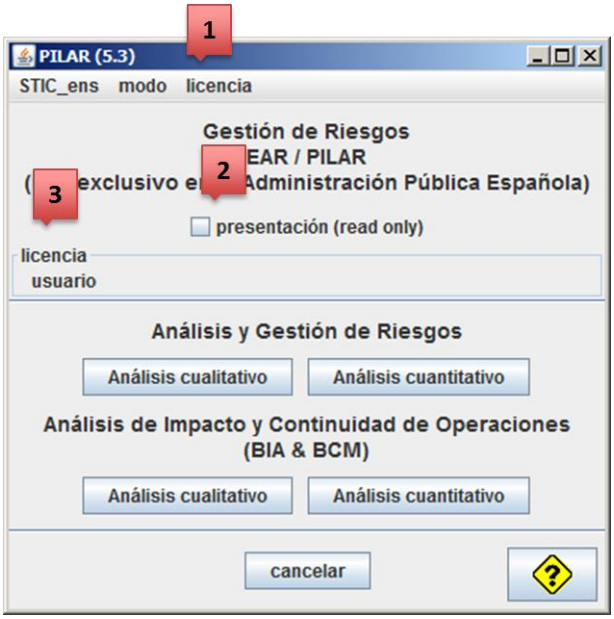
Para empezar rápidamente
Para ver un análisis de riesgos (sólo lectura): • **modo / presentación** • **análisis cualitativo [3]** Para trabajar en un proyecto nuevo o ya existente: • **modo / trabajo** • vaya al directorio donde guardó la licencia (fichero .lic) y selecciónela • **análisis cualitativo**

8.1. 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.
4	Inicia un análisis cuantitativo: confidencialidad, integridad, disponibilidad, etc.
5	Inicia un análisis cualitativo: interrupción y recuperación del servicio. Ver "Continuidad de operaciones" en [http://www.pilar-tools.com/es/tools/pilar/doc.htm]

6	Inicia un análisis cuantitativo: interrupción y recuperación del servicio. Ver “Continuidad de operaciones” en [http://www.pilar-tools.com/es/tools/pilar/doc.htm]
7	Cancelar
8	Ayuda en línea

8.2. 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.

9. PANEL DE CONTROL

9.1. CONTROLES BÁSICOS

1	Ver *Menú proyecto*
2	Ver *Menú fichero*
3	Sólo si la licencia incluye acceso a bases de datos SQL. Las tablas de la base de datos se describen en otro documento Ver [http://www.pilar-tools.com/es/tools/pilar/doc.htm]
4	**Preferencias:** tipo y tamaño de letra. **Opciones:** Ver *Editar / Opciones*
5	Ver *Menú nivel*
6	Ver *Menú ayuda*
	Crea un nuevo proyecto, vacío.
	Selecciona un proyecto de un fichero (.mgr)
	Selecciona un proyecto de una base de datos. Sólo si la licencia incluye acceso a bases de datos SQL.
	Guarda el proyecto en su fichero o en su base de datos.

9.1.1. MENÚ PROYECTO

1 **Menú 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 [http://www.pilar-tools.com/es/tools/pilar/doc.htm]
Exportar (xml)	Exporta datos en formato XML Ver [http://www.pilar-tools.com/es/tools/pilar/doc.htm]
Guardar y cerrar	Guarda el proyecto y termina
Cancelar y cerrar	Termina sin guardar los datos

9.1.2. MENÚ FICHERO

2	**Menú fichero**
Abrir	Abre un proyecto guardado en un fichero (.mgr)
Importar	Importa los datos de otros proyecto sobre este
Integrar	Combina este proyecto con datos de otro proyecto
Diferencias	δ Compara un proyecto con otro resaltando los cambios (experimental)
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

Ver "*importar o integrar*".

9.1.3. MENÚ BASE DE DATOS

3	**Menú base de datos**
Abrir	Abre un proyecto guardado en una base de datos
Importar	Importa los datos de otros proyecto sobre este

Integrar	Combina este proyecto con datos de otro proyecto
Diferencias	δ Compara un proyecto con otro resaltando los cambios (experimental)
Guarda como ...	Guarda una copia. Se puede elegir la base de datos

Ver "*importar o integrar*".

9.1.4. IMPORTAR O INTEGRAR

Cuando se importa un proyecto P2 sobre el proyecto P1, los datos de P2 sobrescriben los de P1. Cuando se integra, los datos de P2 se combinan con los de P1. En ambos casos, cuando P2 no especifica algo (lo deja en blanco), se retienen los datos de P1.

tipo de valor	**importar**	**integrar**
nuevo dominio de seguridad	• se añade	• se añade
dominios en P1 & P2 • fuentes de información • factores	 • se añade • se añade	 • se añade • se añade
nuevo activo	• se añade	• se añade
activos en P1 & P2 • clases • fuentes de información • dependencias • valores • criterios	 • se añade • se añade • se añade • se remplaza • se remplaza	 • se añade • se añade • se añade • valor máximo • se añade
nueva amenaza	• se añade	• se añade
amenazas en P1 & P2 • valoración	 • se remplaza	 • se añade
nueva fase	• se añade	• se añade
fases en P1 & P2 • fuentes de información	 • se añade	 • se añade
salvaguardas • aplicabilidad • dudas • comentarios • fuentes de información • madurez • específicas de activo	 • se remplaza • se añade • se remplaza • se añade • se remplaza • se remplaza	 • $na = na_1$ & na_2 • se añade • se añade • se añade • valor máximo • $na = na_1$ & na_2
protecciones adicionales	como las salvaguardas	como las salvaguardas
perfiles de seguridad	como las salvaguardas	como las salvaguardas

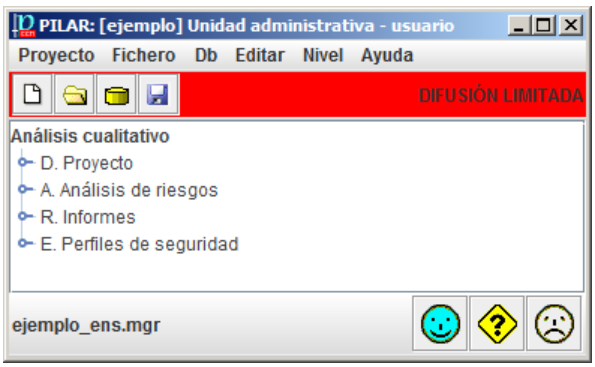
9.1.5. MENÚ NIVEL

5	**Menú nivel** Controla cuántas opciones se le ofrecen al usuario
Basico	Sólo se presentan las opciones básicas. Menús sencillos. Para principiantes.
Medio	Punto medio entre básico y experto
Experto	Se presentan todas las opciones

9.1.6. MENÚ AYUDA

6	**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

9.2. CONTROLES DEL PROYECTO



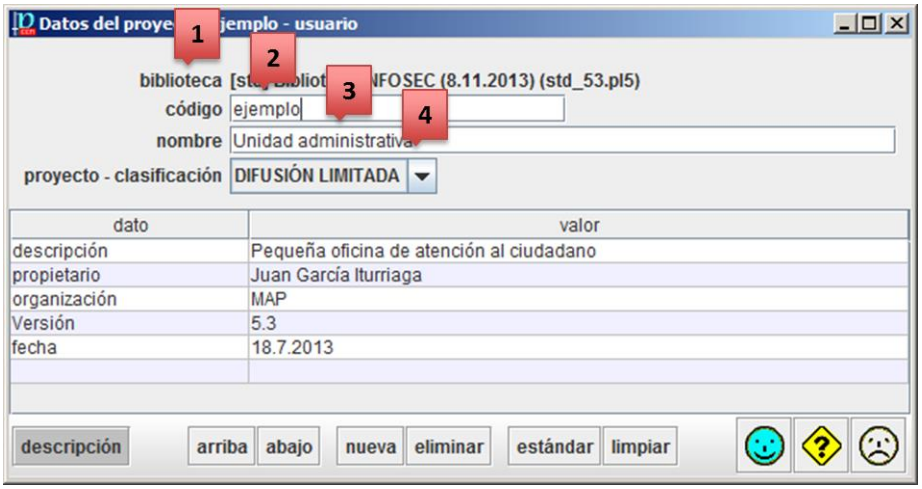
La barra inferior presenta el nombre del fichero, o el URL de la base de datos.

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

10. PROYECTO

10.1. 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.



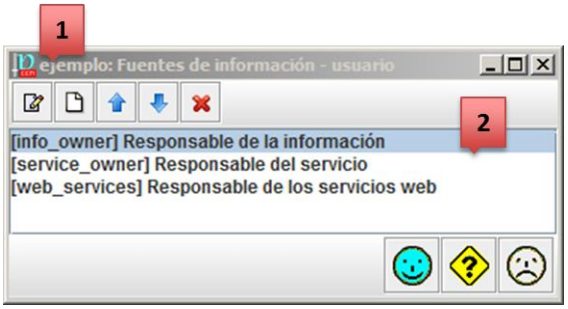
1	La biblioteca. Se selecciona al arrancar. Ver "*Fichero de configuración*".
2	Código del proyecto. Debería ser único.
3	El nombre del proyecto. Una descripción sucinta.
4	La marca de clasificación, por defecto, de los informes.

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.

10.2. FUENTES DE INFORMACIÓN

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



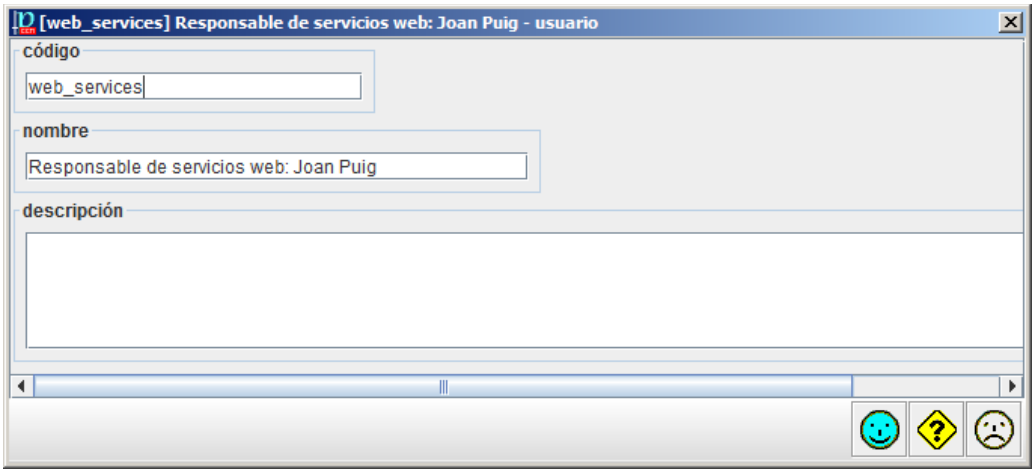
1	operaciones sobre las fuentes de información
	editar: seleccione una fuente en [2] y haga clic para pasar a modo edición
	nueva: seleccione una fuente en [2] y haga clic para crear una nueva fuente
	subir: seleccione una fuente en [2] y haga clic para subirla en la lista también: MAYÚSCULAS + FLECHA_ARRIBA
	bajar: seleccione una fuente en [2] y haga clic para bajarla en la lista también: MAYÚSCULAS + FLECHA_ABAJO
	eliminar: seleccione una fuente en [2] y haga clic para eliminarla también: SUPR
2	panel con la lista de fuentes de información declaradas seleccione y haga clic-clic para editarla

10.2.1. EDICIÓN

Cuando esté editando una fuente de información, puede especificar:

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

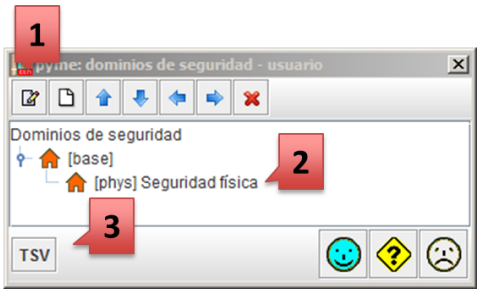
La descripción puede incluir hiperenlaces (URLs). Para ir a la página enlazada, CLIC con el botón derecho, y después



10.3. 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

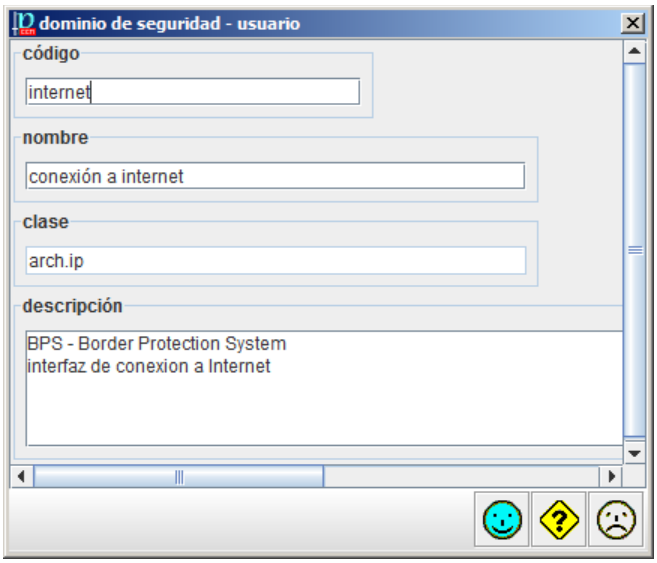
	seleccione un dominio en [2] y haga clic para moverlo hacia la derecha también: MAYÚSCULAS + FLECHA_DERECHA
	seleccione un dominio en [2] y haga clic para eliminarlo también: DELETE
2	panel con la jerarquía de dominios seleccione y haga clic-clic para editar un dominio haga clic en la manivela para expandir o colapsar el árbol
3	para cargar perfiles de amenazas Ver "*Threat Standard Values*

10.3.1. 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
  - arch.ip – punto de interconexión, perfil IP (CCN-STIC 811)
- una descripción más extensa

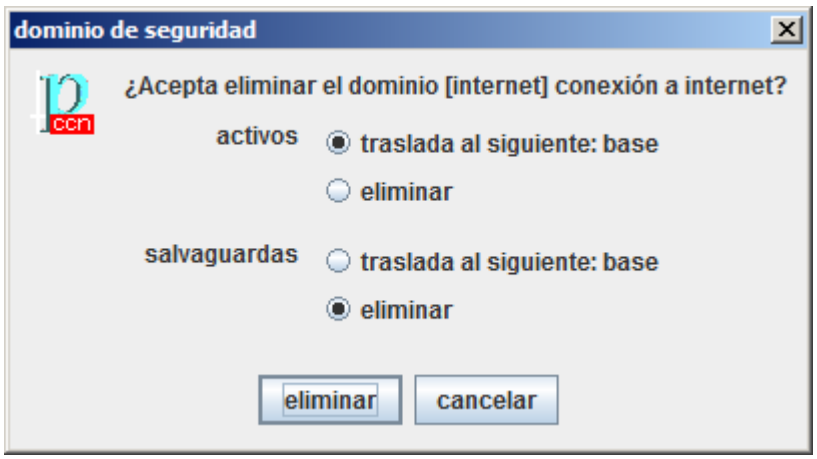
La descripción puede incluir hiperenlaces (URLs). Para ir a la página enlazada, haga clic con el botón derecho y después



10.3.2. 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:

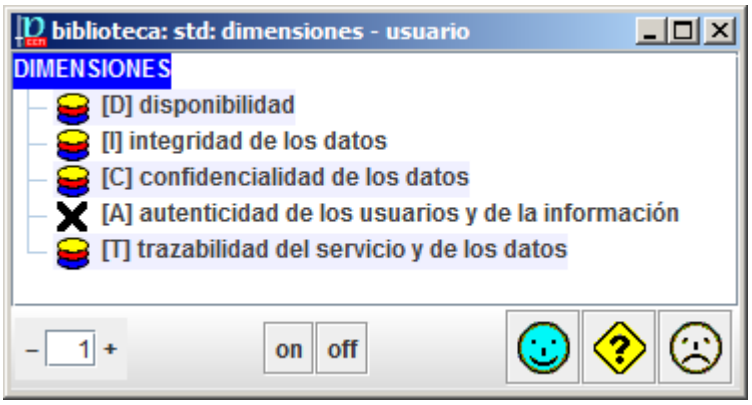


10.4. SUBCONJUNTO DE DIMENSIONES

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 usted puede centrarse en el "asunto del día" eliminando información innecesaria de las pantallas.

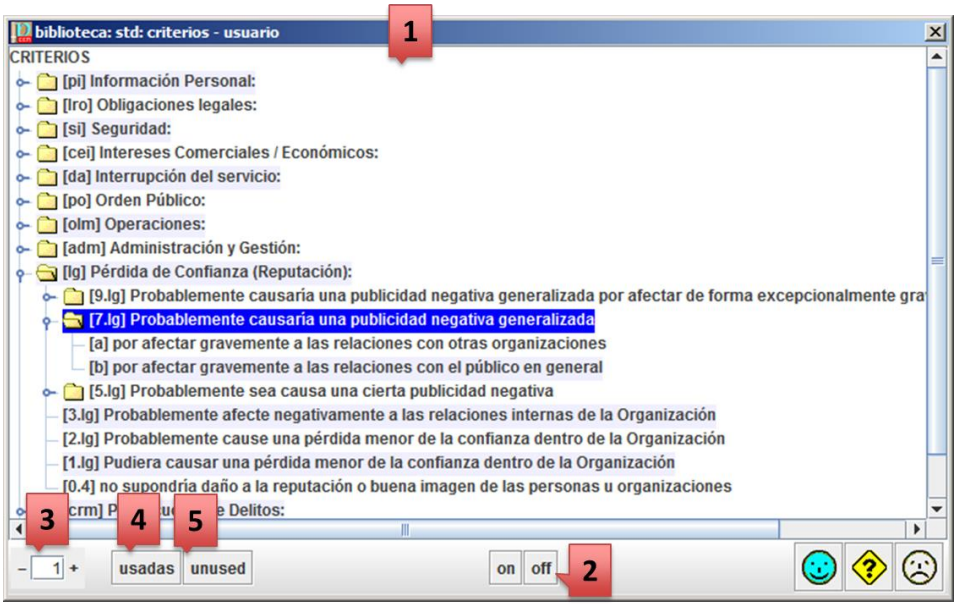


10.5. SUBCONJUNTO DE CRITERIOS DE VALORACIÓN

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

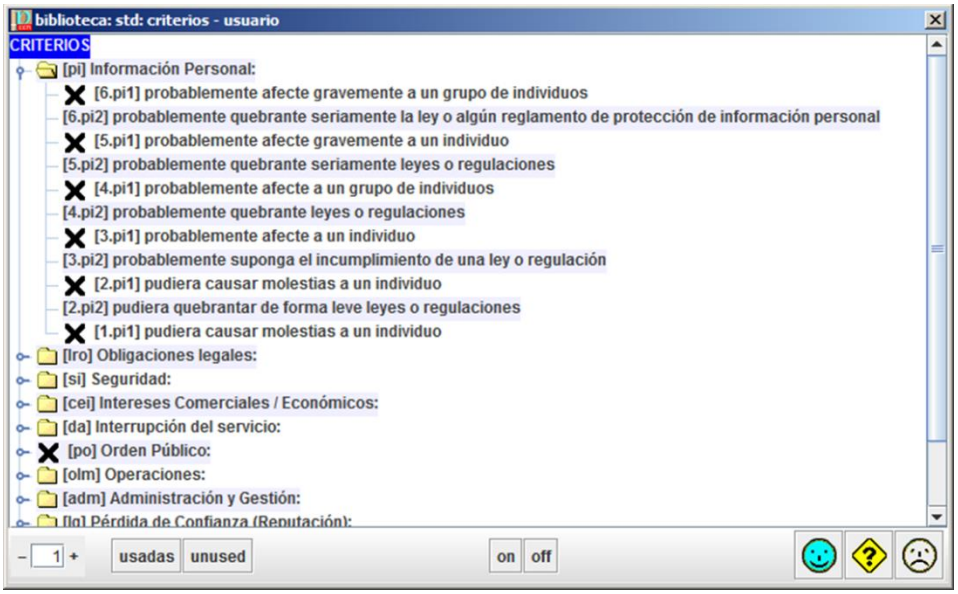
Sin embargo, se puede renunciar a algunos criterios, si no los considera apropiados para su Organización. Seleccione el criterio o grupo de criterios, y use los botones ON / OFF al pie.

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



1	Árbol con los criterios disponibles.
2	Haga clic para activar / desactivar un criterio o un grupo.
- 1 +	Seleccione el nivel de despliegue del árbol.
4	Selecciona aquellos criterios que se utilizan actualmente en el proyecto de análisis de riesgos.
5	Selecciona aquellos criterios que no se utilizan actualmente en el proyecto de análisis de riesgos.

Después de eliminar algunos criterios:



10.6. CUANTIFICACIÓN DEL VALOR

Esta pantalla se ha eliminado en la versión 5.4. Se empleará un fichero de configuración al arrancar PILAR. De esta forma se pueden establecer unos criterios uniformes para toda la organización.

Ver “Personalización” en la documentación de PILAR.

PILAR permite el asociar niveles cualitativos a valores cuantitativos. Esta asociación trabaja solamente si el usuario no proporciona información explícita para ambos.

En un análisis cualitativo, cuando varios servicios dependen de un solo equipo, el nivel acumulado en el equipo compartido es el máximo de los niveles requeridos por los activos soportados. Se pierde información cuando muchos servicios dependen de un punto compartido de fallo. El análisis cuantitativo muestra esta acumulación porque simplemente suma los valores individuales.

En análisis cuantitativo, cuando un servidor con un servicio altamente cualificado se compara a otro servidor con varios servicios cualificados más bajos, la adición de muchos valores pequeños puede alcanzar un alto valor, y el usuario puede verse tentado a proteger la cantidad antes que la calidad. El análisis cualitativo muestra la diferencia al quedarse con el nivel más alto.

El mismo modelo preparado con pilar, puede abrirse en modo cualitativo o cuantitativo; basta elegir la opción deseada al arrancar PILAR. PILAR, abierto en modo cualitativo, utiliza valores cualitativo, bien los que se hayan introducido directamente, bien valores estimados a partir de la valoración cuantitativa. Igualmente, PILAR abierto en modo cuantitativo, trabaja con cantidades numérica, bien las que se hayan introducido directamente, bien valores derivados a partir de los niveles cualitativos.

Paso de niveles cualitativos a valores cuantitativos

Se utiliza cuando el usuario proporciona solamente niveles cualitativos. PILAR puede realizar un análisis cuantitativo ficticio donde el impacto de muchos servicios en un solo equipo queda realzado. De esta forma puede ser informativo ejecutar un modelo cualitativo en términos cuantitativos.

Paso de valores cuantitativos a niveles cualitativos

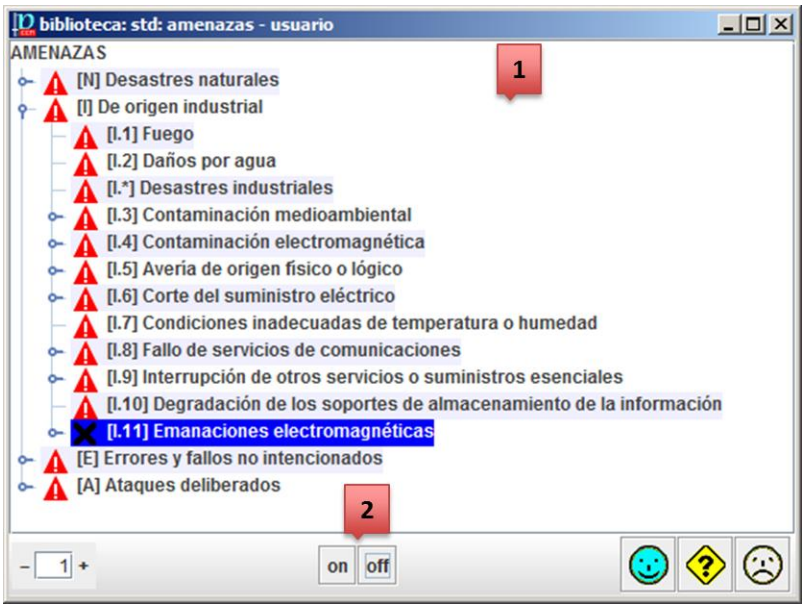
Se utiliza cuando el usuario proporciona solamente la valoración cuantitativa. PILAR puede realizar un análisis cualitativo donde el impacto de un servicio altamente valorado queda realzado. De esta forma puede ser informativo ejecutar un modelo cuantitativo en términos cualitativos.

10.7. SUBCONJUNTO DE AMENAZAS

La biblioteca estándar establece las amenazas disponibles.

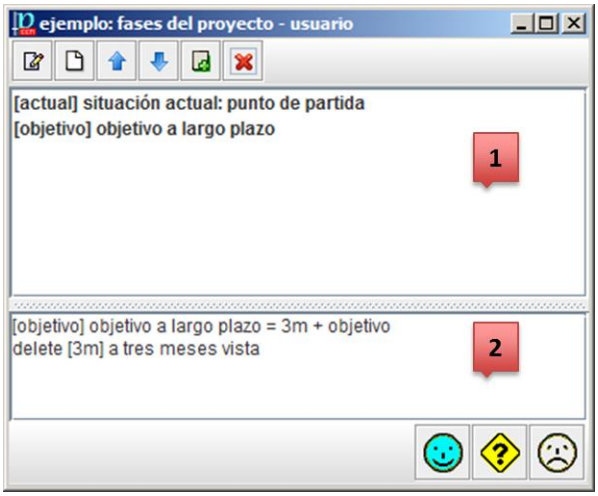
Sin embargo, se puede renunciar a algunas amenazas. Seleccione la amenaza o el grupo de amenazas, y use los botones ON / OFF al pie.

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



1	Árbol con todas las amenazas
2	Haga clic para seleccionar / deseleccionar una amenaza o un grupo de amenazas.
– 1 +	Para seleccionar el nivel de despliegue del árbol.

10.8. FASES DEL PROYECTO



	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 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
1	Una lista ordenada de fases de evaluación.
2	PILAR no ejecuta las acciones inmediatamente, sino que prepara una lista de acciones a realizar. Se hará todo, en el orden indicado, al cerrar la ventana.

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

10.8.1. 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	

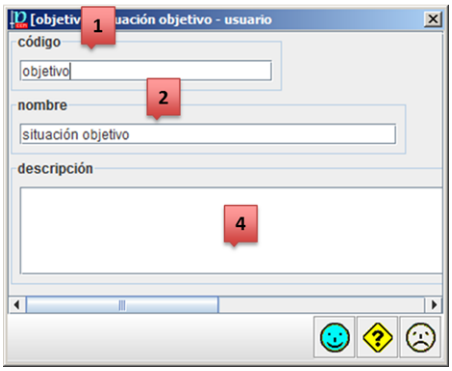
Si combinamos las fases F2 + F3, los valores de la fase F2 no modificados en la fase F3 se copian en la fase F3:

	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	

10.8.2. EDITAR UNA FASE



1	el código; debe ser único
2	el nombre: una descripción sucinta
4	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

11. ANÁLISIS DE RIESGOS

11.1. 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

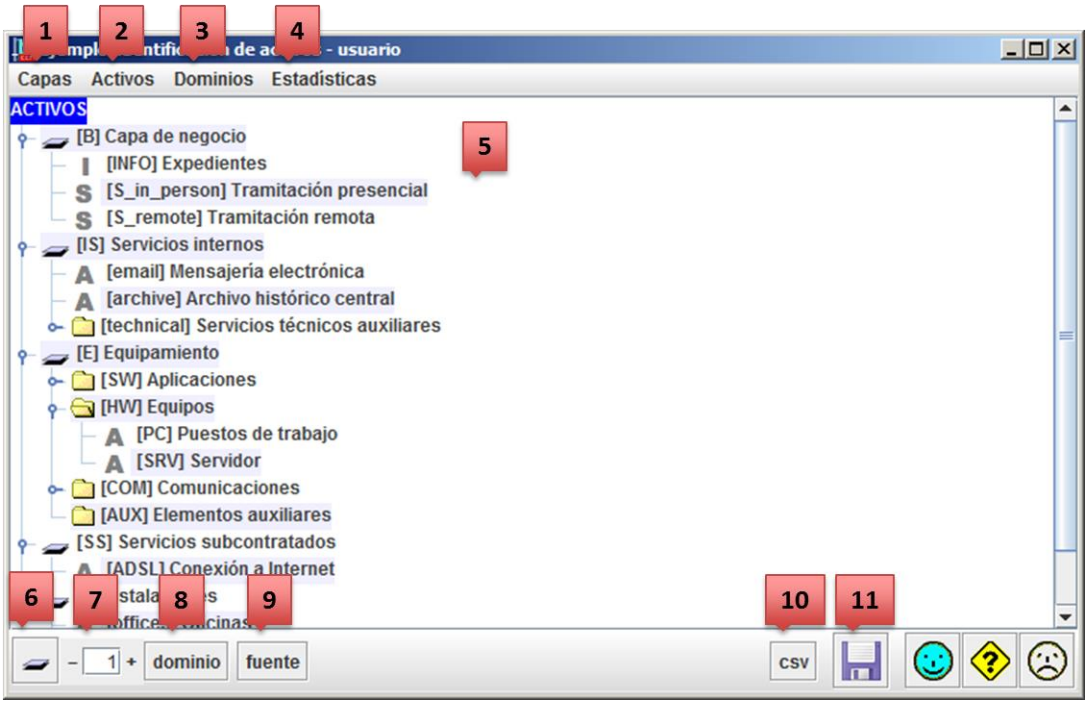
Estos son esenciales para el análisis de riesgos: los activos de verdad.

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	- 1 +	Para seleccionar el nivel de expansión del árbol.
8	dominio	Haga clic y seleccione un dominio. PILAR selecciona los activos en dicho dominio.
9	fuente	Haga clic y seleccione una fuente de información. PILAR selecciona los activos asociados a dicha fuente.
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.

11.1.1. 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

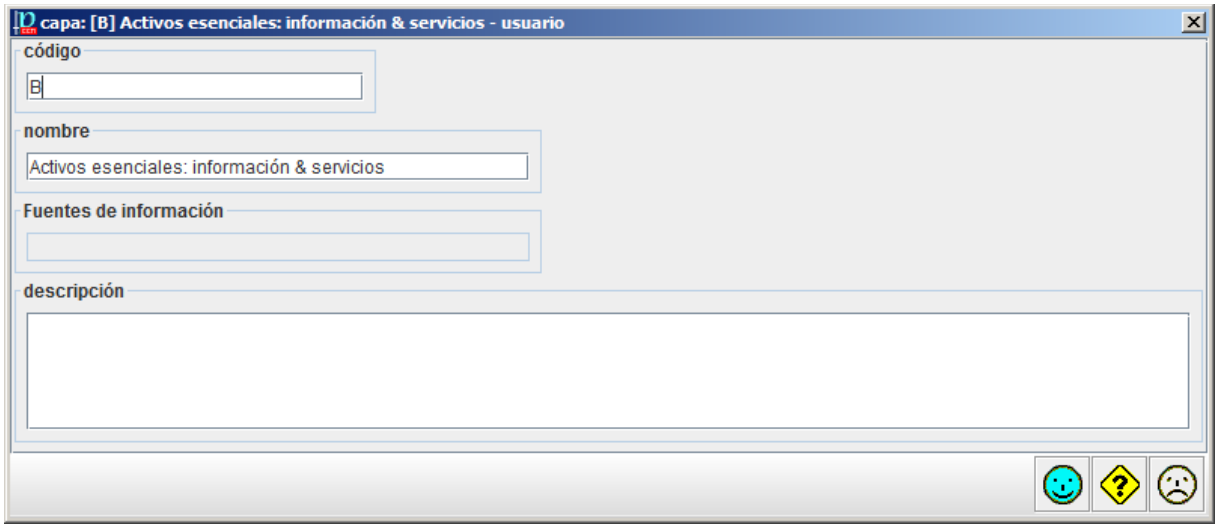
o

- 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.
- 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

11.1.2. MENÚ ACTIVOS

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*".
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	Elimina los hijos de los activos seleccionados.

/ los hijos	
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

11.1.3. 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 / …

11.1.4. 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 / …

11.1.5. 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 / …

11.1.6. 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 / …

11.1.7. MENÚ ESTADÍSTICAS

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

por capas

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	0	1	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

OK

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.

11.1.8. 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

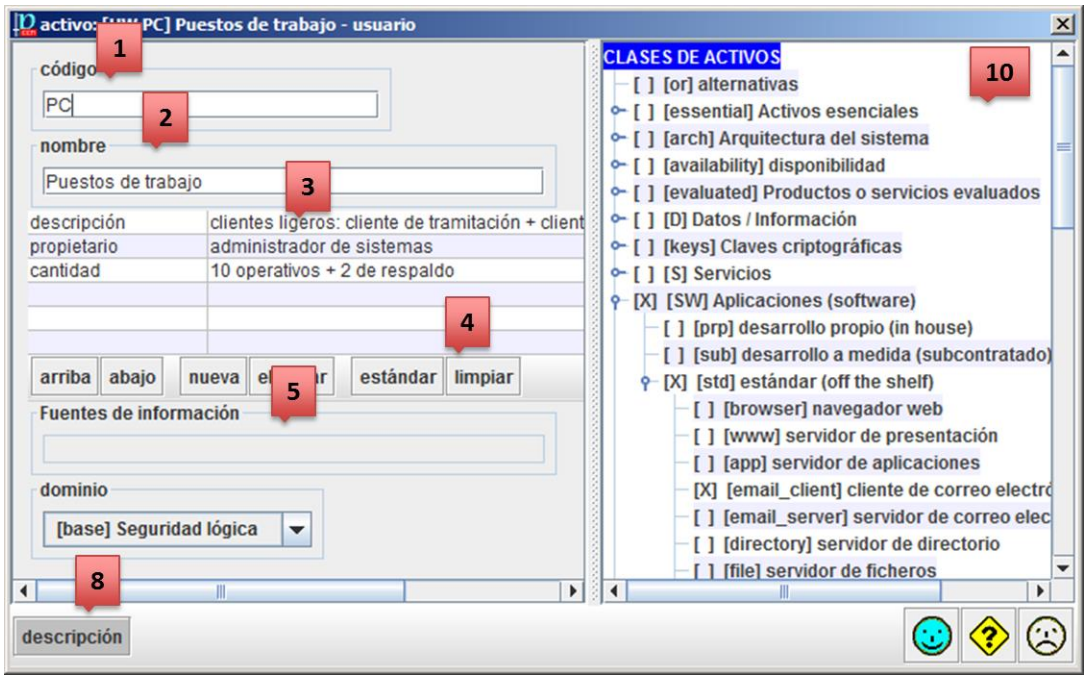
— marcar y dejar caer (drag & drop)

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

11.2. 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

5	Haga clic para asociar un activo a una o más fuentes de información.
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)

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

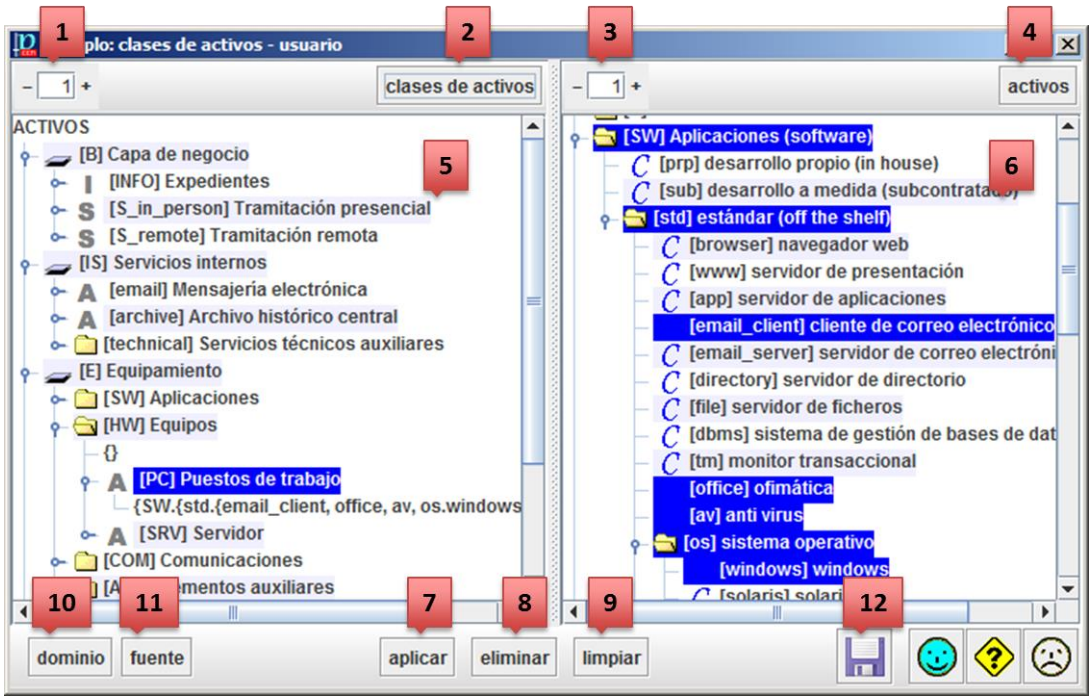
- [X] [keys] claves criptográfi...
  - [X] [info] protección de la Informaci...
    - [X] [encrypt] encryption k...
      - [X] [shared_secret] secreto compartido (clave simétri...
      - [ ] [public_encryption] cifrado con clave pública
      - [ ] [public_decryption] descifrado con clave pública
    - [X] [sign] claves de fir...
      - [ ] [public_signature] firma con clave pública
      - [ ] [public_verification] verificación de firma con clave pública
      - [ ] [shared_secret] secreto compartido (clave simétrica)
  - [ ] [com] Comunicaciones
  - [X] [disk] cifrado de dis...
    - [ ] [encrypt] claves de cifra
  - [ ] [x509] Cerificado X.509

clic derecho + LIMPIAR	clic derecho + ELIMINAR
[-] [keys] claves criptográfi... [-] [info] protección de la Informac... [-] [encrypt] encryption k... [X] [shared_secret] secreto compartido (clave simétri... [ ] [public_encryption] cifrado con clave pública [ ] [public_decryption] descifrado con clave pública [X] [sign] claves de fir... [ ] [public_signature] firma con clave pública [ ] [public_verification] verificación de firma con clave p [ ] [shared_secret] secreto compartido (clave simétrica [ ] [com] Comunicaciones [X] [disk] cifrado de dis... [ ] [encrypt] claves de cifra [ ] [x509] Cerificado X.509	[ ] [keys] claves criptográficas [ ] [info] protección de la Información [ ] [encrypt] encryption keys [ ] [shared_secret] secreto compartido (clave simétrica) [ ] [public_encryption] cifrado con clave pública [ ] [public_decryption] descifrado con clave pública [ ] [sign] claves de firma [ ] [public_signature] firma con clave pública [ ] [public_verification] verificación de firma con clave p [ ] [shared_secret] secreto compartido (clave simétrica) [ ] [com] Comunicaciones [ ] [disk] cifrado de discos [ ] [encrypt] claves de cifra [ ] [x509] Cerificado X.509

11.3. 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.



1	Controla el nivel de despliegue del árbol de activos (izquierda).
2	— Seleccione uno o más activos en [5]. — Haga clic en CLASES DE ACTIVOS. PILAR seleccionará las clases asociadas en [6].

3	Controla el nivel de despliegue del árbol de clases (derecha).
4	— Seleccione una o más clases en [6]. — Haga clic en ACTIVOS. PILAR seleccionará los activos asociados en [5].
5	Los activos y las clases que tienen asociadas
6	Las clases de activos.
7	— Seleccione uno o más activos en [5]. — Seleccione una o más clases en [6]. — Haga clic en APLICAR y quedarán asociados.
8	— Seleccione uno o más activos en [5]. — Seleccione una o más clases en [6]. — Haga clic en ELIMINAR y quedarán disociados.
9	— Seleccione uno o más activos en [5]. — Haga clic en LIMPIAR y quedarán sin clases.
10	— Selecciona los activos en [5] que pertenecen a un cierto dominio
11	— Selecciona los activos en [5] asociados a una cierta fuente
12	Guarda el proyecto en su fichero o en su base de datos.

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 sólo 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

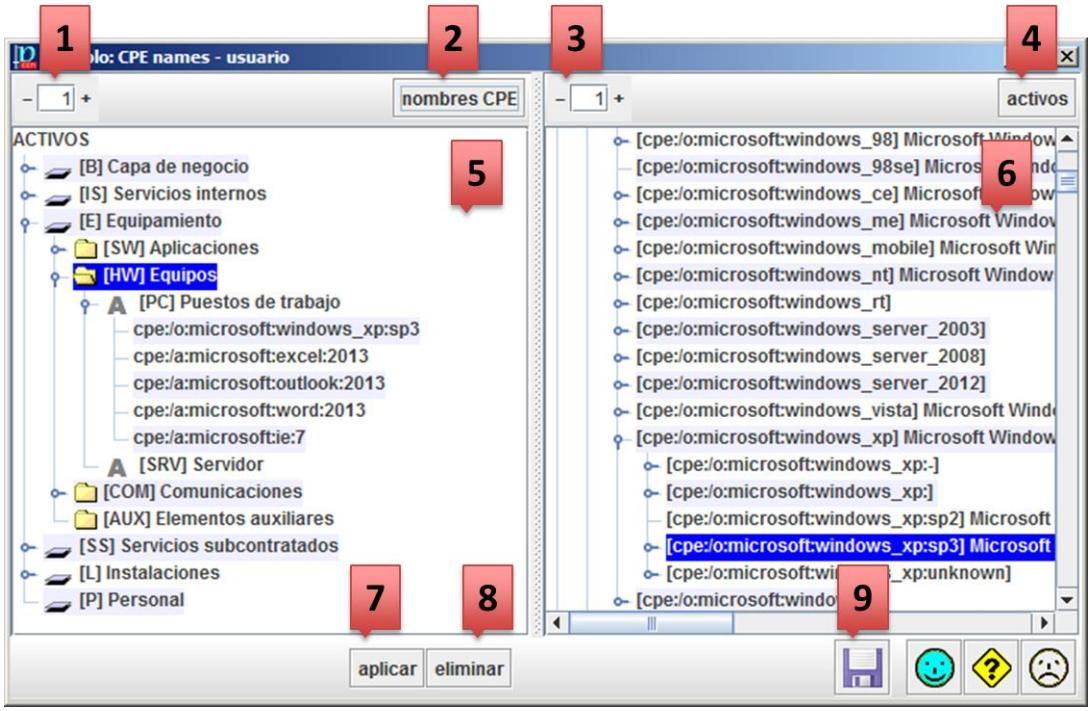
11.4. ACTIVOS / NOMBRES CPE

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

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

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

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



1	Controla el nivel de despliegue del árbol de activos [5].

2	Seleccione uno o más activos a la izquierda. Haga clic en NOMBRES CPE y PILAR seleccionará a la derecha los nombres asociados.
3	Controla el nivel de despliegue del árbol de nombres CPE [6].
4	Seleccione uno o más nombres a la derecha. Haga clic en ACTIVOS y PILAR seleccionará a la izquierda los activos asociados.
5	Los activos y los nombres CPE que tienen asociados.
6	Los nombres CPE
7	Seleccione uno o más activos a la izquierda. Seleccione uno o más activos a la derecha. Haga clic en APLICAR para asociarlos.
8	Seleccione uno o más activos a la izquierda. Seleccione uno o más activos a la derecha. Haga clic en ELIMINAR para disociarlos.
9	Guarda el proyecto en su fichero o en su base de datos.

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

11.5. 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).

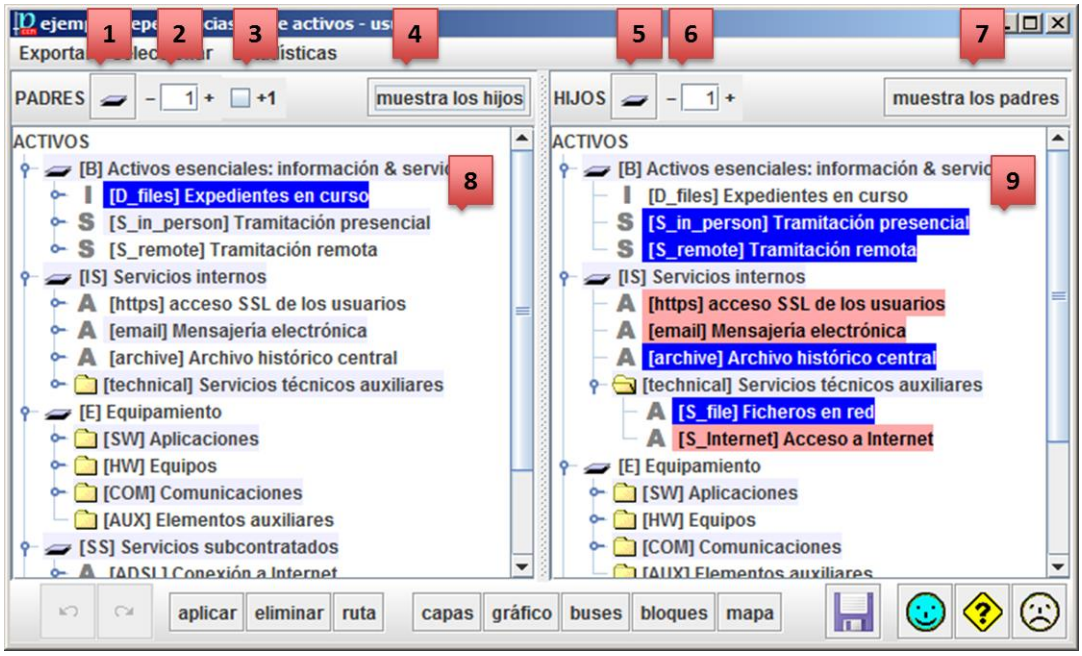
El sistema de información puede valorarse por dominios o activo por activo. Se elige en *Opciones / Valoración*

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

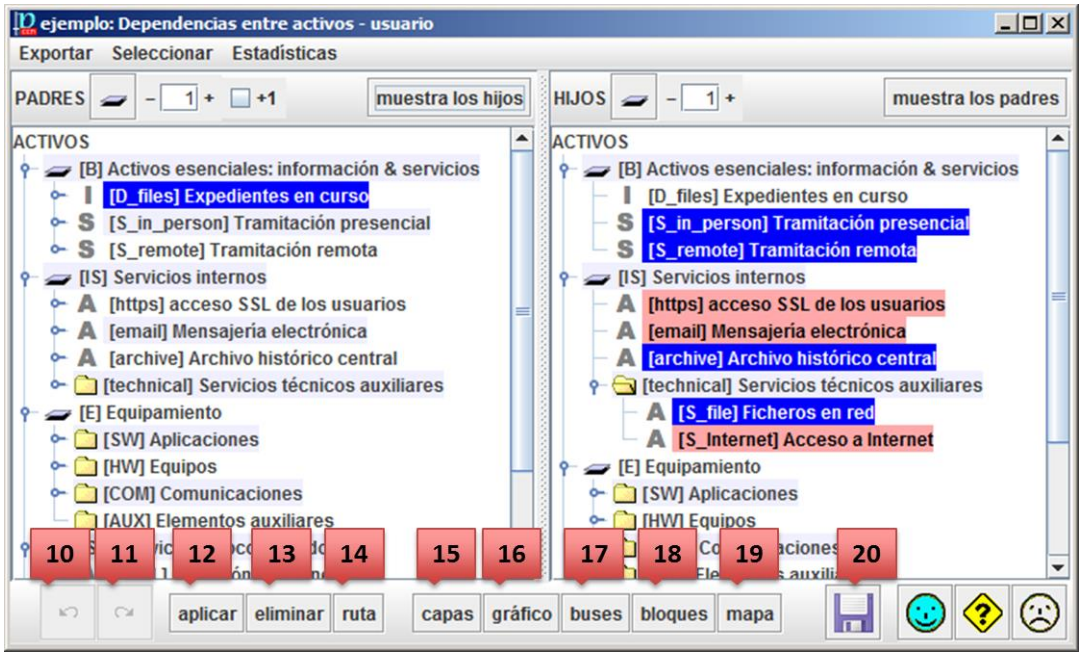
Si está usted valorando activo por activo, entonces debe establecer las dependencias y luego pasar a *Valoración por activos*

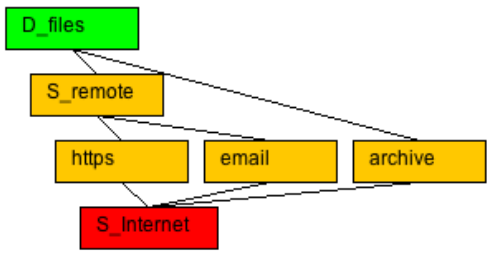
Para empezar rápidamente
Si ha identificado las instalaciones …
• asocie cada equipo a la instalación donde se encuentra
Si ha identificado servicios y equipos …
• asocie cada servicio al equipamiento que utiliza: software, hardware, comunicaciones, medios,…
Si ha identificado personal …
• asocie cada persona a los servicios o al equipo sobre el 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).



1		Haga clic para colapsar el árbol izquierdo.
2	- 1 +	Controla el nivel de expansión del árbol izquierdo. Si está seleccionado [+1], se muestran también los activos de los que depende.
3	+1	Controla si el árbol de activos (izquierdo) incluye las dependencias.
4	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.
5		Haga clic para colapsar el árbol derecho.
6	- 1 +	Control the level of expansion of the right tree.
7	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.
8		Grafo de dependencias mostrado como árbol.
9		Árbol de activos.



10		Deshace el último APILAR o ELIMINAR.
11		Rehace el último APLICAR o ELIMINAR deshecho.
12	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.
13	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.
14	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). 
15	capas	Abre una ventana con tantas cajitas como capas, mostrando las dependencias entre activos de cada capa. Ver "*Activos / Dependencias / Capas*".
16	gráfico	Abre una ventana con tantas cajitas como activos, mostrando las dependencias entre ellos. Ver "*Activos / Dependencias / Grafo*".
17	buses	Abre una ventana con tantas cajitas como activos, mostrando las dependencias entre ellos. Ver "*Activos / Dependencias / Buses*".
18	bloques	Abre una ventana con tantas cajitas como activos, mostrando las dependencias entre activos de cada capa. Ver "*Activos / Dependencias / Bloques*".
19	mapa	Abre una ventana con tantas cajitas como activos, mostrando las dependencias entre ellos. Ver "*Activos / Dependencias / Mapa*".
20		Guarda el proyecto en su fichero o en su base de datos.

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%.

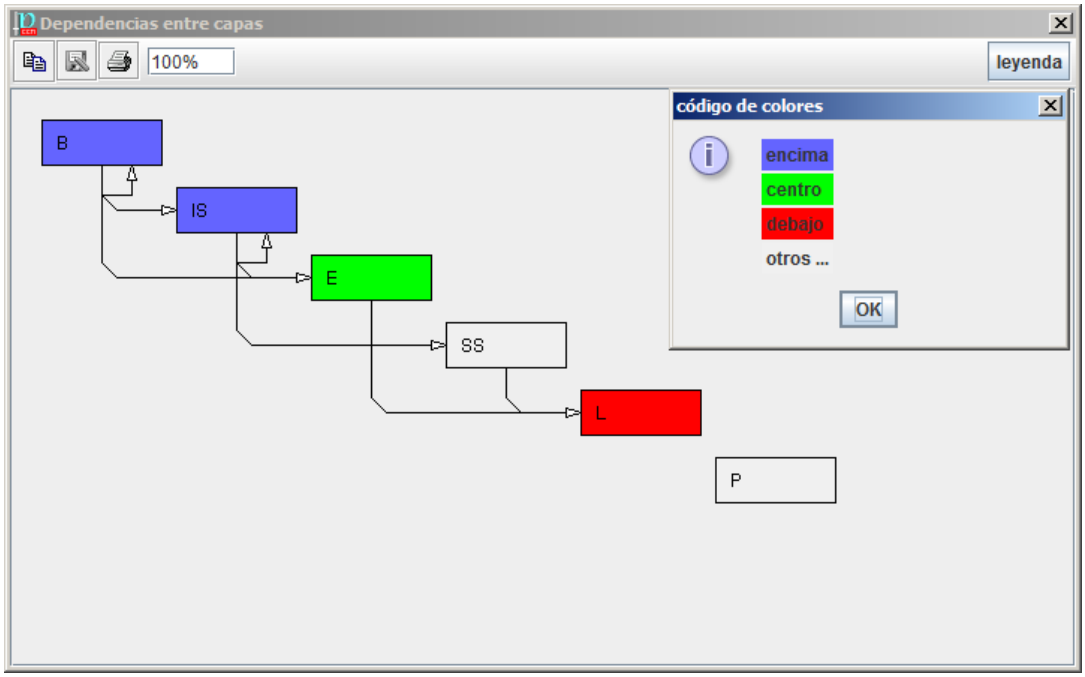
Para fijar un grado entre el 0% y el 100%:

- 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

11.5.1. 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

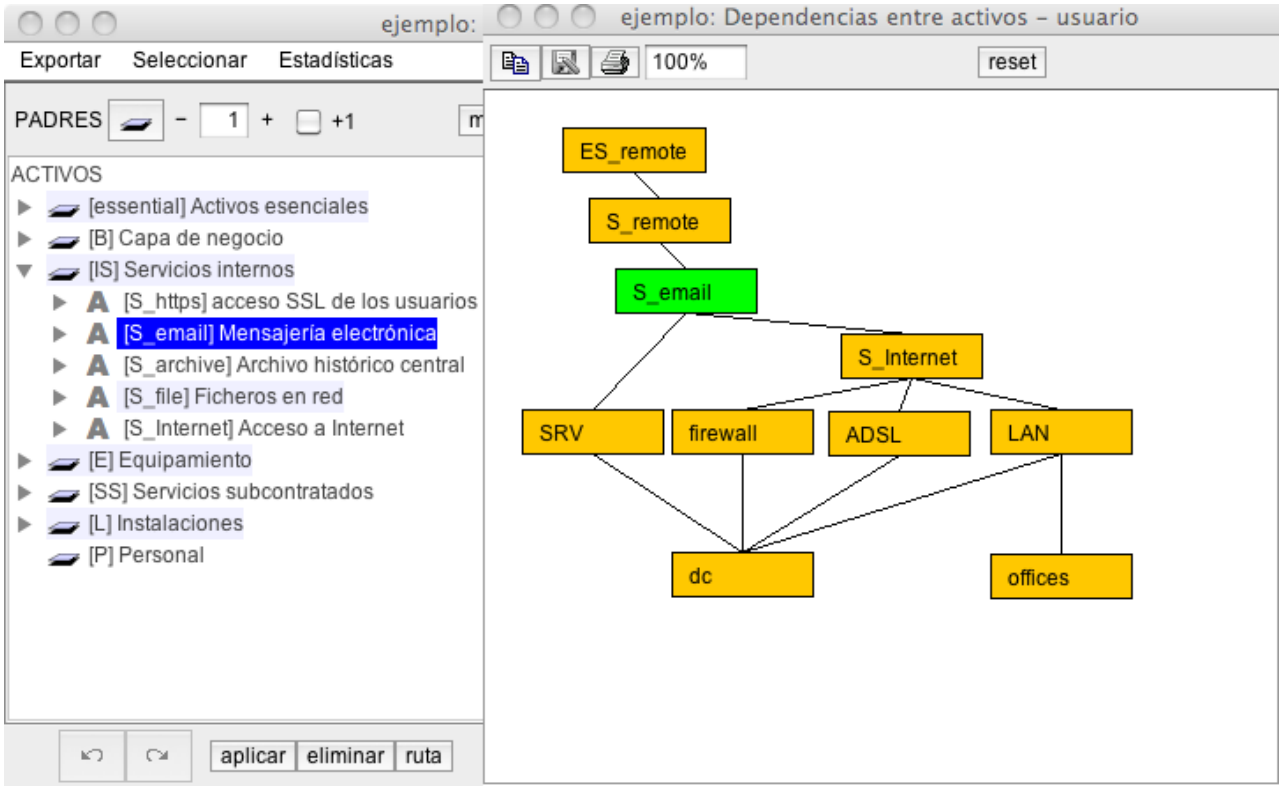
	imprimir	para enviar el gráfico a una impresora
100%	**escala**	para cambiar el tamaño de la imagen
	leyenda	muestra el código de colores

11.5.2. GRAFO DE DEPENDENCIAS ENTRE ACTIVOS

El gráfico muestra las relaciones de dependencia entre activos. Sólo 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.).

El gráfico sigue la selección en la pantalla principal de dependencias. Así pues, si selecciona un activo, un grupo o una capa, sólo 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
100%	**escala**	para cambiar el tamaño de la imagen
	reset	reposiciona las cajas heurísticamente

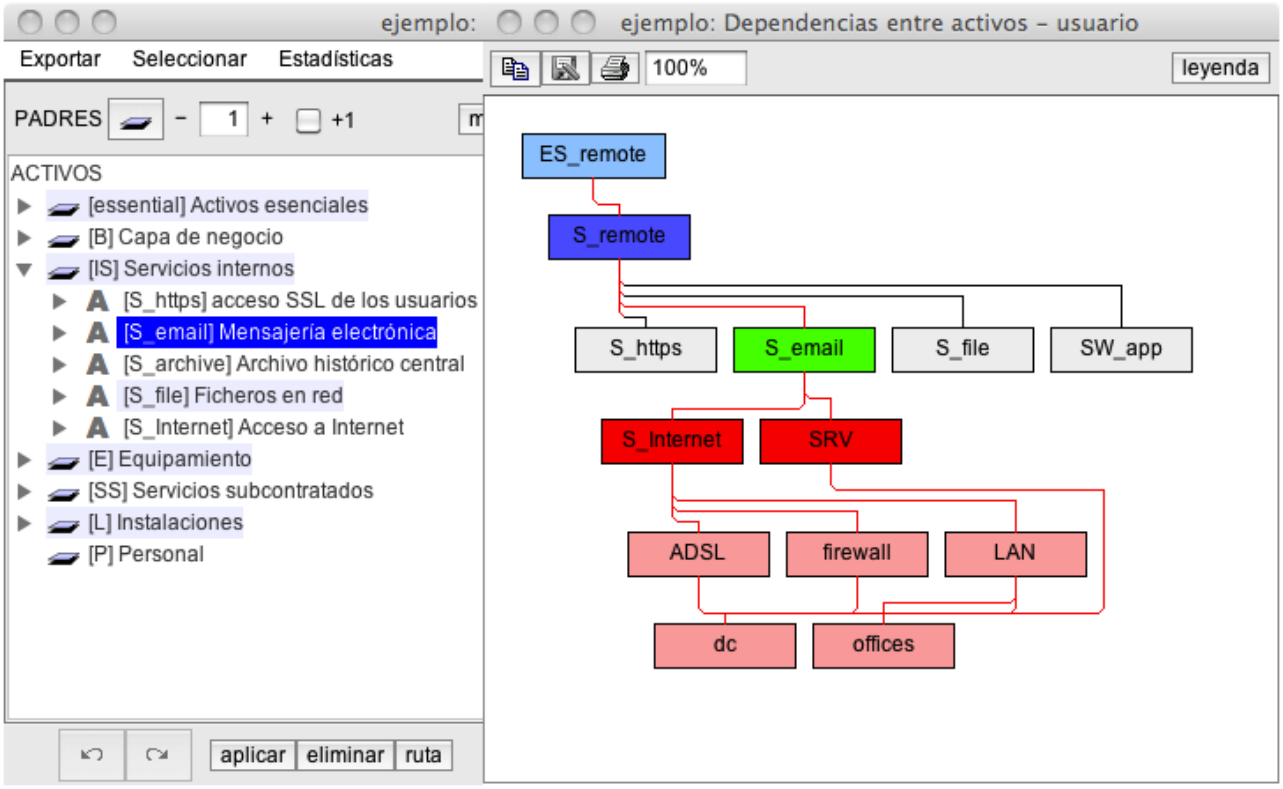
11.5.3. BUSES: DEPENDENCIAS ENTRE ACTIVOS

El gráfico muestra las relaciones de dependencia entre activos. Sólo 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
100%	**escala**	para cambiar el tamaño de la imagen
	leyenda	muestra el código de colores

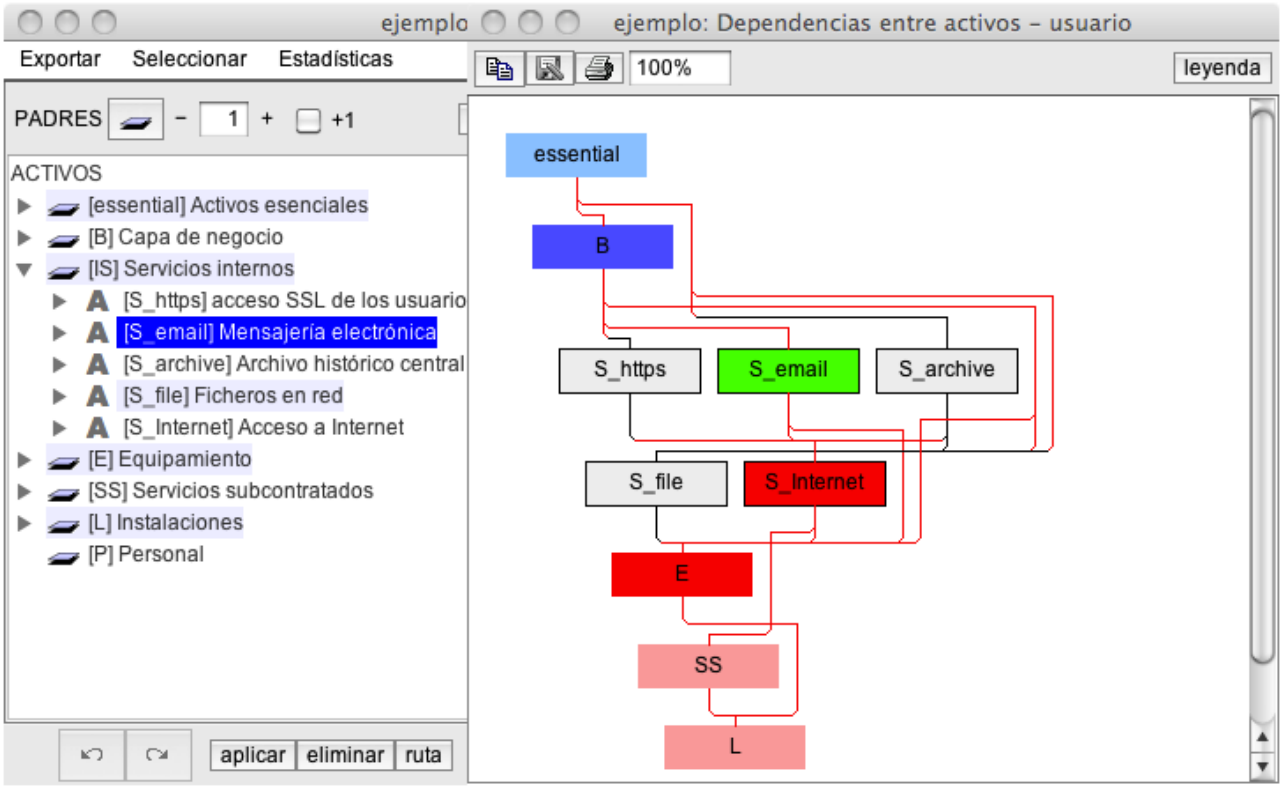
11.5.4. BLOQUES: DEPENDENCIAS ENTRE ACTIVOS

El gráfico muestra las relaciones de dependencia entre activos. Sólo 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
100%	**escala**	para cambiar el tamaño de la imagen
	leyenda	muestra el código de colores

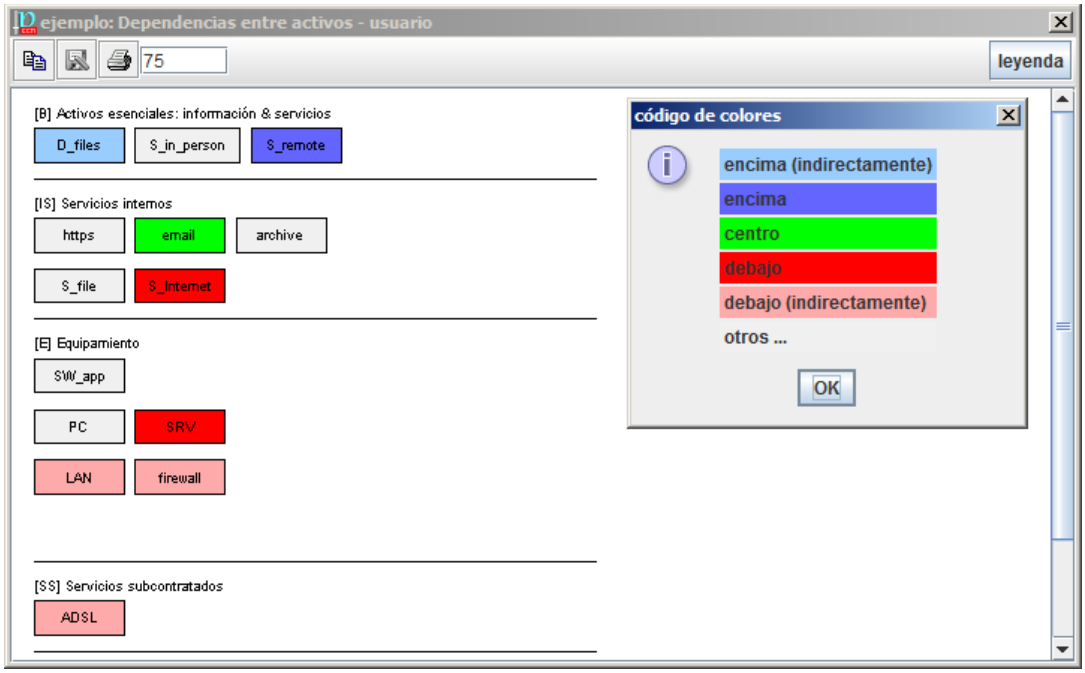
11.5.5. MAPA DE DEPENDENCIAS ENTRE ACTIVOS

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



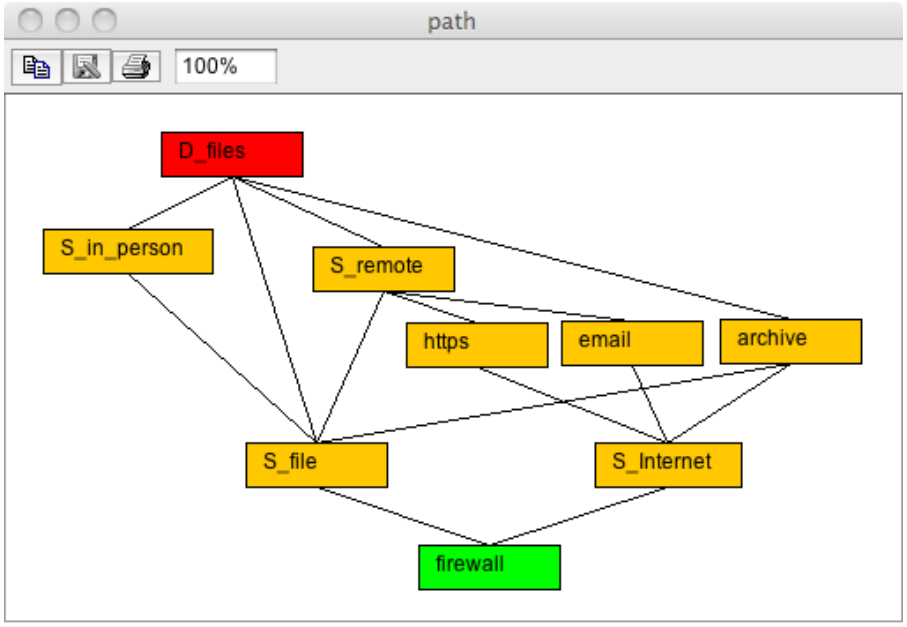
Para modificar las dependencias

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
100%	**escala**	para cambiar el tamaño de la imagen
	leyenda	muestra el código de colores

11.5.6. DEPENDENCIAS POR DIMENSIÓN DE SEGURIDAD

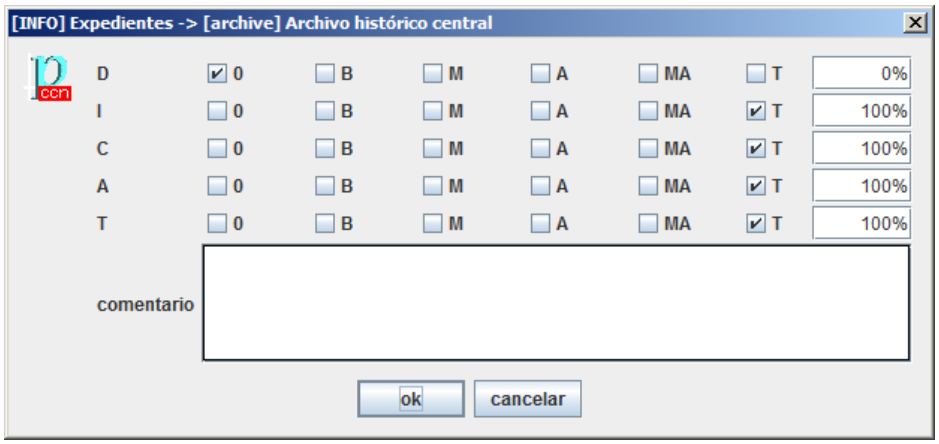
Se puede especificar un grado de dependencia diferente en cada dimensión. Para ello haga clic con el botón derecho sobre la dependencia y aparecerá una pantalla donde puede marcar el grado de dependencia preciso en cada dimensión.

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 sólo — 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.

11.6. ACTIVOS / VALORACIÓN

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

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

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

11.6.1. VALORACIÓN DE LOS DOMINIOS DE SEGURIDAD

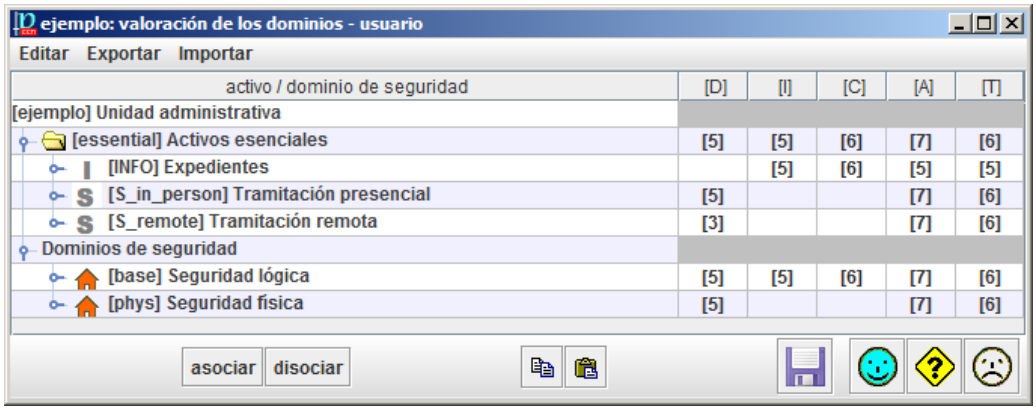
Se hace una valoración "rápida y aproximada" común para todos los activos en el dominio. Es más rápido que la valoración por dependencias. Usando este método, todos los activos en el dominio reciben los mismos valores.

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.

Supongamos que tenemos 2 dominios de seguridad

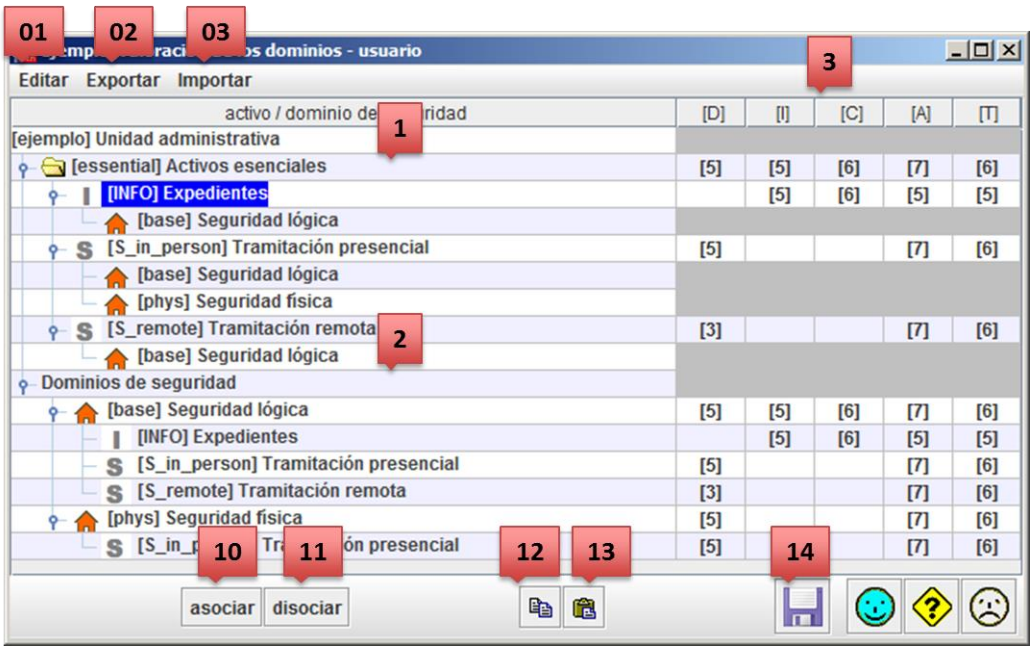
— [base] Seguridad lógica

— [phys] Seguridad física



activo / dominio de seguridad	[D]	[I]	[C]	[A]	[T]
[ejemplo] Unidad administrativa					
[essential] Activos esenciales	[5]	[5]	[6]	[7]	[6]
[INFO] Expedientes		[5]	[6]	[5]	[5]
[S_in_person] Tramitación presencial	[5]			[7]	[6]
[S_remote] Tramitación remota	[3]			[7]	[6]
Dominios de seguridad					
[base] Seguridad lógica	[5]	[5]	[6]	[7]	[6]
[phys] Seguridad física	[5]			[7]	[6]

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. Ver "*Subconjunto de dimensiones*".
4	valor de los activos	Para cada activo esencial y cada dimensión de seguridad, el valor — Ver *Activos / Valoración / cualitativo* — Ver *Activos / Valoración / cuantitativo*
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

11.6.2. VALORACIÓN ACTIVO POR ACTIVO

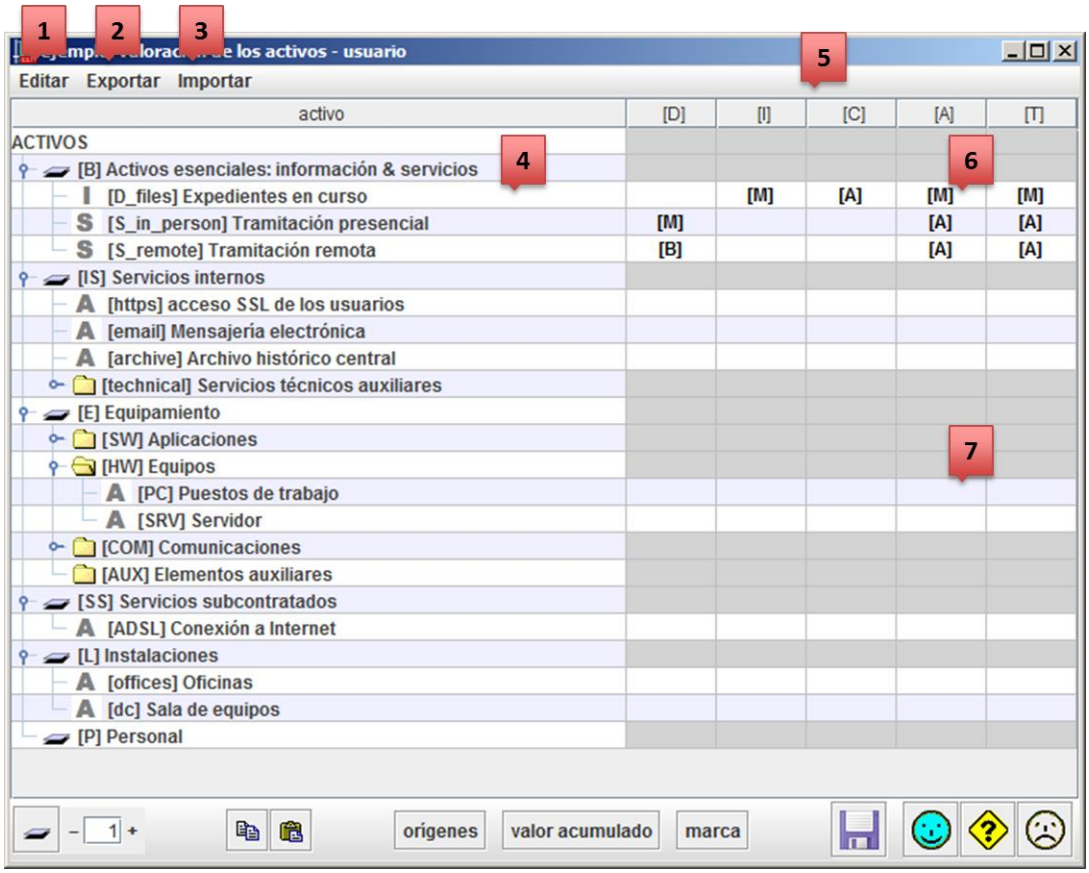
Si está valorando el sistema por activos,, necesita establecer las dependencias (ver "*Dependencias entre activos*").

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.

Esta pantalla se utiliza para asignar valores a activos individuales en cada dimensión.



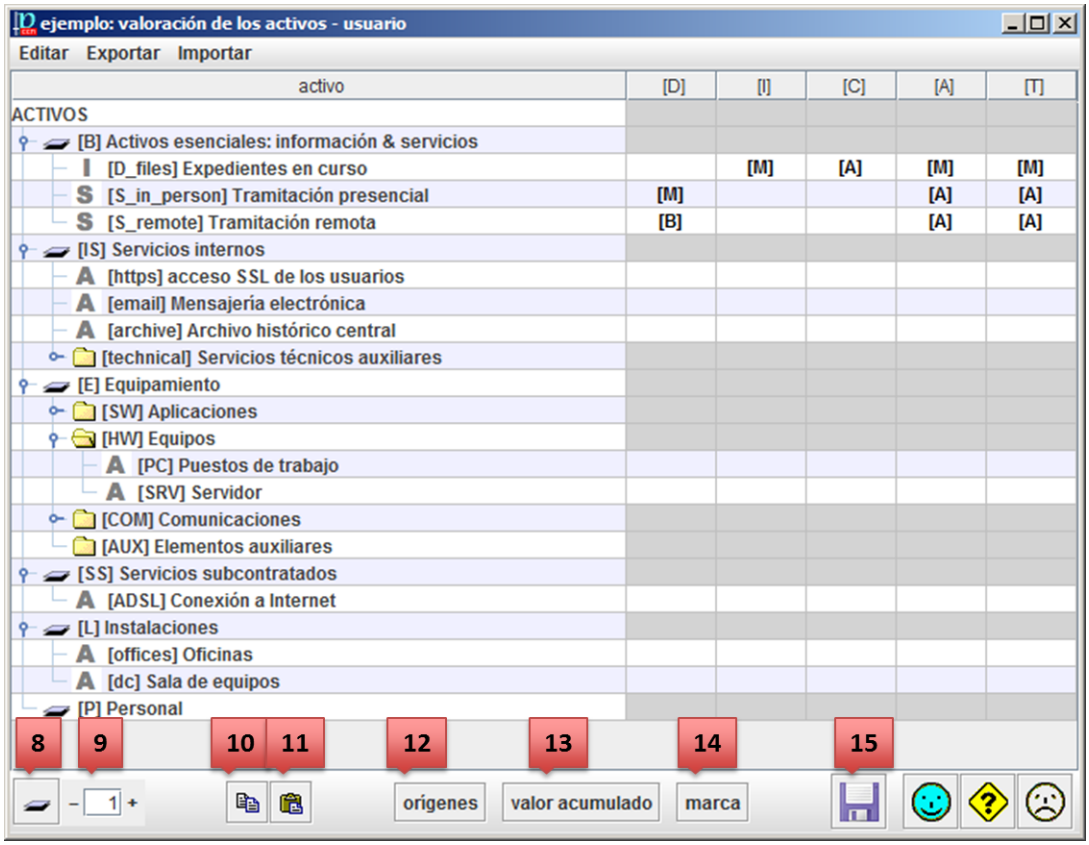
1	editar	Ver copiar [10] y pegar [11] a continuación
2	exportar	Se pueden exportar los datos a — CSV – comma separated values — XML – extensible markup language
3	importar	De XML
4	activos	Árbol de activos

5	dimensiones	Tantas columnas como dimensiones de seguridad.
6 7	valor	Para cada activo y cada dimensión de seguridad. Cuando se presenta el valor propio, el valor aparece sobre fondo blanco Cuando se presenta en valor acumulado, aparece sobre fondo verdoso Cuando el análisis de riesgos es cuantitativo, los valores son cantidades numéricas:

	[M]	[A]	[M]	[M]
[M]			[A]	[A]
[B]			[A]	[A]

[M]	[A]	[A]	[A]	[A]
[M]	[A]	[A]	[A]	[A]

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



8		Haga clic para recoger el árbol de activos
9	- 1 +	Controla el nivel de despliegue del árbol de activos
10		Seleccione una o más celdas. Copie lo valores para pegarlos más tarde.
11		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.
12	fuentes	Seleccione una fuente. PILAR seleccionará los activos que están asociados a dicha fuente.
13	valor acumulado / propio	Conmuta entre presentar sólo el valor propio, o acompañarlo del valor acumulado.
14	marcar	Útil para ver cómo se propaga el valor. Seleccione una celda en [6] o [7] 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: activo | [D] | [I] | [C] | [A] | [T] ACTIVOS [essential] Activos esenciales [essential.info] información | [7] [D] Datos / Información [D.log] registro de actividad (log) | [7] | [7]
15		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 porqué este valor
- para seleccionar los criterios que se aplican de ésos en la biblioteca.
  Es importante intentar utilizar criterios codificados.

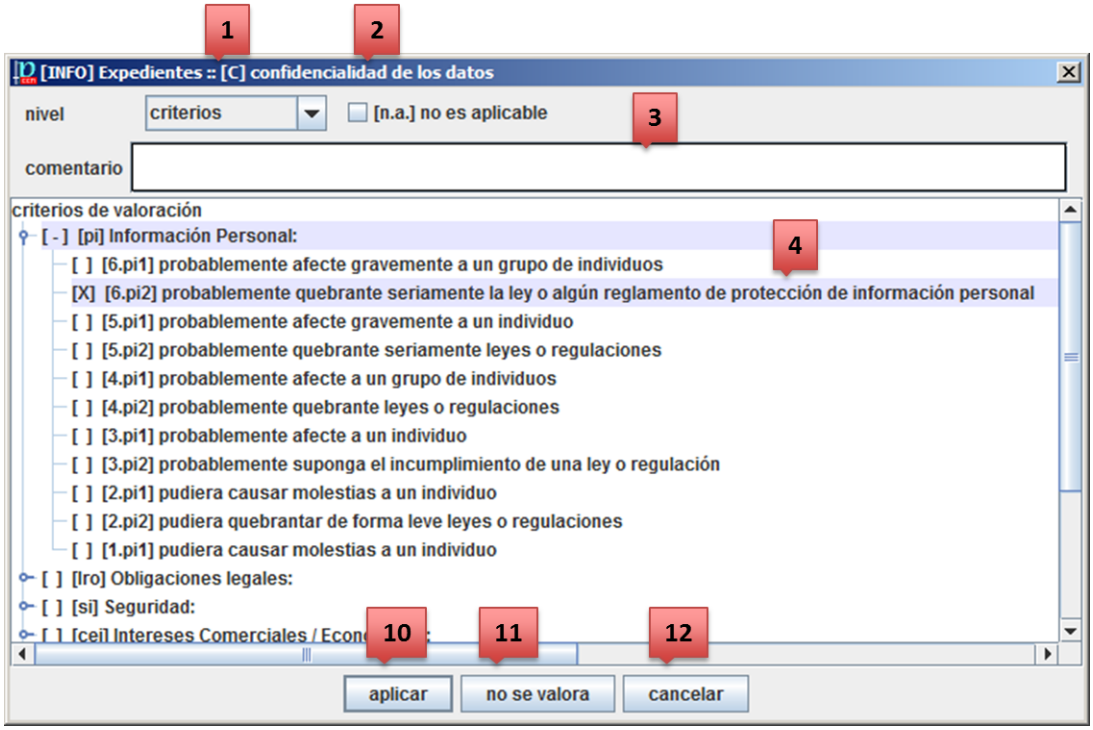
Para descubrir de dónde llega el valor que se acumula en un activo:

- seleccione el activo (una fila)
- clic ORÍGENES

11.6.3. 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. Ver “*Anulación de una valoración*”.
3	Un comentario para explicar el por qué de la valoración
4	Criterios para valorar un activo

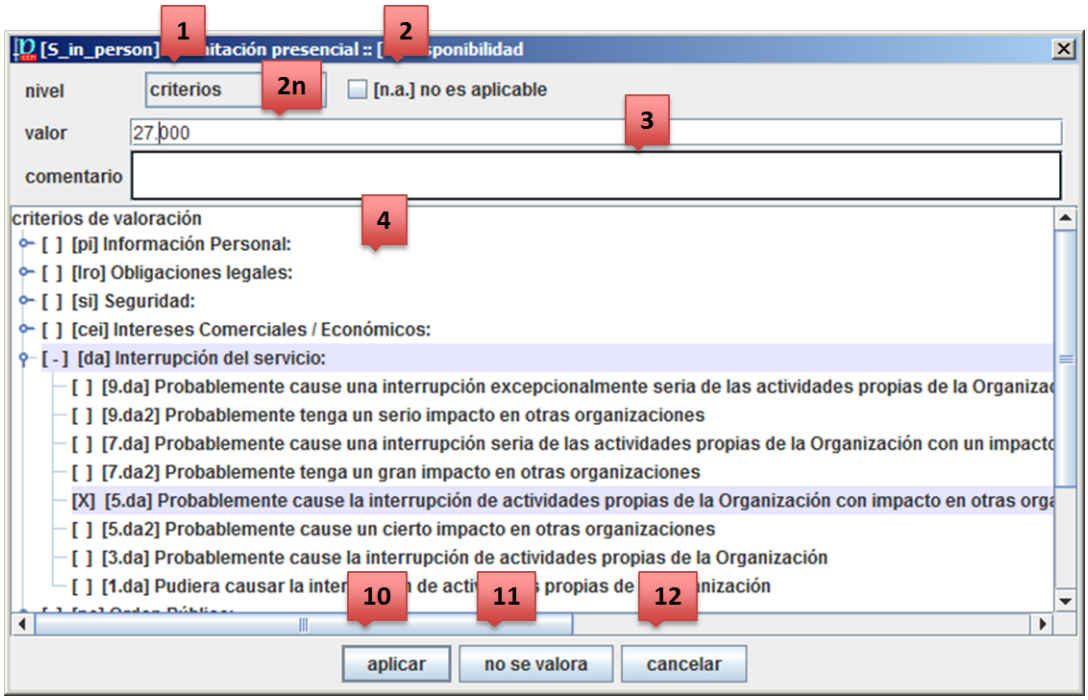
10	Aplica el valor y cierra la ventana
11	Elimina el valor del activo y cierra la ventana
12	Cierra la ventana sin modificar la valoración del activo

11.6.4. 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



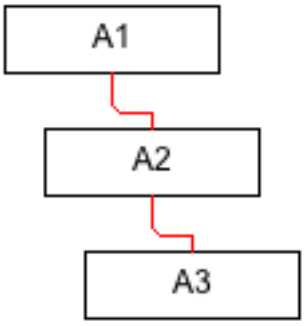
1	Marca el valor cualitativo. Si selecciona “CRITERIOS”, el valor lo decide la marca de mayor valor de los criterios marcados en [4]. Si selecciona un nivel, este será el asignado al activo, independientemente de los criterios marcados.
2	Se marca N.A. cuando esa dimensión no tiene relevancia ni para ese activo ni propaga su valor a los activos de los que depende. Ver “*Anulación de una valoración*”.

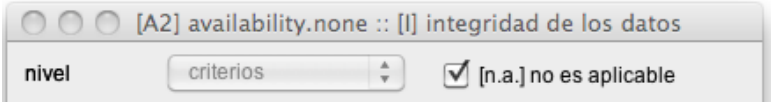
2n	Marca el valor cuantitativo.
3	Un comentario para explicar el por qué de la valoración
4	Criterios para valorar un activo
10	Aplica el valor y cierra la ventana
11	Elimina el valor del activo y cierra la ventana
12	Cierra la ventana sin modificar la valoración del activo

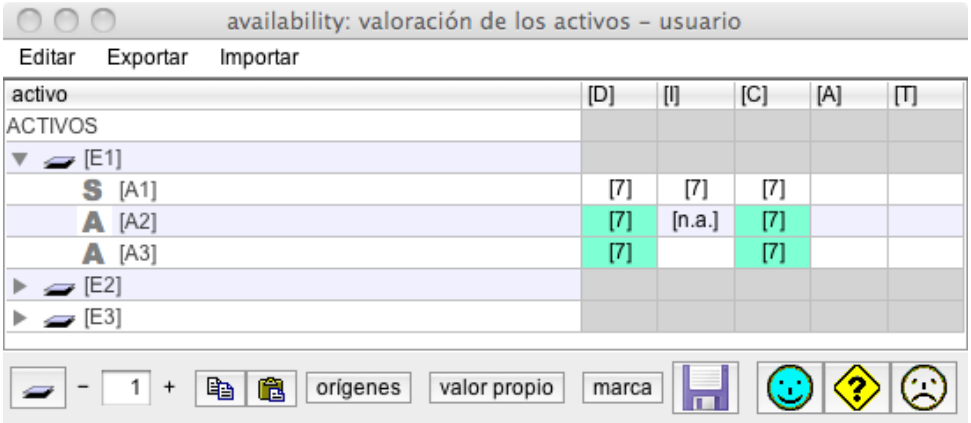
Cuando PILAR conoce sólo una valoración cualitativa o sólo una valoración cuantitativa, recurre a la tabla de *Cuantificación del valor* para estimar el valor que falta.

11.6.5. 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.

11.6.6. VALORACIÓN DE LA DISPONIBILIDAD

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

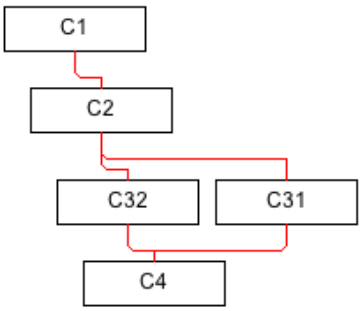
- por *dependencias*
- por *anulación* del valor,
- ajustando algunos calificativos del activo (ver a continuación).

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.



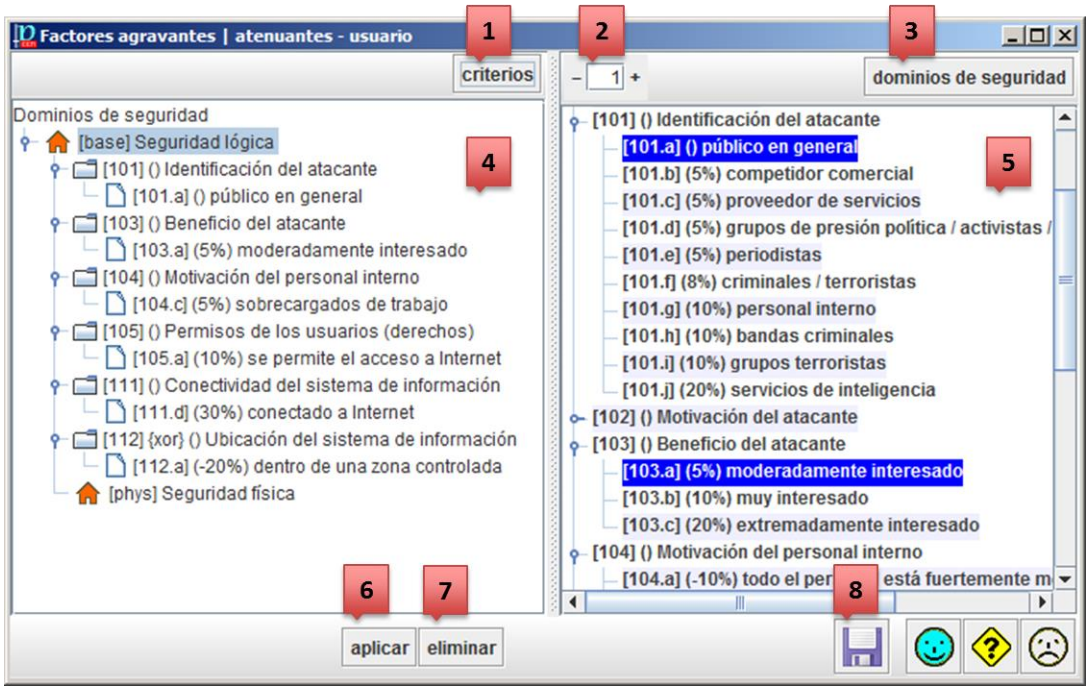
activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[E1]					
[E2]					
[E3]					
S [C1]	[7]		[7]		
A [C2] OR	[7]		[7]		
A [C31]			[7]		
A [C32]			[7]		
A [C4]	[7]		[7]		

11.7. AMENAZAS

11.7.1. 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*").



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)

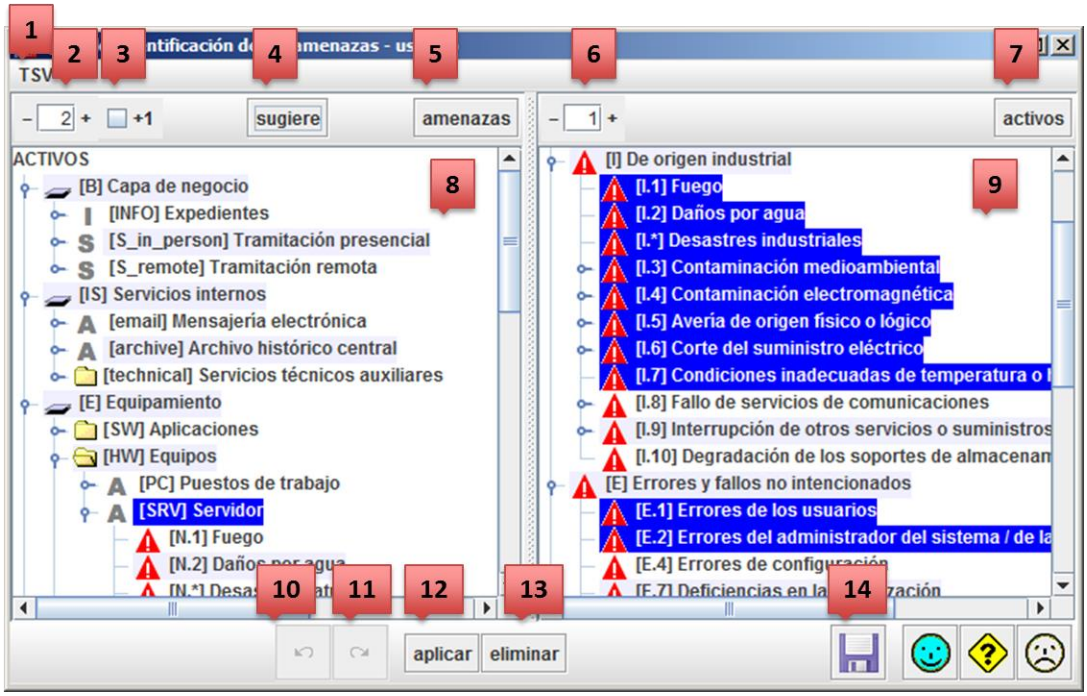
11.7.2. IDENTIFICACIÓN

Para empezar rápidamente
Seleccione los **ACTIVOS** en el panel izquierdo (arriba). Seleccione la **BIBLIOTECA** (abajo a la izquierda). Acaba de establecer un mapa típico de ataques en base a la naturaleza de los activos. Seleccione **OK** para continuar.
Aún más rápido
Seleccione amenazas automáticas en *Opciones / Amenazas*

Identificamos qué amenazas son posibles para cada activo. Más adelante determinaremos la frecuencia 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



1	TSV	Ver "*Threat Standard Values*

2	- 1 +	Controla el despliegue del árbol de activos.
3	+1	Ajusta el efecto de [2]. Si se marca [+1], PILAR muestra también las amenazas asociadas a cada activo.
4	sugiere	— Seleccione uno o más activos a la izquierda ([8]). — Haga clic en SUGIERE. PILAR presenta a la derecha ([9]) las amenazas que tienen sentido para los activos seleccionados. Para ello, tiene en cuenta las clases de activos y la valoración en cada dimensión. Usted puede revisar la selección, y hacer clic en APLICAR para asociar las amenazas seleccionadas a los activos seleccionados.
5	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.
6	- 1 +	Controla el despliegue del árbol de amenazas.
7	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
10		Revierte la última asociación de activos y amenazas.
11		Reaplica la última asociación de activos y amenazas revertida.
12	aplicar	— Seleccione uno o más activos a la izquierda ([8]). — Seleccione una o más amenazas a la derecha ([9]). — Haga clic en APLICAR. PILAR asociada las amenazas seleccionadas a los activos seleccionados.
13	eliminar	— Seleccione uno o más activos a la izquierda ([8]). — Seleccione una o más amenazas a la derecha ([9]). — Haga clic en ELIMINAR. PILAR disocia las amenazas seleccionadas de los activos seleccionados. Ó

		— Seleccione una o más amenazas a la izquierda ([8]) — Haga clic en ELIMINAR PILAR disocia las amenazas seleccionadas de los activos seleccionados.
14		Guarda el proyecto en su fichero o en su base de datos.

Si desea cambiar el perfil de amenazas cargado por la biblioteca

- clic en CARGA

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 sólo 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

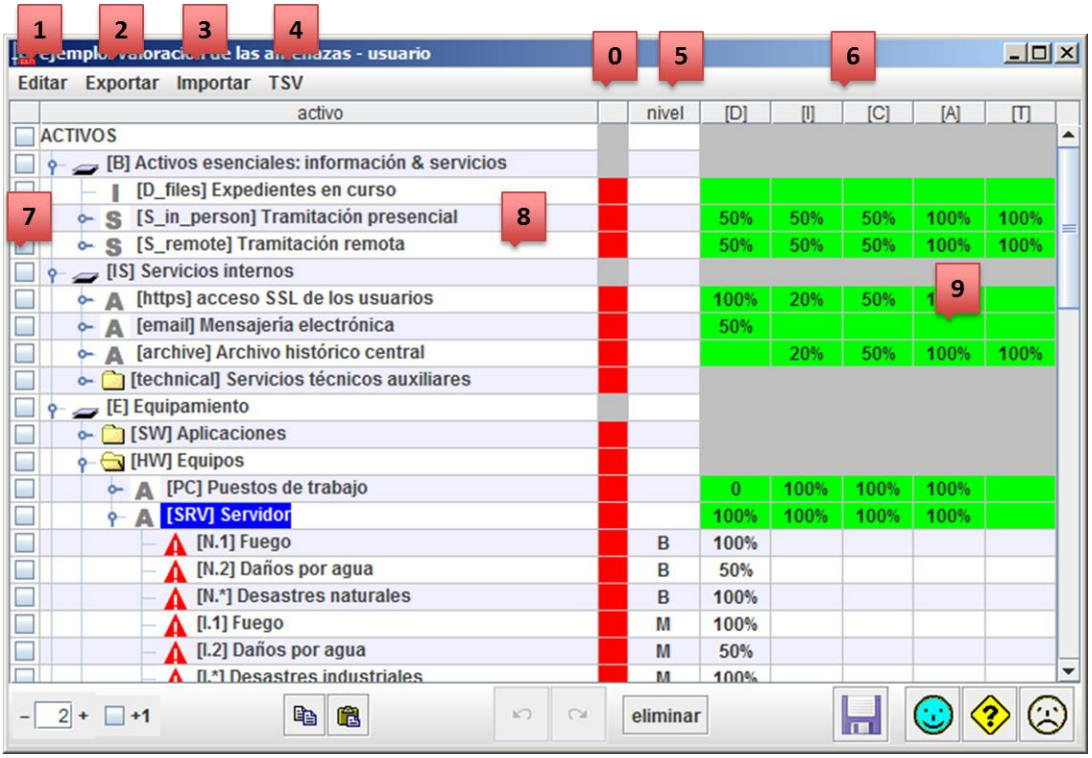
Puede utilizar la biblioteca para que le ayude. Seleccione uno o más activos en el panel izquierdo y ...

- 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

11.7.3. VALORACIÓN

Para empezar rápidamente
Seleccione amenazas automáticas en *Opciones / Amenazas*

Esta sección describe el funcionamiento en modo manual. Si pone PILAR en modo automático, la mayor parte de las opciones están anuladas ya que PILAR aplica los valores del fichero TSV (ver "*Threat Standard Values*").



0		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.

1	editar	opciones – ver *Editar / Opciones* copiar – ver [12] más abajo pegar – ver [13] más abajo
2	exportar	Genera un fichero CSV o XML
3	importar	Carga un fichero XML
4	TSV cargar aplicar	Ver "*Threat Standard Values*". Carga un fichero TSV. Aplica los valores del fichero TSV a las filas seleccionadas (ver [7]).
5		Esta columna presenta la probabilidad de ocurrencia. El formato se puede ajustar en *Opciones / Probabilidad*
6		Estas columnas presentan la degradación causada por la amenaza en cada dimensión. El formato se puede ajustar en *Opciones / Degradación*
7	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 ([4]) o se borran los valores ([16]).
8		Activos y amenazas
9		Valoraciones de probabilidad y degradación

10	− 1 +	Controla el despliegue del árbol de activos.
11	+1	Ajusta el despliegue ([10]). Si se marca [+1], PILAR muestra las amenazas asociadas a cada activo.
12		Seleccione una o más celdas en [9]. Haga clic para copiar los valores.
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		Revierte los últimos cambios
15		Aplica de nuevo los últimos cambios revertidos
16	eliminar	— Seleccione una o más filas ([8]). — Haga clic en ELIMINAR. PILAR elimina los valores de las filas seleccionadas.
17		Guarda el proyecto en su fichero o en su base de datos.

Ejemplo (modo mix) donde una amenaza se ha marcado como manual mientras el resto sigue en modo automático:

[SS] Servicios subcontratados			
[ADSL] Conexión a Internet			50%
[I.8] Fallo de servicios de comunicaciones		A	50%
[I.9] Interrupción de otros servicios o suministros esenciales		M	50%
[E.2] Errores del administrador del sistema / de la seguridad		M	20%
[E.18] Destrucción de la información		M	10%
[E.24] Caída del sistema por agotamiento de recursos		M	50%
[A.7] Uso no previsto		M	10%
[A.18] Destrucción de la información		M	50%
[A.24] Denegación de servicio		A	50%

Las amenazas marcadas como manuales pueden editarse.

11.7.4. 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

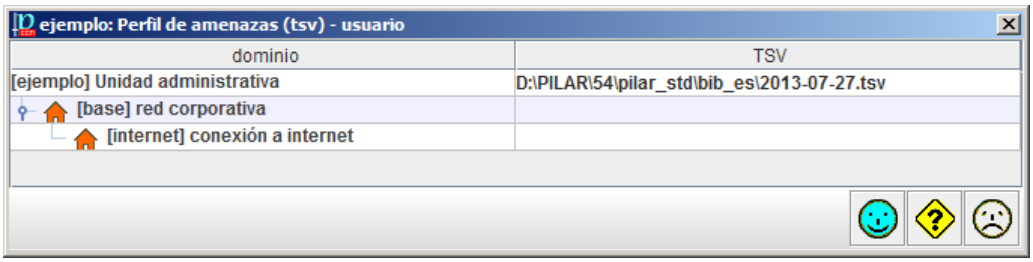
[http://www.pilar-tools.com/es/tools/pilar/doc.htm]

aunque también puede abrir el fichero con un editor XML

bib_es / 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> <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>	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

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.

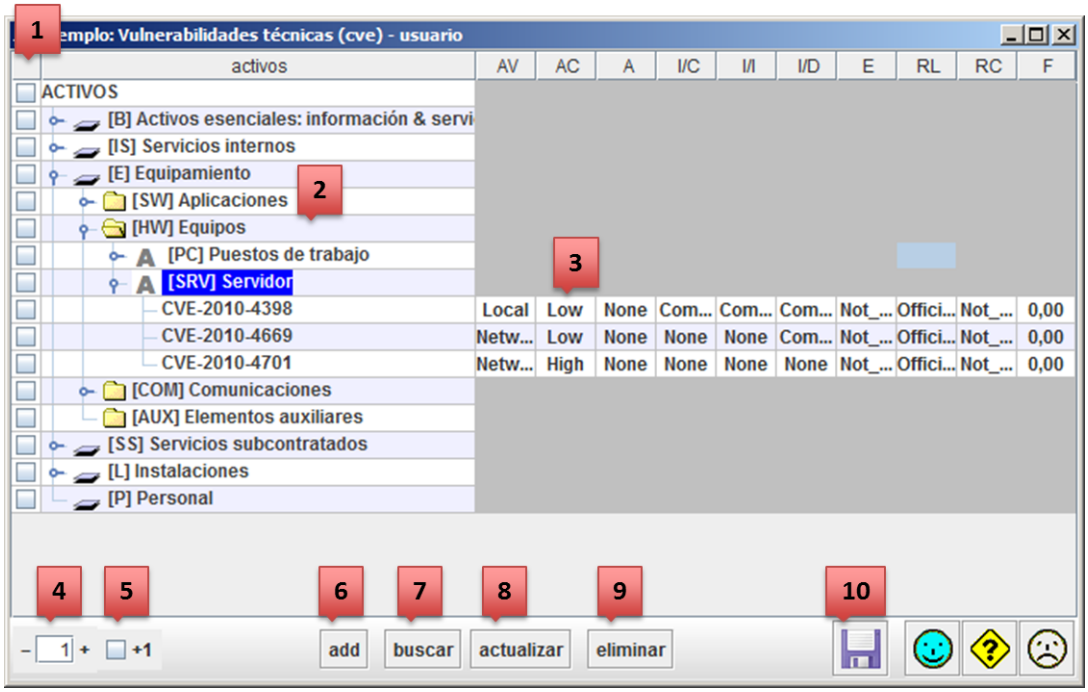
El nombre y la ruta de los ficheros TSV se almacenan con el proyecto. Cuando se abre el proyecto, pilar intenta recargarlo y verifica si el fichero ha cambiado. PILAR se queja amargamente si el proceso no funciona como la seda.

11.7.5. VULNERABILIDADES TÉCNICAS (CVE)

Ver

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

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



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 aplican los botones [6] a [9].
2	activos	Activos y vulnerabilidades CVE.
3	CVE	Ver abajo.
4	- 1 +	Controla el despliegue del árbol de activos y CVE.
5	+1	Ajusta el funcionamiento de [4]. Si se marca [+1], PILAR presenta las CVE asociados a cada activo.
6	añadir	— Seleccione un activo a la izquierda ([1]). — Haga clic en AÑADIR para introducir manualmente una CVE.
7	buscar	— Seleccione uno o más activos a la izquierda ([1]). — 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.
8	actualizar	Como BUSCAR ([7]), pero ahora sólo se actualizan datos ya cargados.
9	eliminar	— Seleccione uno o más activos a la izquierda ([1]) — Haga clic en ELIMINAR PILAR elimina las CVE asociadas Ó — Seleccione una o más vulnerabilidades a la izquierda ([1]) — Haga clic en ELIMINAR PILAR elimina las CVE marcadas
10		Guarda el proyecto en su fichero o en su base de datos.

Las columnas presentan los valores asociados a una vulnerabilidad según el formato CVSS v2 (ver [http://nvd.nist.gov/cvss.cfm]).

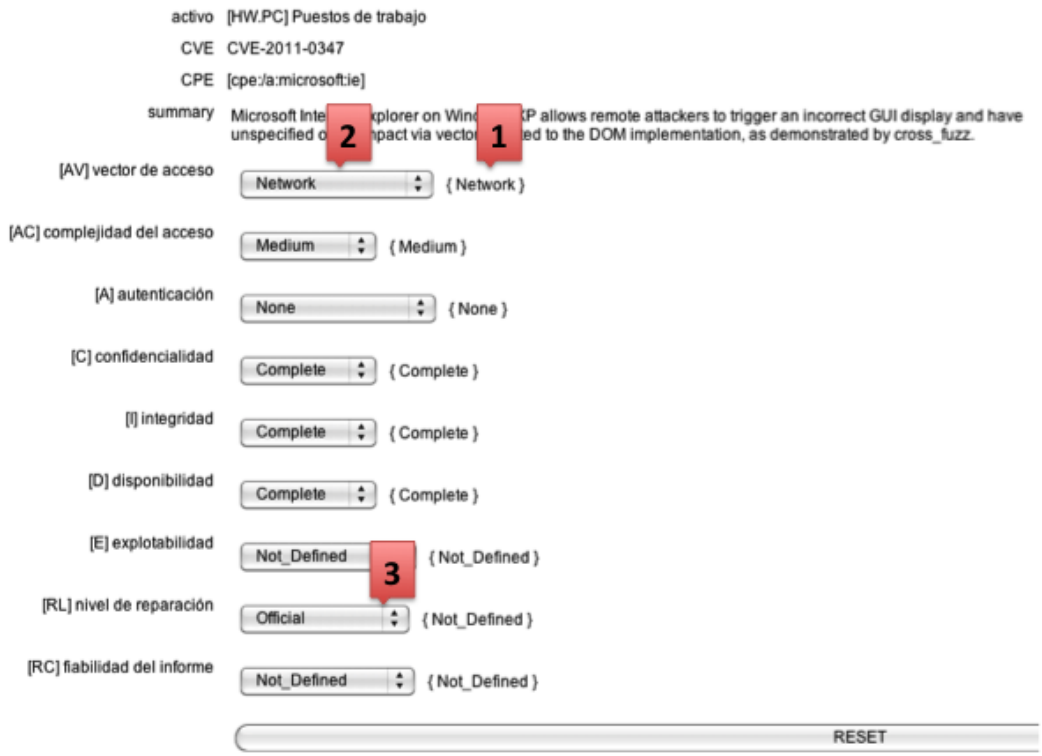
La información de vulnerabilidades se extrae de ficheros externos en formato XML que puede fabricar el usuario o descargar de algún repositorio de vulnerabilidades, por ejemplo de

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

La sección [3] está un poco saturada. La siguiente figura transpone filas y columnas:

activos	[PC]	CVE-2011-0346	CVE-2011-0347		
AV		Network	Network	access vector	vector de acceso
AC		Low	Medium	access complexity	complejidad del acceso
A		None	None	authentication	autenticación
I/C		Complete	Complete	impact / confidentiality	impacto / confidencialidad
I/I		Complete	Complete	impact / integrity	impacto / integridad
I/A		Complete	Complete	impact / availability	impacto / disponibilidad
E		Unproven	Functional	exploitability	si es explotable
RL		Official	Work Around	remediation level	nivel de reparación
RC		Unconfirmed	Confirmed	report confidence	confianza en el informe
F		0	22.5	frequency	frecuencia

Puede editar los valores (clic-clic en el nombre de la CVE, en [2]).



Para cada campo en CVSSv2, hay un valor por defecto ([1]) cargado de la base de datos de CVEs, y un valor que puede modificar ([2]). El campo más importante es RL ([3]) donde se actualiza si el parche existe y está instalado, cerrando la vulnerabilidad.

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

11.8. SALVAGUARDAS

11.8.1. ASPECTO

Aspecto que trata la salvaguardas

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

11.8.2. 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

11.8.3. PESO RELATIVO

3	máximo peso	crítica

2	peso alto	muy importante
1	peso normal	importante
0	peso bajo	interesante
✓	aseguramiento: componentes certificados	

11.8.4. INFORMACIÓN ADICIONAL

Una ventana separada presenta información adicional relativa a la salvaguarda

safeguard

[D.C.4.1] {xor} Shared secret (symmetric encryption)
Aspect: [T] technical
Type of protection: [EL] elimination

Additional information:
[D] Protection of Data / Information:
[D.C] Encryption of information:
[D.C.4] {xor} Encryption mechanism:
[D.C.4.1] {xor} Shared secret (symmetric encryption):
- ISO/IEC 10116 - Modes of operation for an n-bit block cipher algorithm"
  http://www.iso.org/
- ISO/IEC 18033 - Encryption algorithms"
  http://www.iso.org/
- FIPS 197 - Advanced Encryption Standard (AES)"
  http://www.itl.nist.gov/fipspubs/index.htm
- ISO/IEC 10116 - Modes of operation for an n-bit block cipher algorithm"
  http://www.iso.org/

11.8.5. 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*".

n.a.

marca la salvaguarda como no aplicable, para todas las fases

aplicable

marca la salvaguarda como aplicable, para todas las fases

11.8.6. IDENTIFICACIÓN

Para empezar rápidamente
— Seleccione el botón RECOMENDACIÓN en la barra inferior. — OK. Acaba de aceptar la recomendación de PILAR. Si no está 100% de acuerdo, puede cambiar lo que considere oportuno.

Esta pantalla permite retirar del análisis aquellas salvaguardas que se considere que están fuera de lugar y por tanto no son aplicables.

11.8.6.1. MENÚS BARRA SUPERIOR

Menú EDITAR

Ver "*Salvaguardas / Buscar*".

Menú EXPANDIR

Expande el árbol hasta un determinado perímetro:

- basado en el nivel: BÁSICO, MEDIO o EXPERTO
- hasta llegar a las salvaguardas no aplicables
- hasta perímetros definidos en la librería
- hasta perímetros definidos por el usuario (ver *Perímetros*

Menú EXPORTAR

Genera un informe: "*SoA – Declaración de Aplicabilidad*".

Menú VER

Riesgos – Seleccione una o más líneas en la primera columna. Haciendo clic sobre riesgos, PILAR le lleva a la tabla de riesgos acumulados ("*Tabla de impacto y riesgo acumulado*") filtrando sólo los riesgos que se pueden mitigar por medio de alguna de las salvaguardas seleccionadas.

Esta función busca que el usuario pueda centrarse en los riesgos derivados de una deficiente implementación de una o más salvaguardas. En otras palabras, en los riesgos provocados por una vulnerabilidad estructural por ausencia o debilidad de mecanismos de control.

Menú ESTADÍSTICAS

Genera una tabla resumen con al número de salvaguardas evaluadas en cada dominio de seguridad.

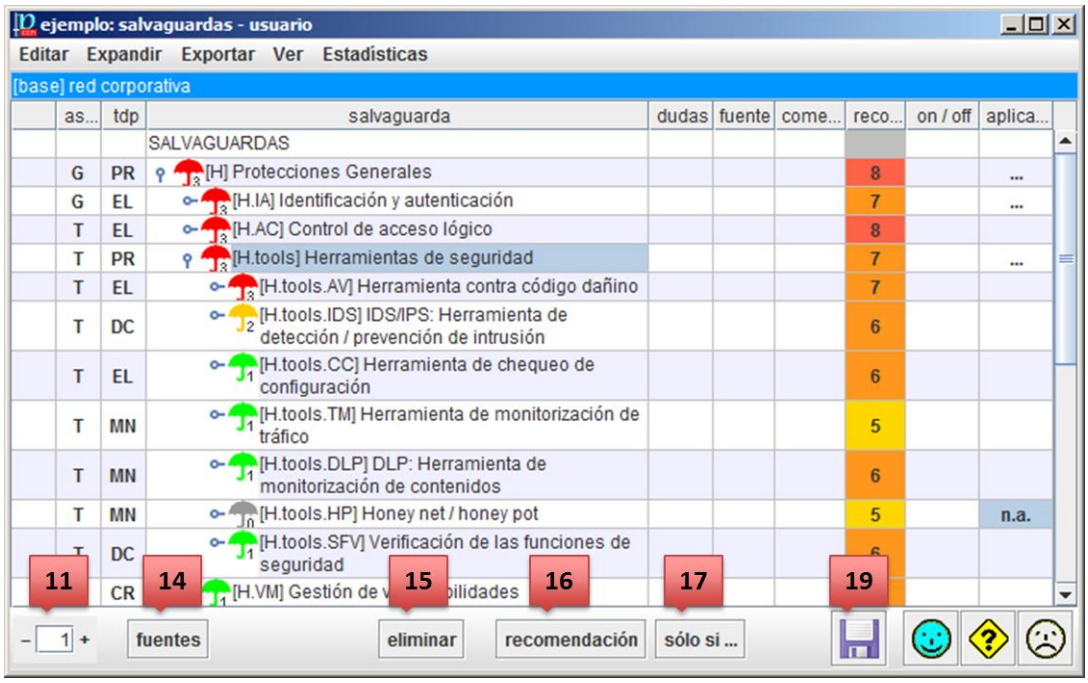
11.8.6.2. PANTALLA PRINCIPAL, CUERPO

0		**Trabaja en combinación con el menú Ver >> Riesgos** Seleccione una o más líneas. Haciendo clic sobre riesgos, PILAR le lleva a la tabla de riesgos acumulados ("*Tabla de impacto y riesgo acumulado*") filtrando sólo los riesgos que se pueden mitigar por medio de alguna de las salvaguardas seleccionadas. Esta función busca que el usuario pueda centrarse en los riesgos derivados de una deficiente implementación de una o más

		salvaguardas. En otras palabras, en los riesgos provocados por una vulnerabilidad estructural por ausencia o debilidad de mecanismos de control.
1	dominio de seguridad	Pueden haber diferentes salvaguardas en diferentes dominios. Haga clic para seleccionar el dominio en el que vamos a trabajar.
2	aspecto	Ver "*Salvaguardas / Aspecto*".
3	tdp	Ver "*Salvaguardas / Tipo de protección*".
4		Árbol de salvaguardas. Haga clic-clic para colapsar / expandir el árbol. Clic con el botón derecho para acceder a *Salvaguardas / tree*
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	comentario	Haga clic para asociar un comentario a la salvaguarda.
8	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.
9	on / off	Se usa para descartar de forma temporal algunas salvaguardas. Funciona como [10] pero no es una declaración formal de no-aplicabilidad.
10	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.

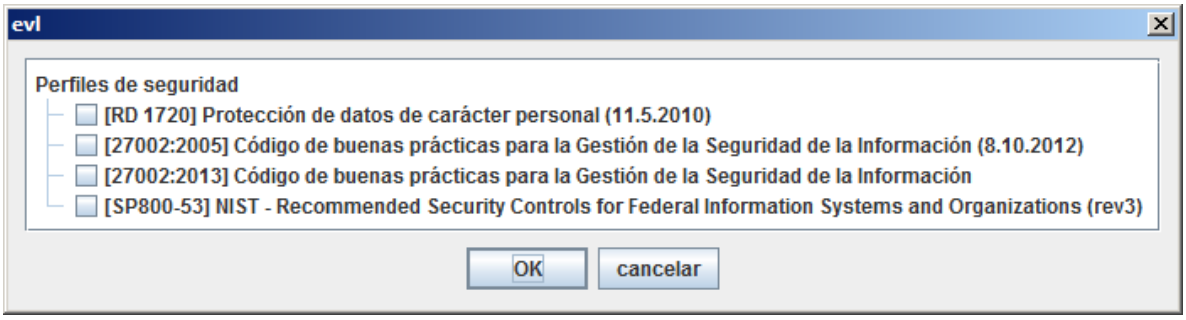
11.8.6.3. BARRA INFERIOR DE HERRAMIENTAS



11	− 1 +	Controla el despliegue del árbol de salvaguardas.
14	fuentes	Seleccione una o más fuentes de información. PILAR seleccionará todas las salvaguardas a las que está asociada.
15	eliminar	Elimina todas las marcas en [9] y [10].
16	recomendación	Haga clic y PILAR marcará como no aplicables todas las salvaguardas que PILAR no sabe cómo aplicar; es decir, las que tienen una recomendación gris.
17	sólo si …	PILAR retiene solamente las salvaguardas que se necesitan para cumplir con uno o más perfiles de seguridad.
19		Guarda el proyecto en su fichero o en su base de datos.

11.8.6.4. SÓLO SI …

PILAR presenta una lista de los perfiles de seguridad (EVL) cargados. Seleccione aquellos cuyo cumplimiento le preocupa. PILAR eliminará las salvaguardas no cubiertas por dichos perfiles.



11.8.6.5. 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	Puede seleccionar un subconjunto de los dominios para el informe. Mientras

seguridad	no indique lo contrario, se imprimen todos.
Nivel	Ver *Perímetros*
Incluye	Puede incluir sólo las salvaguardas que aplican, sólo las que no, o ambas categorías.
Formato	El formato RTF es útil para documentos. El formato HTML es útil para intranets.

11.8.7. VALORACIÓN POR DOMINIOS

Para empezar rápidamente

- Vaya al **combo** inferior a la izquierda, y seleccione **básico.**
- 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).

11.8.7.1. BARRA SUPERIOR - MENÚS

01	editar copiar ⌘C pegar ⌘V buscar ⌘F	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	expandir	Expande el árbol hasta alguno de los perímetros disponibles: • por nivel: BÁSICO, MEDIO o EXPERTO • hasta las salvaguardas no-aplicables • hasta perímetros definidos en la biblioteca • hasta perímetros definidos por el usuario (ver *Perímetros*
03	exportar ... a CSV ... a XML informe < Lx < objetivo	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

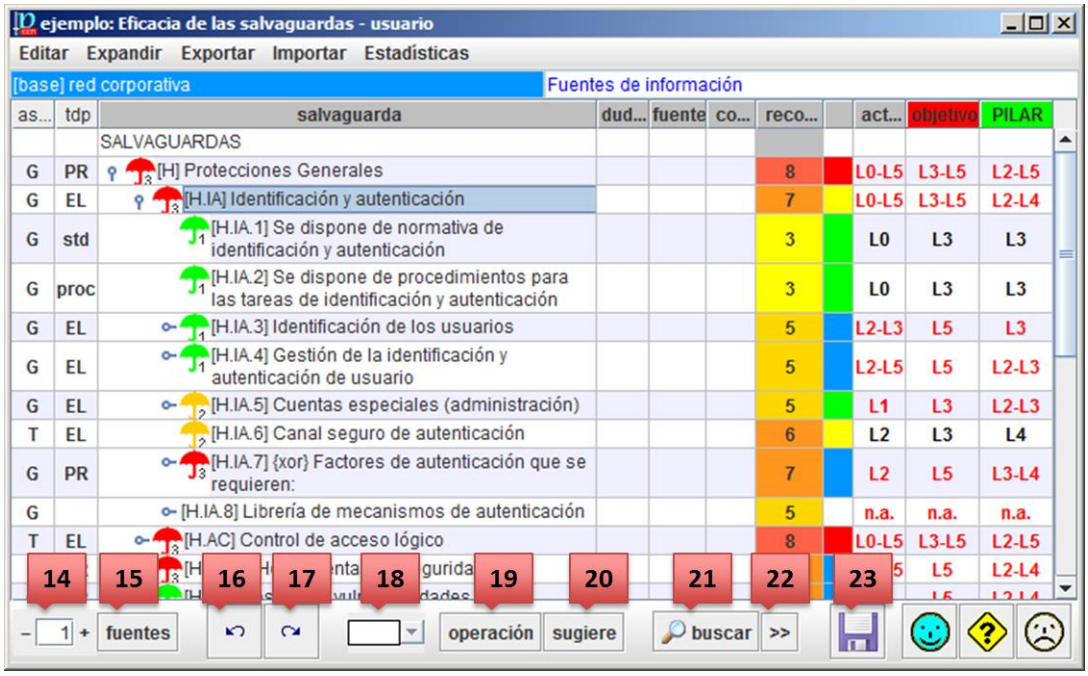
		pero están por debajo de un cierto umbral de madurez < objetivo Se genera un informe con las salvaguardas que están por debajo de la fase OBJETIVO. Ver *Salvaguardas / Fases de referencia y objetivo*
04	importar	Lee los niveles de madures de un fichero, CSV o XML.
05	estadísticas	Genera una tabla resumen con al número de salvaguardas evaluadas en cada dominio de seguridad.

11.8.7.2. PANTALLA PRINCIPAL – CUERPO

1	dominio de seguridad	Pueden haber diferentes salvaguardas en diferentes dominios. Haga clic para seleccionar el dominio en el que vamos a trabajar.
2	fuentes de información	Haga clic para seleccionar fuentes de información. PILAR recortará el árbol [5] para mostrar sólo las asociadas a alguna de las fuentes de información marcadas.
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.
7	fuentes	Haga clic para asociar fuentes de información a la salvaguarda (la marcada y sus descendientes).
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 "*Valoración de salvaguardas por dominios*".

11.8.7.3. BARRA INFERIOR DE HERRAMIENTAS

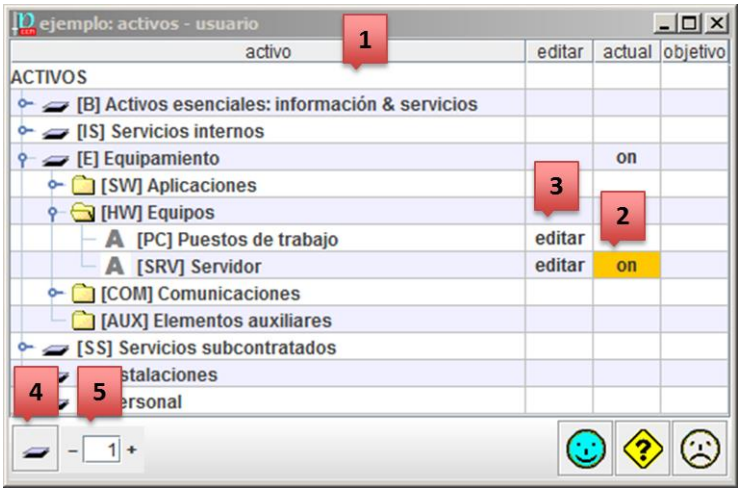


14	- 1 +	Controla el despliegue del árbol de salvaguardas.
15	fuentes	Seleccione una o más fuentes de información. PILAR seleccionará todas las salvaguardas a las que está asociada.
16		Revierte los últimos cambios
17		Rehace los últimos cambios revertidos
18	L3	Con el combo puede elegir una madurez para las *Salvaguardas / Valoración / Operaciones*
19	operación	Ver "*Salvaguardas / Valoración / Operaciones*".
20	sugiere	Ver "*Salvaguardas / Sugiere*".
21	find	Ver "*Salvaguardas / Buscar*".
22	>>	Ver "*Salvaguardas / Buscar*".

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

11.8.8. VALORACIÓN POR ACTIVOS

Esta pantalla permite el especificar si la evaluación de las salvaguardas se va a hacer de forma común para todos los activos del dominio, o si vamos a hacer alguna evaluación singular para algún activo.



1	activos	Árbol de activos
2		COLOREADO – el activo tiene valores de madurez propios VACÍO – no tiene valores propios ON - PILAR usa los valores específicos VACÍO – PILAR usa los valores del dominio Por defecto, los valores propios están deshabilitados. Incluso si se especifican, COLOREADO, PILAR los ignora hasta que se activan (ON). Haga clic para activar (on) / desactivar ().
3	editar	Haga clic para editar valores de madurez específicos del activo
4		Haga clic para colapsar el árbol [1] a nivel de capas

5	– 1 +	Para controlar el despliegue del árbol [1]

Cuando va a EDITAR ([2]), PILAR presenta 2 pestañas:

— la pestaña etiquetada con el nombre del activo presenta los valores específicos del activo
— la pestaña etiquetada con el nombre del dominio presenta los valores comunes del dominio (es la misma que cuando evalúa salvaguardas por dominio
— la fase PILAR siempre se refiere al dominio

El panel para editar los valores específicos de un activo sólo presenta los valores propios en los que el activo difiere del dominio. Si la salvaguarda no tiene hijos (refinamiento), queda en blanco. Si tiene hijos y algún hijo tiene valores propios, presenta "---". Ver "*Valoración de salvaguardas por dominios*".

11.8.9. 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

11.8.10. 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 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 "*Opciones / Salvaguardas no evaluadas*".

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

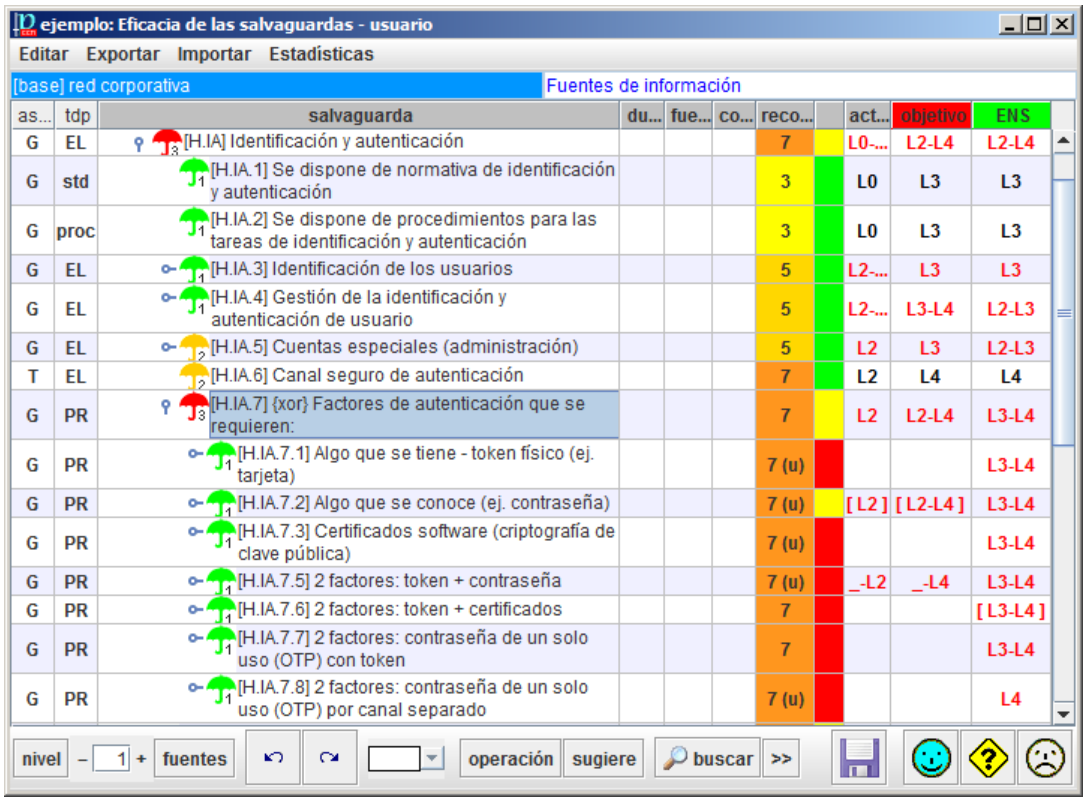
- haga clic con el botón derecho y elija un valor
- seleccione una madurez en el combo [18] y use alguna de las operaciones en "*Salvaguardas / Valoración / Operaciones*

— puede usar las operaciones copiar y pegar del menú EDITAR ([01]) para trasladar el valor de unas celdas a otras

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:



as...	tdp	salvaguarda	du...	fue...	co...	reco...	act...	objetivo	ENS
G	EL	[H.IA] Identificación y autenticación				7	L0-...	L2-L4	L2-L4
G	std	[H.IA.1] Se dispone de normativa de identificación y autenticación				3	L0	L3	L3
G	proc	[H.IA.2] Se dispone de procedimientos para las tareas de identificación y autenticación				3	L0	L3	L3
G	EL	[H.IA.3] Identificación de los usuarios				5	L2-...	L3	L3
G	EL	[H.IA.4] Gestión de la identificación y autenticación de usuario				5	L2-...	L3-L4	L2-L3
G	EL	[H.IA.5] Cuentas especiales (administración)				5	L2	L3	L2-L3
T	EL	[H.IA.6] Canal seguro de autenticación				7	L2	L4	L4
G	PR	[H.IA.7] {xor} Factores de autenticación que se requieren:				7	L2	L2-L4	L3-L4
G	PR	[H.IA.7.1] Algo que se tiene - token físico (ej. tarjeta)				7 (u)			L3-L4
G	PR	[H.IA.7.2] Algo que se conoce (ej. contraseña)				7 (u)	[L2]	[L2-L4]	L3-L4
G	PR	[H.IA.7.3] Certificados software (criptografía de clave pública)				7 (u)			L3-L4
G	PR	[H.IA.7.5] 2 factores: token + contraseña				7 (u)	_-L2	_-L4	L3-L4
G	PR	[H.IA.7.6] 2 factores: token + certificados				7			[L3-L4]
G	PR	[H.IA.7.7] 2 factores: contraseña de un solo uso (OTP) con token				7			L3-L4
G	PR	[H.IA.7.8] 2 factores: contraseña de un solo uso (OTP) por canal separado				7 (u)			L4

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

11.8.11. 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

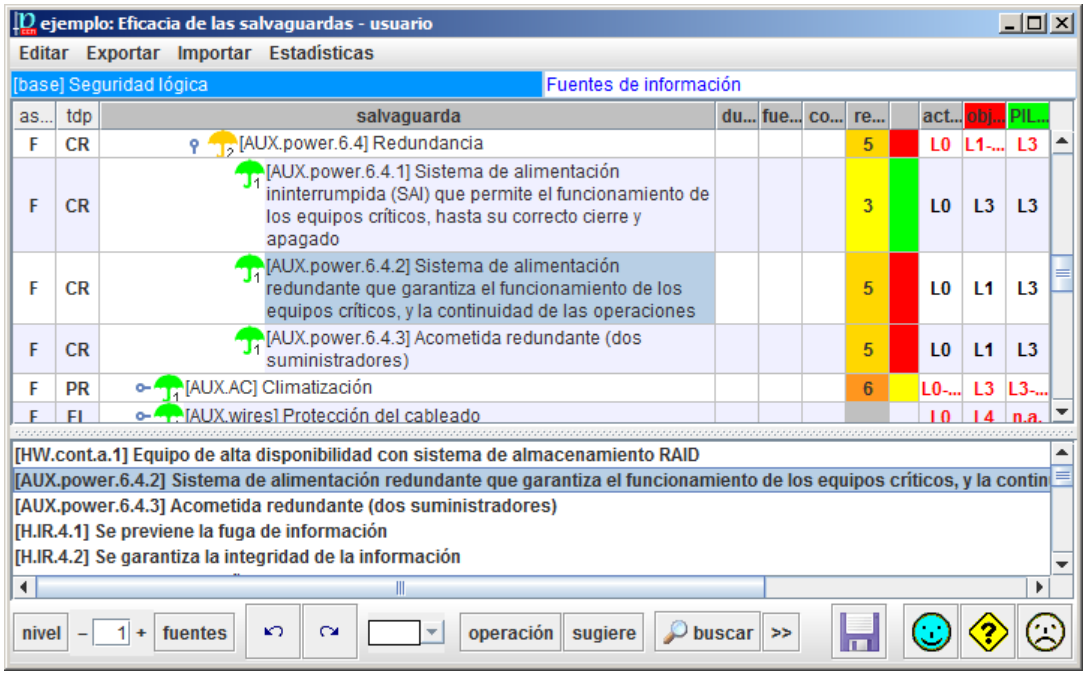
teniendo en cuenta la recomendación, PILAR sugiere unos valores de madurez que considera mínimos para satisfacer las necesidades del sistema. Meramente heurístico, con ánimo de marcar una referencia por debajo de la cual no se debería operar el sistema

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

11.8.12. 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.



11.8.13. 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

11.8.14. NORMATIVA DE SEGURIDAD

Es una vista reducida de las salvaguardas. PILAR sólo presenta las marcadas como normativa (std).

Ver "*Valoración de salvaguardas por dominios*".

11.8.15. PROCEDIMIENTOS OPERATIVOS DE SEGURIDAD

Es una vista reducida de las salvaguardas. PILAR sólo presenta las marcadas como procedimientos (proc).

Ver "*Valoración de salvaguardas por dominios*".

11.9. IMPACTO Y RIESGO

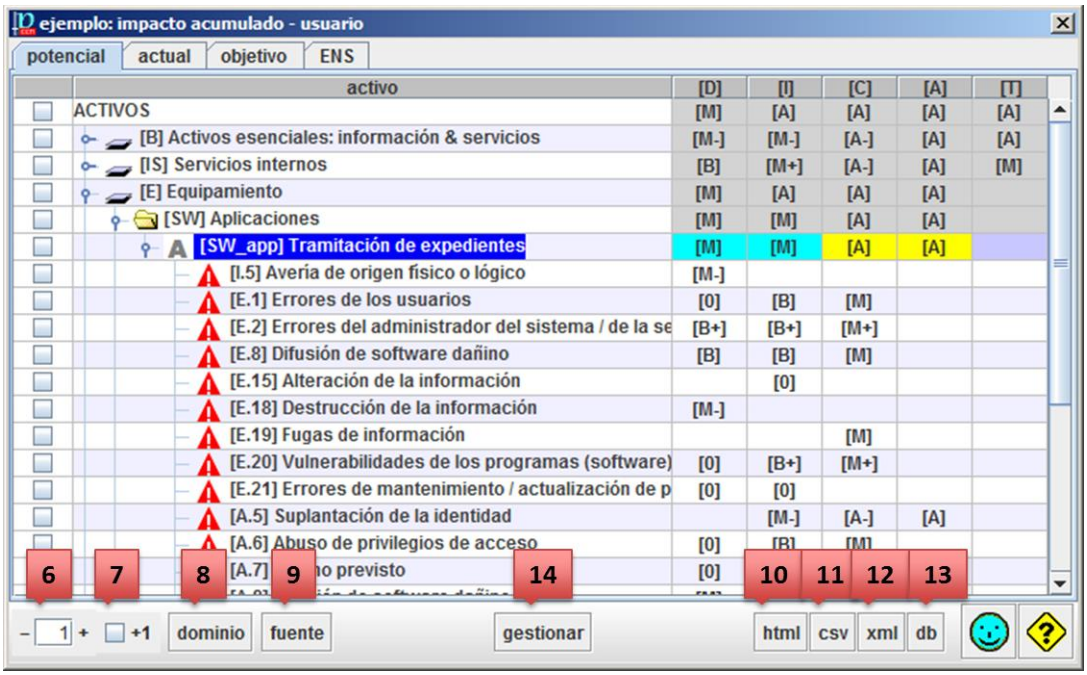
11.9.1. NIVELES DE CRITICIDAD – CÓDIGO DE COLORES

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

11.9.2. IMPACTO ACUMULADO

0	pestañas	Una por fase del proyecto. Haga clic para cambiar. La pseudo-fase POTENCIAL muestra el impacto 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	Árbol de activos y amenazas

3	dimensiones	Una columna por dimensión de seguridad. Haga clic en la cabecera para tener una *vista alternativa*, por dimensión.
5		Valores de impacto. El impacto se evalúa en cada amenaza y se agrega por activos, grupos de activos, capas y proyecto.



6	− 1 +	Para controlar el despliegue del árbol de activos.
7	+1	Ajusta la expansión de [6]. Si se marca, se incluyen las amenazas en el árbol.
8	dominio	Seleccione un dominio de seguridad. PILAR seleccionará los activos ([4]) en ese dominio.
9	fuente	Seleccione una o más fuentes de información. PILAR seleccionará los activos ([4]) asociados a esa fuente.
10	html	Exporta los datos a un fichero HTML
11	csv	Exporta los datos a un fichero CSV

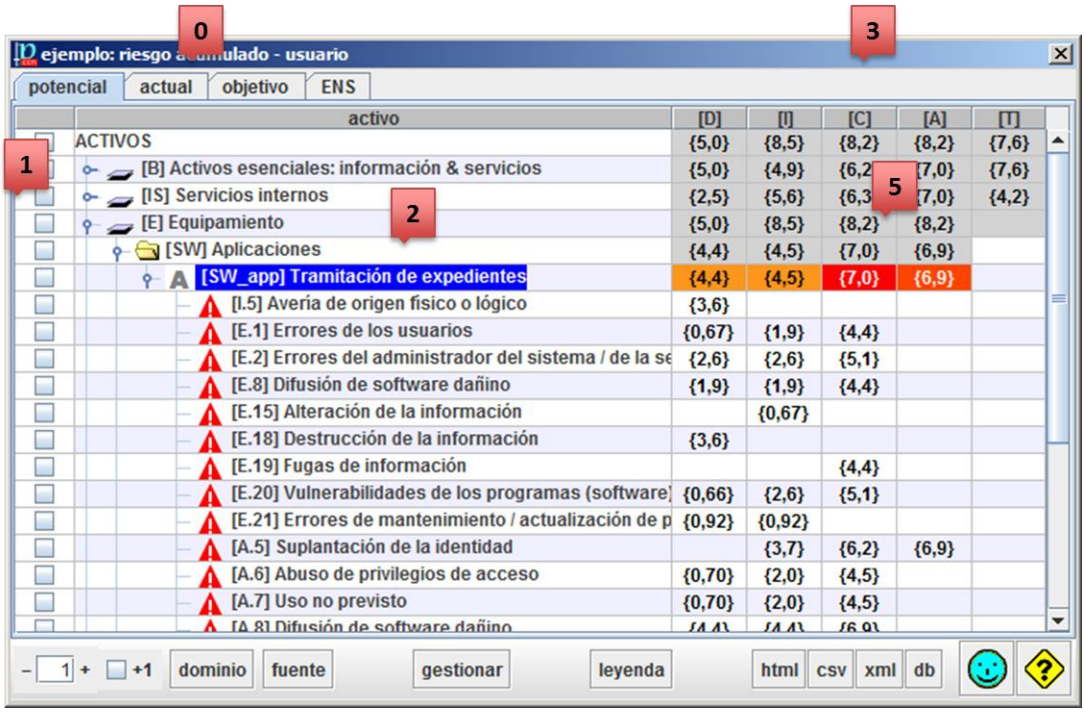
12	xml	Exporta los datos a un fichero XML
13	db	Exporta los datos a una base de datos. Sólo parece si la licencia habilita el uso de bases de datos SQL.
14	gestionar	Para las filas seleccionadas ([1]), PILAR recolecta los riesgos asociados y salta a la ventana de *valoración de salvaguardas*, teniendo en cuenta sólo dichos riesgos.

11.9.2.1. VISTA ALTERNATIVA

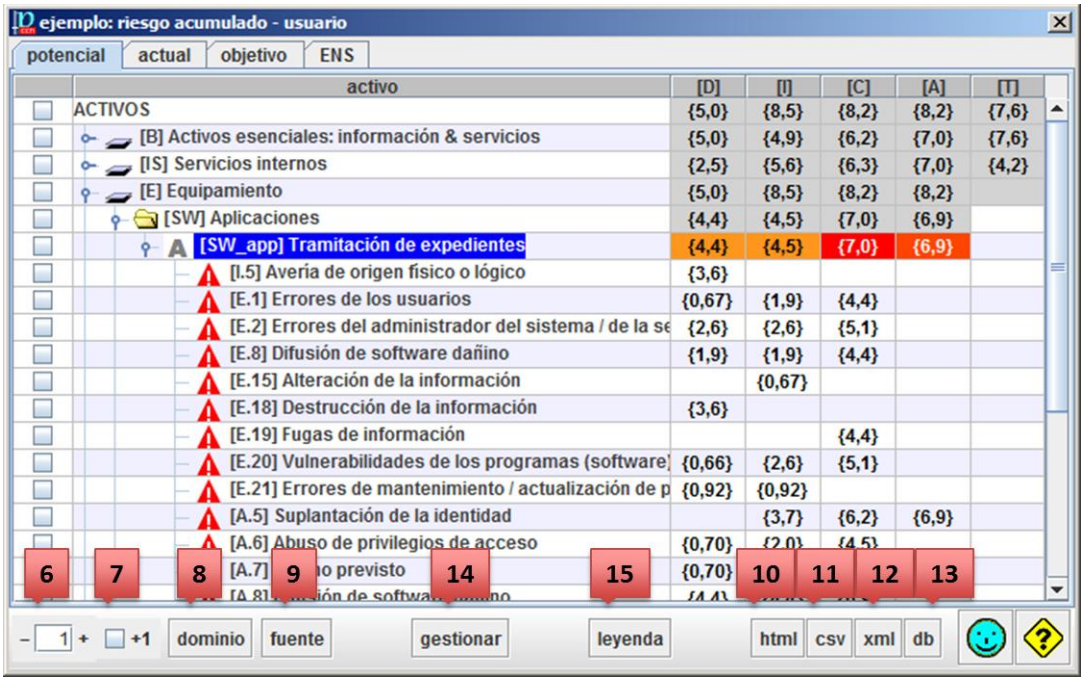
Si hace clic en la cabecera de una columna, PILAR conmuta entre columnas y pestañas:

0	Una columna por fase. Para regresar a la otra vista, haga clic en la cabecera de una columna.
3	Una pestaña por dimensión de seguridad. Haga clic para presentar una u otra dimensión.

11.9.3. RIESGO ACUMULADO



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	Árbol de activos y amenazas
3	dimensiones	Una columna por dimensión de seguridad. Haga clic en la cabecera para tener una *vista alternativa*, por dimensión.
5		Valores de riesgo. El riesgo se evalúa en cada amenaza y se agrega por activos, grupos de activos, capas y proyecto.

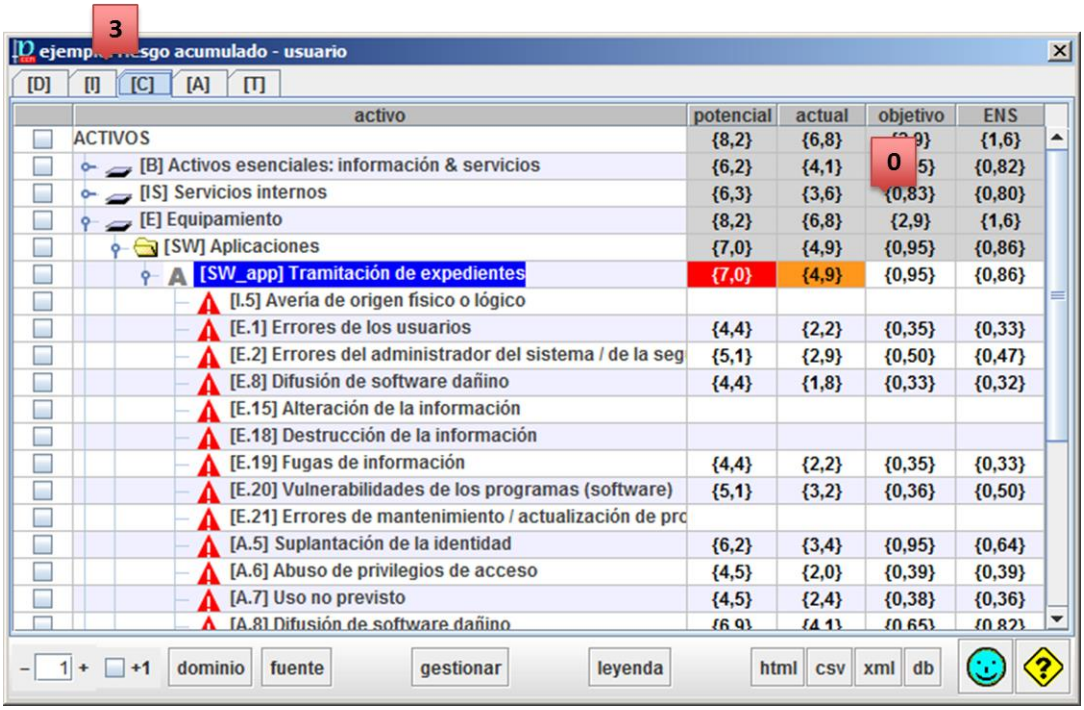


6	− 1 +	Para controlar el despliegue del árbol de activos.
7	+1	Ajusta la expansión de [6]. Si se marca, se incluyen las amenazas en el árbol.
8	dominio	Seleccione un dominio de seguridad. PILAR seleccionará los activos ([4]) en ese dominio.
9	fuente	Seleccione una o más fuentes de información. PILAR seleccionará los activos ([4]) asociados a esa fuente.
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
13	db	Exporta los datos a una base de datos. Sólo parece si la licencia habilita el uso de bases de datos SQL.
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*

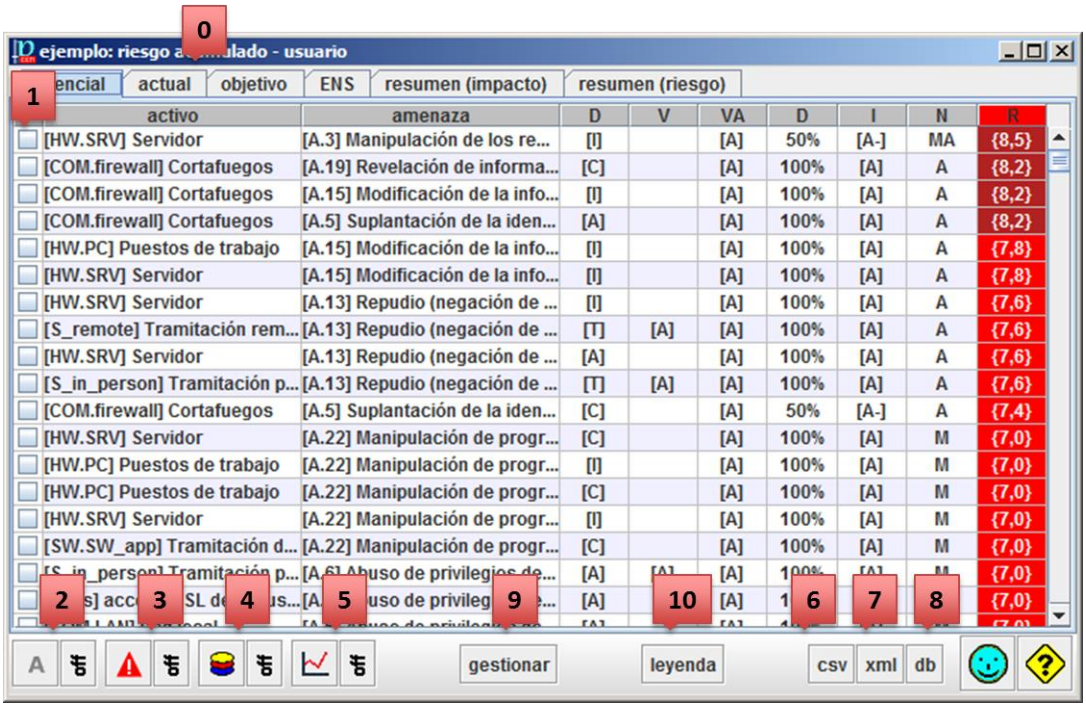
11.9.3.1. VISTA ALTERNATIVA

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



0	Una columna por fase. Para regresar a la otra vista, haga clic en la cabecera de una columna.
3	Una pestaña por dimensión de seguridad. Haga clic para presentar una u otra dimensión.

11.9.4. TABLA DE IMPACTO Y RIESGO ACUMULADO



0	pestañas	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)*
1	columnas	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 / Degradación*") I – el impacto N – la probabilidad (ver *Opciones / Probabilidad* R – el riesgo
2	A off	Filtro de activos: sólo se presentan los activos seleccionados. Haga clic en la imagen para seleccionar activos. Haga clic en ON / OFF para activar / desactivar el filtro.

3		Filtro de amenazas: sólo se presentan las amenazas seleccionadas. Haga clic en la imagen para seleccionar amenazas. Haga clic en ON / OFF para activar / desactivar el filtro.
4		Filtro de dimensiones: sólo se presentan las dimensiones seleccionadas. Haga clic en la imagen para seleccionar dimensiones. Haga clic en ON / OFF para activar / desactivar el filtro.
5		Filtro para ver sólo 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) impacto 10% probabilidad 10% 0% implica no ver ninguno. 100% sería como eliminar el filtro. Haga clic en ON / OFF para activar / desactivar el filtro.
6	csv	Exporta los valores a un fichero CSV
7	xml	Exporta los valores a un fichero XML
8	db	Exporta los valores a una base de datos SQL (sólo si la licencia habilita bases de datos SQL)
9	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.
10	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)

11.9.4.1. RESUMEN DE IMPACTO

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

ejemplo: riesgo acumulado - usuario

potencial | actual | objetivo | ENS | resumen (impacto) | resumen (riesgo)

activo	amenaza	dimensi...	impacto	actual	objetivo	ENS
[HW.SRV] Servidor	[A.22] Manipulación de programas	[C]	[A]	[A-]	[B+]	[B+]
[HW.PC] Puestos de trabajo	[A.25] Robo de equipos	[C]	[A]	[A-]	[B+]	[B+]
[HW.SRV] Servidor	[A.8] Difusión de software dañino	[I]	[A]	[M+]	[B]	[B+]
[HW.SRV] Servidor	[A.8] Difusión de software dañino	[C]	[A]	[A-]	[B]	[B]
[HW.PC] Puestos de trabajo	[A.22] Manipulación de programas	[I]	[A]	[A-]	[B+]	[B+]
[HW.PC] Puestos de trabajo	[A.22] Manipulación de programas	[C]	[A]	[A-]	[B+]	[B+]
[HW.SRV] Servidor	[A.22] Manipulación de programas	[I]	[A]	[A-]	[B+]	[B+]
[COM.LAN] Red local	[A.5] Suplantación de la identidad	[A]	[A]	[M+]	[B]	[B+]
[archive] Archivo histórico central	[A.11] Acceso no autorizado	[A]	[A]	[M]	[B]	[B]
[SW.SW_app] Tramitación de ex...	[A.22] Manipulación de programas	[C]	[A]	[M+]	[B+]	[B+]
[S_in_person] Tramitación pres...	[A.6] Abuso de privilegios de acc...	[A]	[A]	[M+]	[B]	[B+]
[HW.PC] Puestos de trabajo	[A.5] Suplantación de la identidad	[A]	[A]	[M+]	[M-]	[B]
[https] acceso SSL de los usuari...	[A.6] Abuso de privilegios de acc...	[A]	[A]	[M+]	[B+]	[B+]
[SW.SW_app] Tramitación de ex...	[A.8] Difusión de software dañino	[C]	[A]	[A-]	[B]	[B+]
[archive] Archivo histórico central	[A.5] Suplantación de la identidad	[A]	[A]	[M]	[B+]	[B+]
[COM.LAN] Red local	[A.6] Abuso de privilegios de acc...	[A]	[A]	[A-]	[B]	[B+]
[S_in_person] Tramitación pres...	[A.5] Suplantación de la identidad	[A]	[A]	[M+]	[M-]	[B]
[SW.SW_app] Tramitación de ex...	[A.5] Suplantación de la identidad	[A]	[A]	[M+]	[M-]	[B]

A | off | off | off | off | gestionar | leyenda | csv | xml | db

11.9.4.2. RESUMEN DE RIESGO

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

ejemplo: riesgo acumulado - usuario

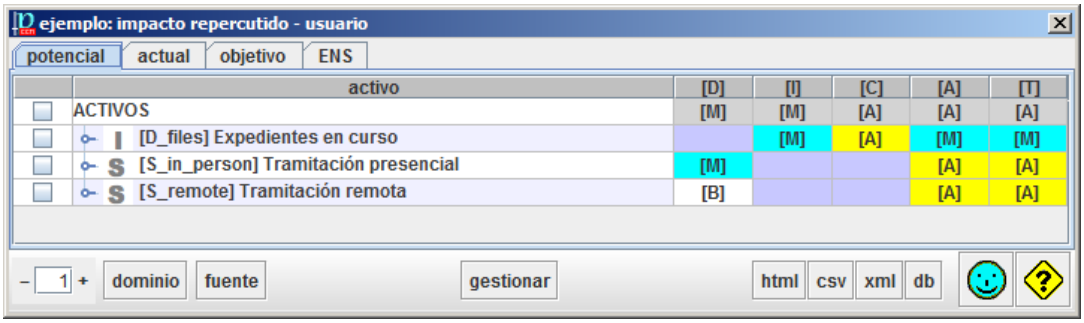
potencial | actual | objetivo | ENS | resumen (impacto) | resumen (riesgo)

activo	amenaza	dimensi...	riesgo	actual	objetivo	ENS
[HW.SRV] Servidor	[A.3] Manipulación de los registr...	[I]	{8,5}	{6,9}	{2,5}	{2,2}
[COM.firewall] Cortafuegos	[A.19] Revelación de información	[C]	{8,2}	{6,8}	{2,9}	{1,6}
[COM.firewall] Cortafuegos	[A.15] Modificación de la informa...	[I]	{8,2}	{6,6}	{2,0}	{1,7}
[COM.firewall] Cortafuegos	[A.5] Suplantación de la identidad	[A]	{8,2}	{5,9}	{3,7}	{1,3}
[HW.PC] Puestos de trabajo	[A.15] Modificación de la informa...	[I]	{7,8}	{6,3}	{1,9}	{1,4}
[HW.SRV] Servidor	[A.15] Modificación de la informa...	[I]	{7,8}	{6,2}	{1,8}	{1,5}
[HW.SRV] Servidor	[A.13] Repudio (negación de act...	[I]	{7,6}	{6,7}	{0,90}	{1,1}
[S_remote] Tramitación remota	[A.13] Repudio (negación de act...	[T]	{7,6}	{4,8}	{0,83}	{1,1}
[HW.SRV] Servidor	[A.13] Repudio (negación de act...	[A]	{7,6}	{6,7}	{0,90}	{1,1}
[S_in_person] Tramitación pres...	[A.13] Repudio (negación de act...	[T]	{7,6}	{4,8}	{0,83}	{1,1}
[COM.firewall] Cortafuegos	[A.5] Suplantación de la identidad	[C]	{7,4}	{5,0}	{2,7}	{0,90}
[HW.SRV] Servidor	[A.22] Manipulación de programas	[C]	{7,0}	{5,8}	{1,7}	{0,91}
[HW.PC] Puestos de trabajo	[A.22] Manipulación de programas	[I]	{7,0}	{5,6}	{1,1}	{0,92}
[HW.PC] Puestos de trabajo	[A.22] Manipulación de programas	[C]	{7,0}	{5,8}	{1,7}	{0,90}
[HW.SRV] Servidor	[A.22] Manipulación de programas	[I]	{7,0}	{5,5}	{1,1}	{0,94}
[SW.SW_app] Tramitación de ex...	[A.22] Manipulación de programas	[C]	{7,0}	{4,9}	{0,94}	{0,86}
[S_in_person] Tramitación pres...	[A.6] Abuso de privilegios de acc...	[A]	{7,0}	{4,8}	{0,86}	{1,0}
[https] acceso SSL de los usuari...	[A.6] Abuso de privilegios de acc...	[A]	{7,0}	{4,5}	{0,96}	{0,95}

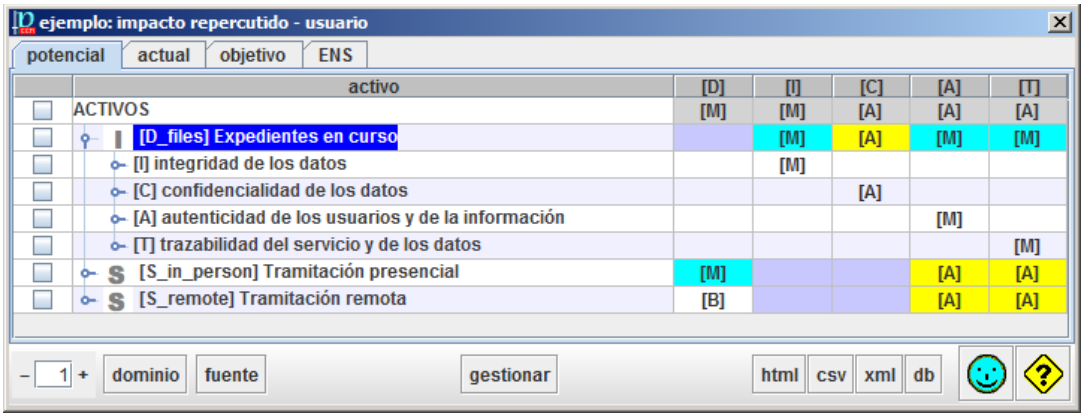
A | off | off | off | off | gestionar | leyenda | csv | xml | db

11.9.5. IMPACTO REPERCUTIDO

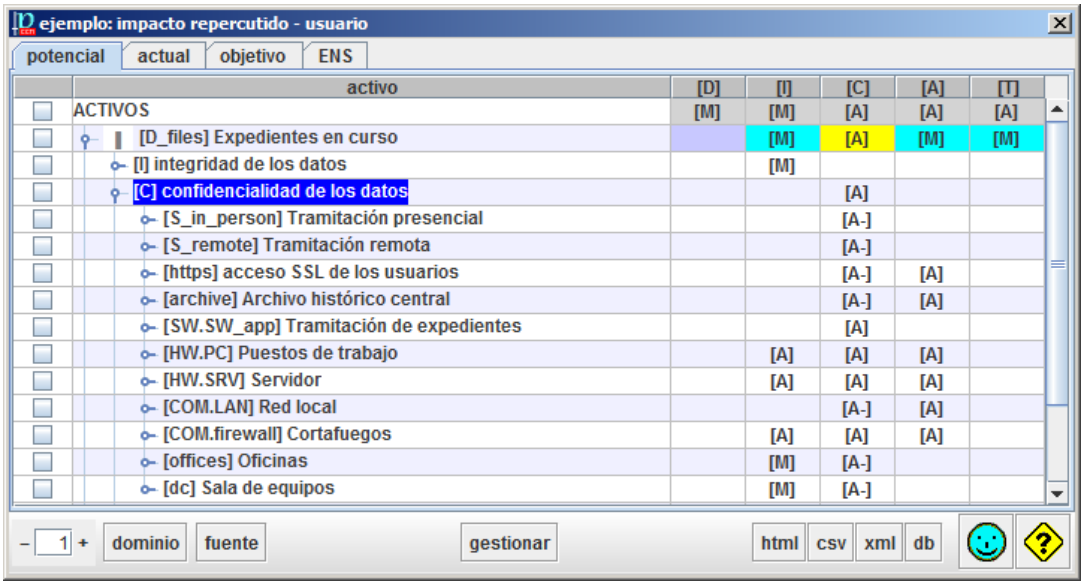
PILAR presenta el impacto repercutido sobre los activos con valor propio:



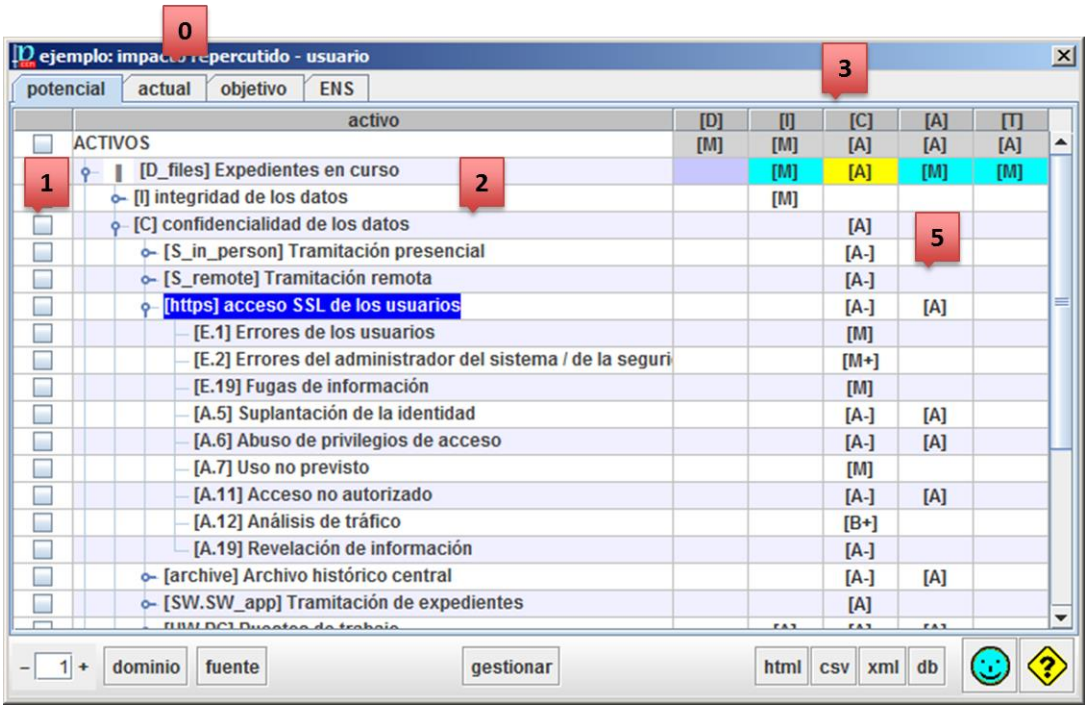
Puede expandir el árbol para segregar cada dimensión:



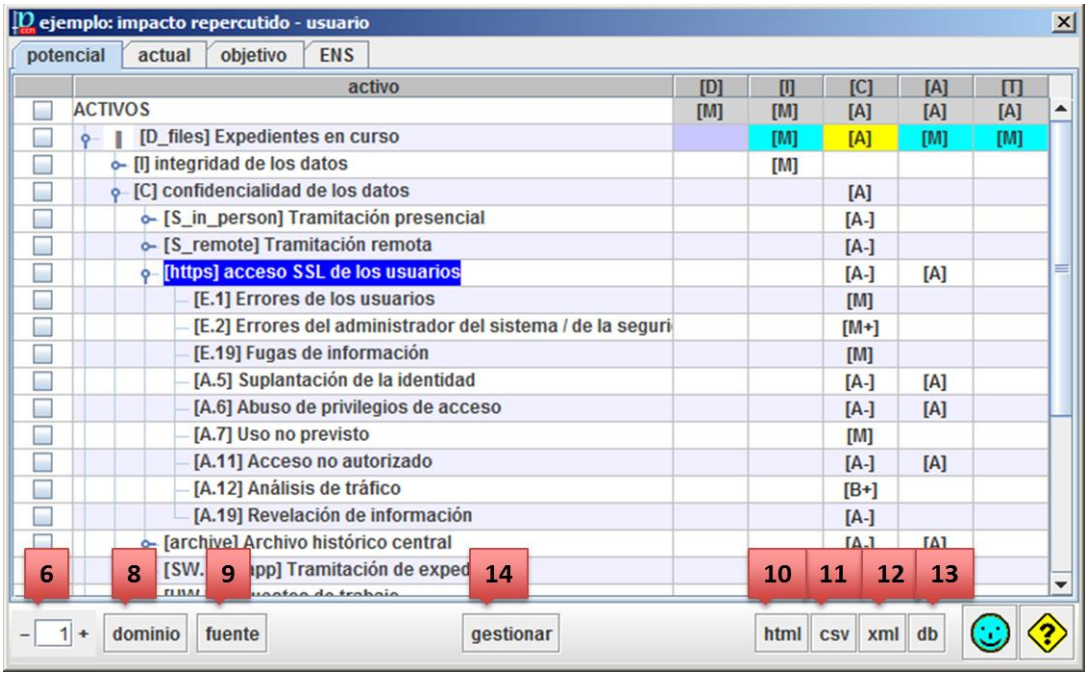
Puede seguir expandiendo el árbol para ver cómo es afectada cada dimensión en los activos de los que depende:



Y puede llegar a amenazas concretas:



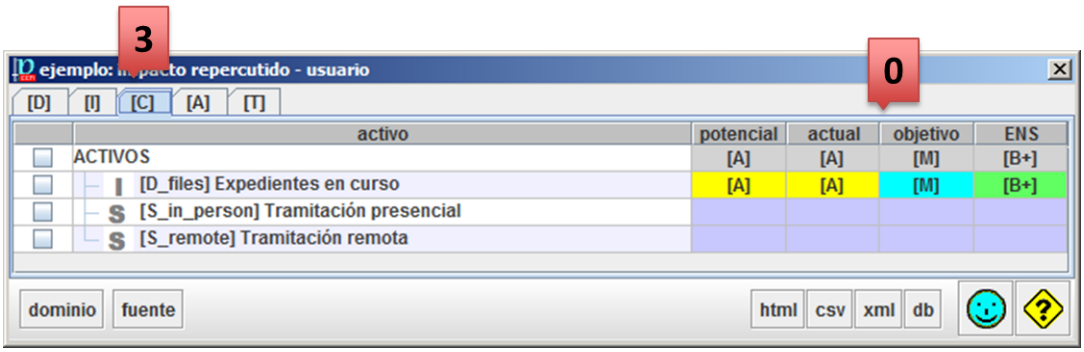
0	pestañas	Una por fase del proyecto. Haga clic para cambiar. La pseudo-fase POTENCIAL muestra el riesgo potencial (sin salvaguarda alguna).
1	selección	Haga clic en las cajitas para seleccionar / deseleccionar. Haga MAYÚSCULAS+clic para seleccionar un rango. Haga clic en la cabecera de la columna para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



6	− 1 +	Para controlar el despliegue del árbol
8	dominio	Seleccione un dominio de seguridad. PILAR seleccionará los activos ([2]) en ese dominio.
9	fuente	Seleccione una o más fuentes de información. PILAR seleccionará los activos ([2]) asociados a esa fuente.
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
13	db	Exporta los datos a una base de datos. Sólo parece si la licencia habilita el uso de bases de datos SQL.
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.

11.9.5.1. VISTA ALTERNATIVA

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

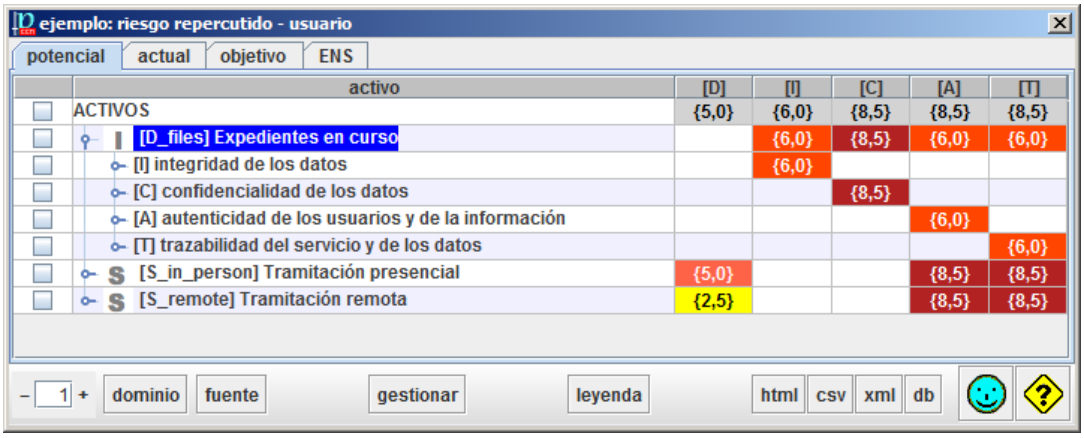


0	Una columna por fase. Para regresar a la otra vista, haga clic en la cabecera de una columna.
3	Una pestaña por dimensión de seguridad. Haga clic para presentar una u otra dimensión.

11.9.6. RIESGO REPERCUTIDO

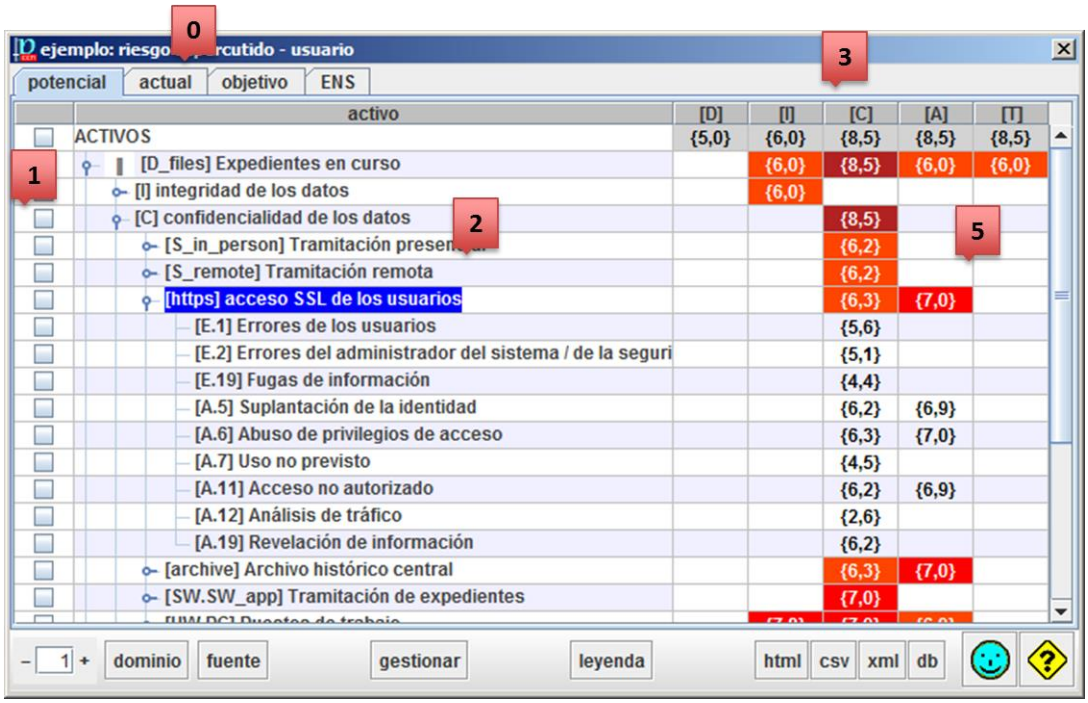
PILAR presenta el riesgo repercutido sobre los activos con valor propio:

Puede expandir el árbol para segregar cada dimensión:

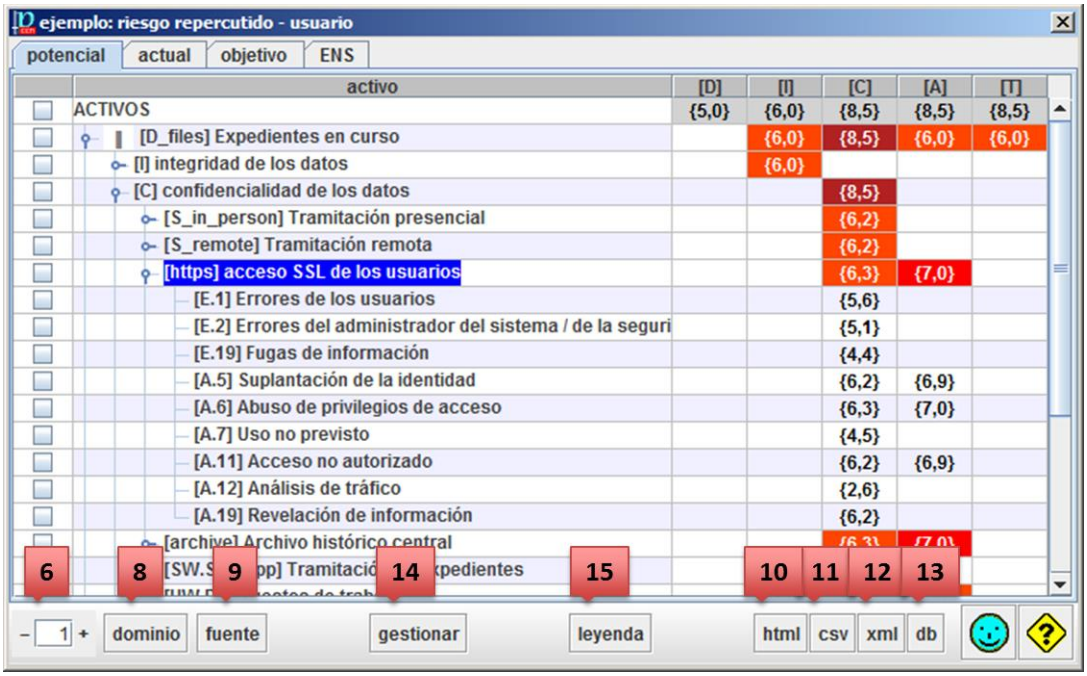


Puede seguir expandiendo el árbol para ver cómo es afectada cada dimensión en los activos de los que depende:

Y puede llegar a amenazas concretas:



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	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
2	dimensiones	Una columna por dimensión de seguridad. Haga clic en la cabecera para tener una *vista alternativa*, por dimensión.
5		Valores de riesgo



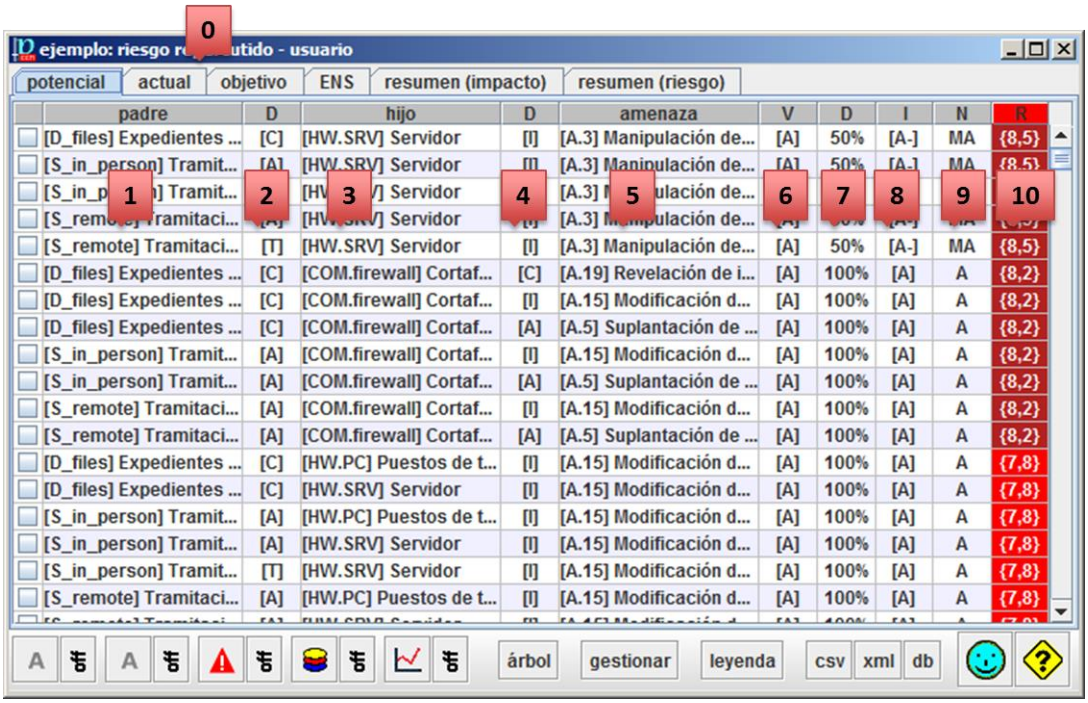
6	− 1 +	Para controlar el despliegue del árbol
8	dominio	Seleccione un dominio de seguridad. PILAR seleccionará los activos ([4]) en ese dominio.
9	fuente	Seleccione una o más fuentes de información. PILAR seleccionará los activos ([4]) asociados a esa fuente.
10	html	Exporta los datos a un fichero HTML
11	csv	Exporta los datos a un fichero CSV
12	xml	Exporta los datos a un fichero XML
13	db	Exporta los datos a una base de datos. Sólo parece si la licencia habilita el uso de bases de datos SQL.
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*

11.9.6.1. VISTA ALTERNATIVA

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

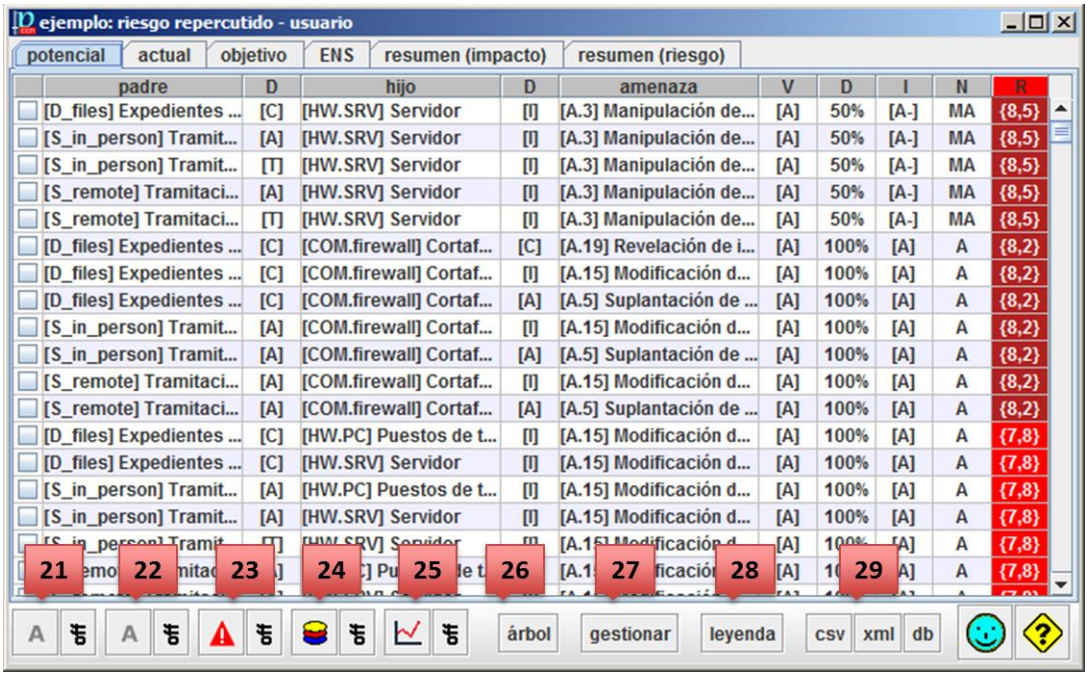
0	Una columna por fase. Para regresar a la otra vista, haga clic en la cabecera de una columna.
3	Una pestaña por dimensión de seguridad. Haga clic para presentar una u otra dimensión.

11.9.7. TABLA DE IMPACTO Y RIESGO REPERCUTIDO



0	pestañas	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)*
1	padre	El activo superior sobre el que repercute la amenaza
2	dimensión superior	Dimensión en la que repercute la amenaza
3	hijo	El activo inferior, sobre el que se materializa la amenaza
4	dimensión inferior	La dimensión afectada directamente por la amenaza
5	amenaza	La amenaza
6	valor	El valor del activo superior ([1]) en la dimensión superior ([2])
7	degradación	Degradación causada por la amenaza [5] en la dimensión [4] del activo [3]
8	impacto	Impacto de la amenaza [5] en la dimensión [2] del activo superior ([1])
9	probabilidad	Probabilidad de la amenaza [5] sobre el activo [3]. La cabecera se denomina según *Opciones / Probabilidad*
10	risk	Riesgo de la amenaza [5] en la dimensión [2] del activo superior ([1])



21		Filtro de activos superiores: sólo se presentan los activos seleccionados. Haga clic en la imagen para seleccionar activos. Haga clic en ON / OFF para activar / desactivar el filtro.
21		Filtro de activos inferiores: sólo se presentan los activos seleccionados. Haga clic en la imagen para seleccionar activos. Haga clic en ON / OFF para activar / desactivar el filtro.
23		Filtro de amenazas: sólo se presentan las amenazas seleccionadas. Haga clic en la imagen para seleccionar amenazas. Haga clic en ON / OFF para activar / desactivar el filtro.
24		Filtro de dimensiones: sólo se presentan las dimensiones seleccionadas. Haga clic en la imagen para seleccionar dimensiones. Haga clic en ON / OFF para activar / desactivar el filtro.
25		Filtro para ver sólo 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)

		impacto 10% probabilidad 10% 0% implica no ver ninguno. 100% sería como eliminar el filtro. Haga clic en ON / OFF para activar / desactivar el filtro.
26	árbol	
27	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.
28	leyenda	Ver *Riesgos / Niveles de criticidad / código de colores*
29	csv xml db	Exporta los datos a un fichero CSV. Exporta los datos a un fichero XML. Exporta los datos a una base de datos (si la licencia habilita SQL).

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.

11.9.7.1. RESUMEN DE IMPACTO

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

ejemplo: riesgo repercutido - usuario

potencial | actual | objetivo | ENS | resumen (impacto) | resumen (riesgo)

padre	D	hijo	D	amenaza	V	D	I	N	R
[D_files] Expedientes ...	[C]	[HW.SRV] Servidor	[I]	[A.3] Manipulación de...	[A]	50%	[A-]	MA	{8,5}
[S_in_person] Tramit...	[A]	[HW.SRV] Servidor	[I]	[A.3] Manipulación de...	[A]	50%	[A-]	MA	{8,5}
[S_in_person] Tramit...	[T]	[HW.SRV] Servidor	[I]	[A.3] Manipulación de...	[A]	50%	[A-]	MA	{8,5}
[S_remote] Tramitaci...	[A]	[HW.SRV] Servidor	[I]	[A.3] Manipulación de...	[A]	50%	[A-]	MA	{8,5}
[S_remote] Tramitaci...	[T]	[HW.SRV] Servidor	[I]	[A.3] Manipulación de...	[A]	50%	[A-]	MA	{8,5}
[D_files] Expedientes ...	[C]	[COM.firewall] Cortaf...	[C]	[A.19] Revelación de i...	[A]	100%	[A]	A	{8,2}
[D_files] Expedientes ...	[C]	[COM.firewall] Cortaf...	[I]	[A.15] Modificación d...	[A]	100%	[A]	A	{8,2}
[D_files] Expedientes ...	[C]	[COM.firewall] Cortaf...	[A]	[A.5] Suplantación de ...	[A]	100%	[A]	A	{8,2}
[S_in_person] Tramit...	[A]	[COM.firewall] Cortaf...	[I]	[A.15] Modificación d...	[A]	100%	[A]	A	{8,2}
[S_in_person] Tramit...	[A]	[COM.firewall] Cortaf...	[A]	[A.5] Suplantación de ...	[A]	100%	[A]	A	{8,2}
[S_remote] Tramitaci...	[A]	[COM.firewall] Cortaf...	[I]	[A.15] Modificación d...	[A]	100%	[A]	A	{8,2}
[S_remote] Tramitaci...	[A]	[COM.firewall] Cortaf...	[A]	[A.5] Suplantación de ...	[A]	100%	[A]	A	{8,2}
[D_files] Expedientes ...	[C]	[HW.PC] Puestos de t...	[I]	[A.15] Modificación d...	[A]	100%	[A]	A	{7,8}
[D_files] Expedientes ...	[C]	[HW.SRV] Servidor	[I]	[A.15] Modificación d...	[A]	100%	[A]	A	{7,8}
[S_in_person] Tramit...	[A]	[HW.PC] Puestos de t...	[I]	[A.15] Modificación d...	[A]	100%	[A]	A	{7,8}
[S_in_person] Tramit...	[A]	[HW.SRV] Servidor	[I]	[A.15] Modificación d...	[A]	100%	[A]	A	{7,8}
[S_in_person] Tramit...	[T]	[HW.SRV] Servidor	[I]	[A.15] Modificación d...	[A]	100%	[A]	A	{7,8}
[S_remote] Tramitaci...	[A]	[HW.PC] Puestos de t...	[I]	[A.15] Modificación d...	[A]	100%	[A]	A	{7,8}

árbol | gestionar | leyenda | csv | xml | db

11.9.7.2. RESUMEN DE RIESGO

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

ejemplo: riesgo repercutido - usuario

potencial | actual | objetivo | ENS | resumen (impacto) | resumen (riesgo)

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

árbol | gestionar | leyenda | csv | xml | db

12. PROTECCIONES ADICIONALES

Las protecciones adicionales son, en muchos aspectos, similares a las salvaguardas; pero no serán tomadas en consideración para evaluar el impacto y riesgo residuales.

12.1. EN EL ÁRBOL KB

Si hace clic con el botón derecho en alguna medida de protección de árbol de protecciones adicionales, se le presentan varias opciones …

copiar

copia en el portapapeles el nombre de la protección

copiar ruta

copia en el portapapeles el camino completo de la protección

texto completo

código y nombre de la protección

camino completo

muestra la protección 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

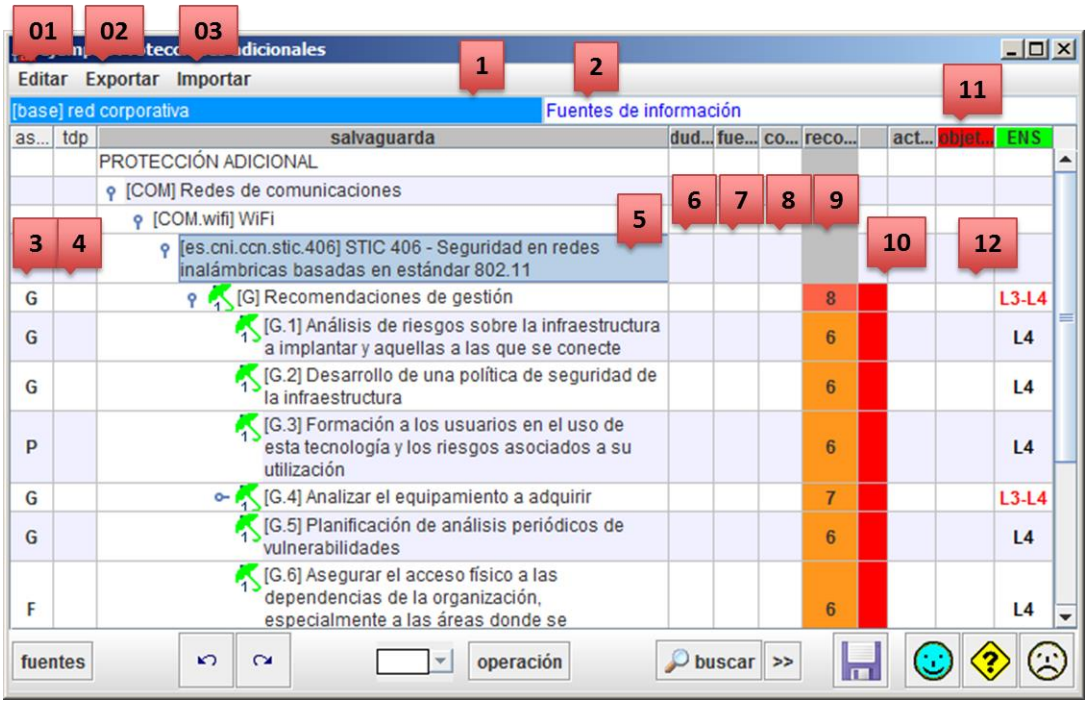
compacta el árbol, cerrando todos los hermanos del nodo seleccionado

más información

presenta información adicional sobre la salvaguarda.

Ver "*Salvaguardas / Información adicional*".

12.2. VALORACIÓN DEL ÁRBOL KB



01	editar copiar ⌘C pegar ⌘V buscar ⌘F	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 ... a CSV ... a XML informe	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)
03	importar	Lee los niveles de madures de un fichero, CSV o XML.
1	dominio de seguridad	Pueden haber diferentes medidas en diferentes dominios. Haga clic para seleccionar el dominio en el que vamos a trabajar.
2	fuentes de información	Haga clic para seleccionar fuentes de información. PILAR recortará el árbol [5] para mostrar sólo las asociadas a alguna de las fuentes de información marcadas.

3	aspecto	Ver "*Salvaguardas / Aspecto*".
4	tdp	Ver "*Salvaguardas / Tipo de protección*".
5		Árbol de medidas de protección. Haga clic-clic para colapsar / expandir el árbol. La primera filas presentan las clases de activos a las que afectan las medidas. Luego ya se concretan las medidas de protección propiamente dichas. Clic con el botón derecho para acceder a *KB / 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.
7	fuentes	Haga clic para asociar fuentes de información a la salvaguarda (la marcada y sus descendientes).
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 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.
10	semáforo	Ver "*Salvaguardas / Fases de referencia y objetivo*".
11		Fases del proyecto

12		Ver "*Valoración de salvaguardas por dominios*".

15	fuentes	Seleccione una o más fuentes de información. PILAR seleccionará todas las salvaguardas a las que está asociada.
16		Revierte los últimos cambios
17		Rehace los últimos cambios revertidos
18	L3	Con el combo puede elegir una madurez para las *Salvaguardas / Valoración / Operaciones*
19	operación	Ver "*Salvaguardas / Valoración / Operaciones*".
21	find	Ver "*Salvaguardas / Buscar*".
22	>>	Ver "*Salvaguardas / Buscar*".

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

12.3. PROTECCIONES PARA UN ACTIVO

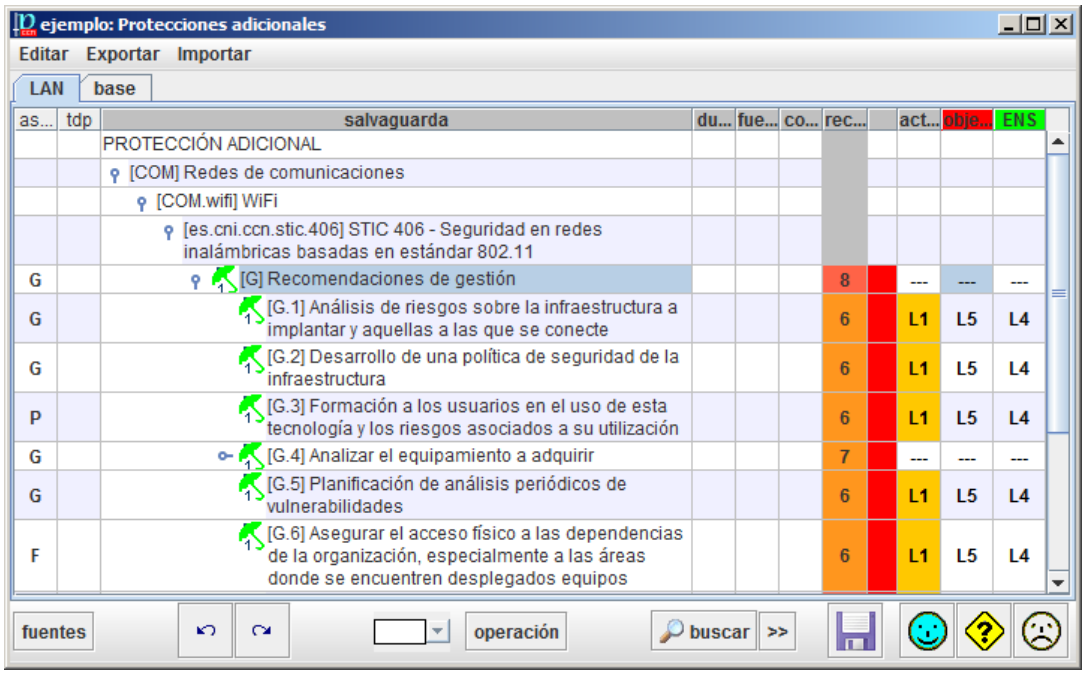
Puede especificar niveles de madurez específicos para activos individuales. Por defecto, las protecciones se evalúan por dominio, y cada activo hereda la valoración del dominio al que pertenece.

1	activos	Árbol de activos
2		ROJO – el activo tiene valores de madurez propios VACÍO – no tiene valores propios ON - PILAR usa los valores específicos VACÍO – PILAR usa los valores del dominio Por defecto, los valores propios están deshabilitados. Incluso si se especifican, ROJO, PILAR los ignora hasta que se activan (ON). Haga clic para activar (on) / desactivar ().
3	editar	Haga clic para editar valores de madurez específicos del activo
4		Haga clic para colapsar el árbol a nivel de capas
5	– 1 +	Para controlar el despliegue del árbol

Cuando va a EDITAR ([2]), PILAR presenta 2 pestañas:

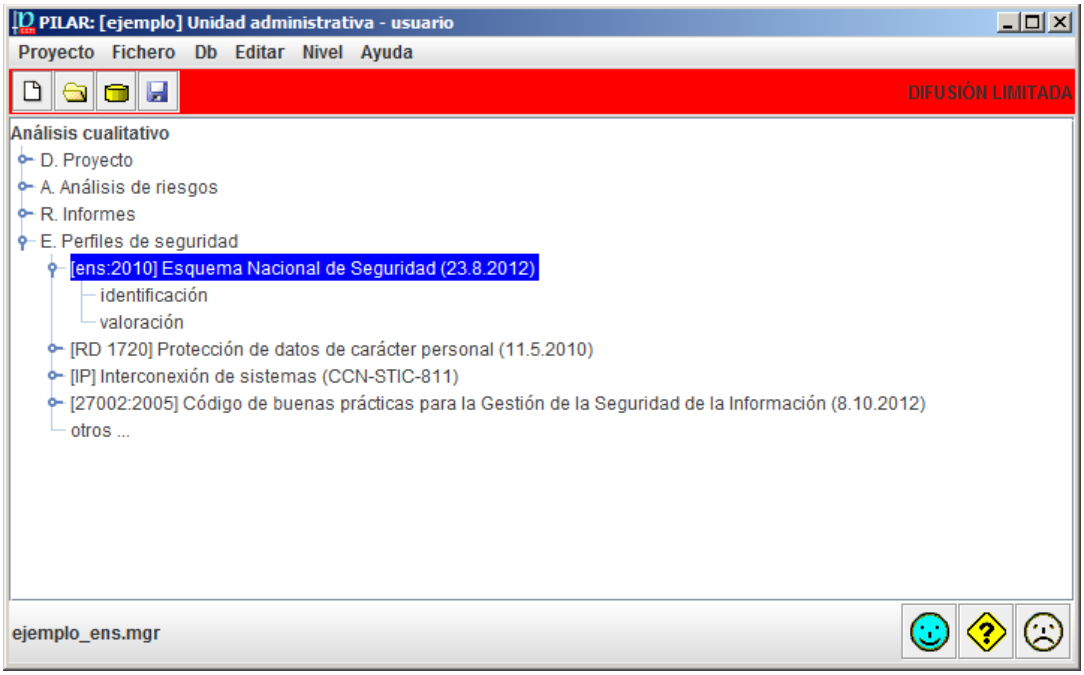
— la pestaña etiquetada con el nombre del activo presenta los valores específicos del activo
— la pestaña etiquetada con el nombre del dominio presenta los valores comunes del dominio (es la misma que cuando evalúa salvaguardas por dominio
— la fase ENS siempre se refiere al dominio

El panel para editar los valores específicos de un activo sólo presenta los valores propios en los que el activo difiere del dominio. Si la protección no tiene hijos (refinamiento), queda en blanco. Si tiene hijos y algún hijo tiene valores propios, presenta "---". Ver "*KB / Valoración / por dominio*".



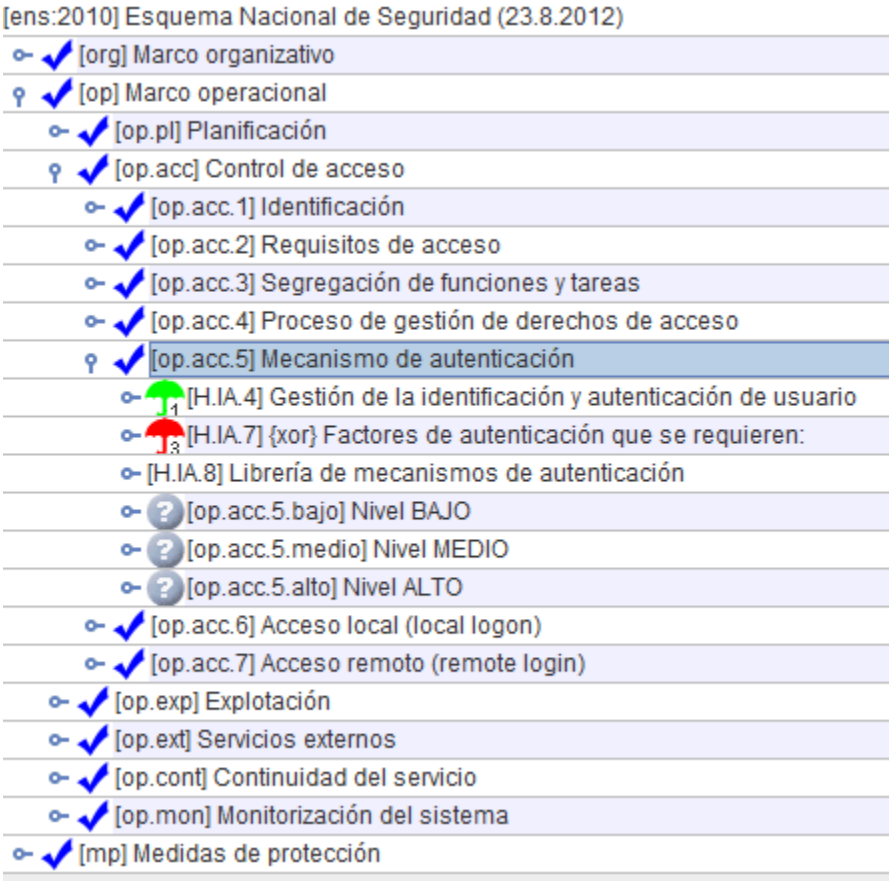
13. PERFILES DE SEGURIDAD

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

13.1. 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.

13.2. EVL – APLICABILIDAD

Para cada control ( ), cada pregunta ( ), y cada una de las salvaguardas ( ), se puede indicar si aplica o no.

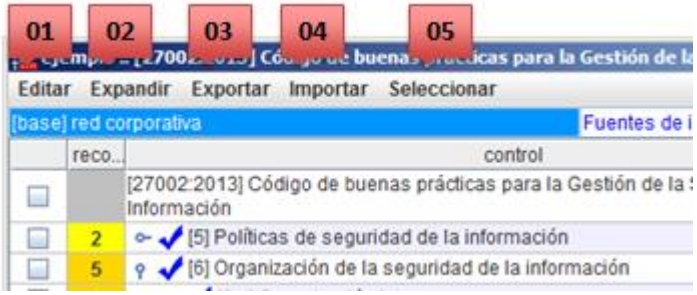
Todo es aplicable por defecto, hasta que se diga lo contrario. Se puede desactivar un control de varias formas:

- en la pantalla de identificación, teniendo como consecuencia que el control no aparecerá en las pantallas de valoración
- en las pantallas de valoración: el control aparece como n.a.

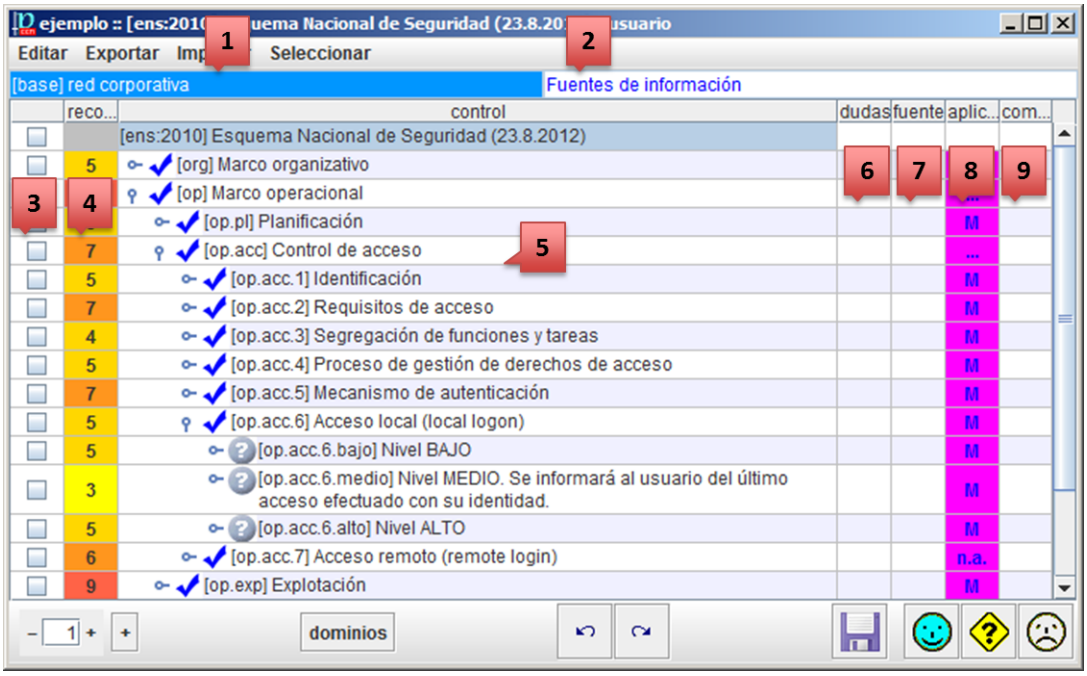
Los controles están conectados a las salvaguardas que los materializan. Un control puede estar conectado a varias salvaguardas y una salvaguarda puede estar conectada a varios controles. Es por ello que cuando se marca un control como n.a, la marca no se propaga automáticamente a las salvaguardas a las que se conecta. Y viceversa. Aunque PILAR intenta tomar decisiones sensatas, en general hay que marcar manualmente tanto las salvaguardas como los controles que son de aplicación.

La aplicabilidad de las salvaguardas es mejor establecerla en “*Identificación de salvaguardas*”.

13.3. EVL – IDENTIFICACIÓN

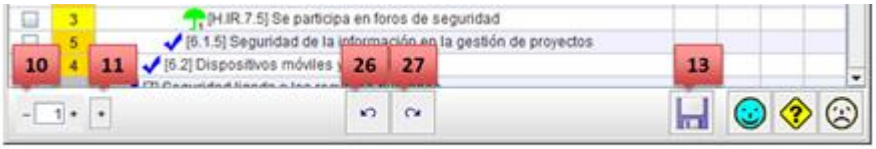


01	editar	buscar busca un cierto texto en el árbol [5] pregunta salta a la siguiente pregunta en el árbol [5]
02	expandir	Expande el árbol hasta el perímetro definido • hasta perímetros definidos en la biblioteca • hasta perfiles definidos por el usuario (ver *Perímetros*
03	exportar	CSV Las filas desplegadas se copian a un fichero CSV XML Los datos se copian a un fichero XML BASE DE DATOS (si la licencia habilita bases de datos SQL)) Los valores se copian a una base de datos INFORME Se genera un informe RTF o HTML SoA Se genera un informe "Declaración de Aplicabilidad)
04	importar	Carga los valores de un fichero CSV o XML o de otro proyecto en fichero o en base de datos. También se puede combinar los datos de este proyecto con los de otro (merge)
05	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 obligatorio Permite seleccionar los controles que son de obligado cumplimiento



1	dominio de seguridad	Pueden haber diferentes valores en diferentes dominios. Haga clic para seleccionar el dominio en el que vamos a trabajar.
2	fuentes de información	Haga clic para seleccionar fuentes de información. PILAR recortará el árbol [5] para mostrar sólo las asociadas a alguna de las fuentes de información marcadas.
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 al menú del árbol.

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.
7	fuentes	Haga clic para asociar fuentes de información a la salvaguarda (la marcada y sus descendientes).
8	aplica	Haga clic para conmutar. Ver *EVL / Aplicabilidad*
9	comentario	Haga clic para asociar un comentario a la salvaguarda.



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.
13		Guarda el proyecto en su fichero o en su base de datos.
26		Revierte los últimos cambios
27		Rehace los últimos cambios revertidos

13.4. 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.

En salvaguardas de tipo XOR, podemos indicar cual e s 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.

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

porcentje 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.

13.5. 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

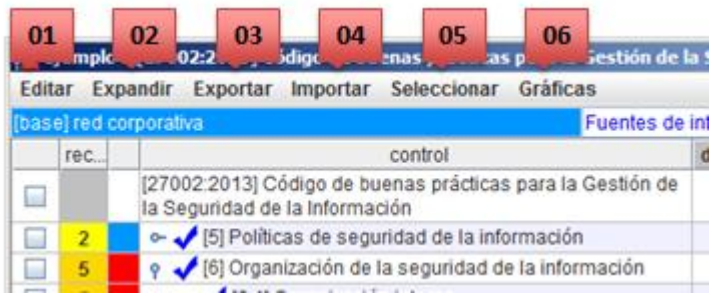
ROJA: la madurez evaluada

- 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:

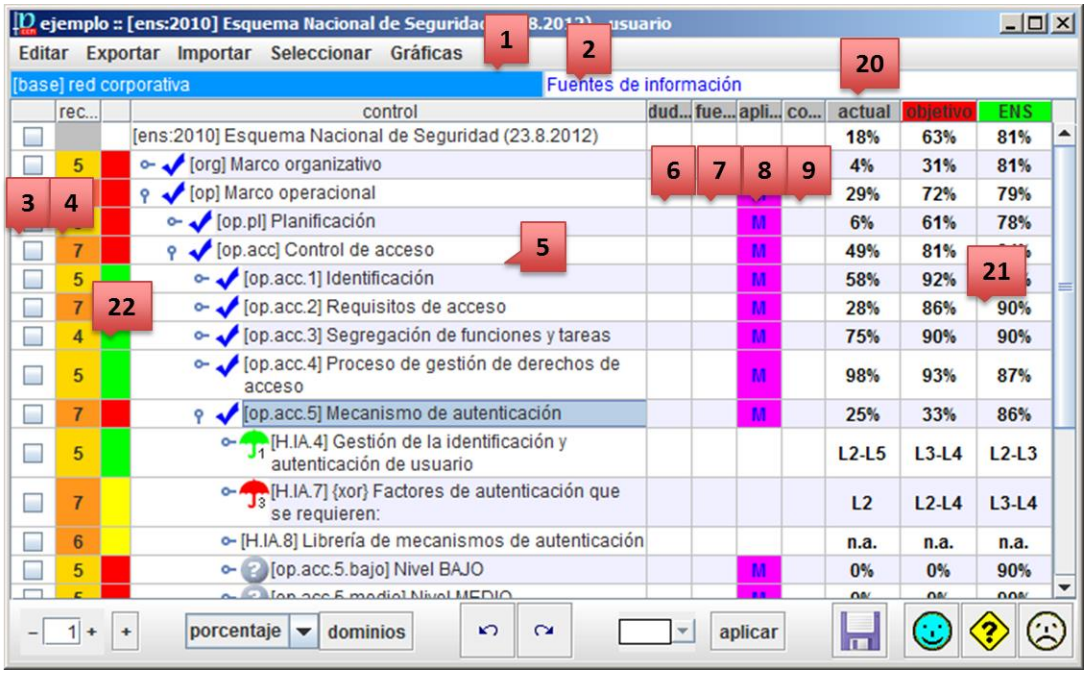
AZUL	la madurez actual (ROJA) está por encima del objetivo (VERDE)
VERDE	la madurez actual (ROJA) está a la altura del objetivo (VERDE)
AMARILLO	la madurez actual (ROJA) está por debajo del objetivo (VERDE)
ROJO	la madurez actual (ROJA) está muy por debajo del objetivo (VERDE)
GRIS	la salvaguarda no es aplicable

13.6. EVL - VALORACIÓN POR FASES



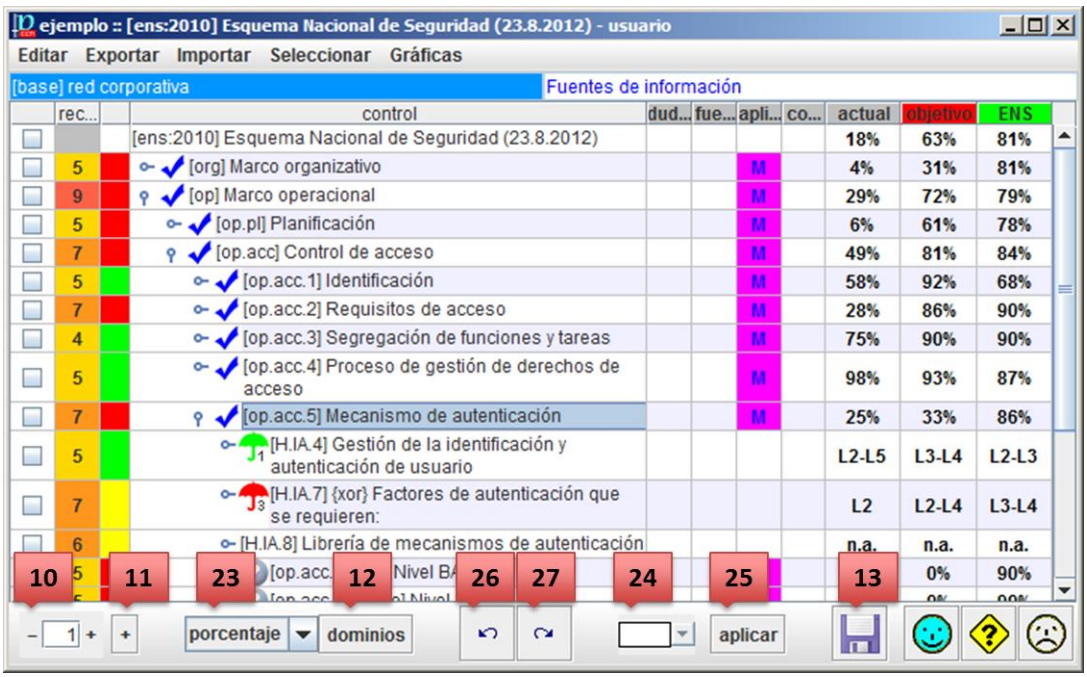
01	editar	buscar busca un cierto texto en el árbol [5] pregunta salta a la siguiente pregunta en el árbol [5]
02	expandir	Expande el árbol hasta el perímetro definido • hasta perímetros definidos en la biblioteca • hasta perfiles definidos por el usuario (ver *Perímetros*

03	exportar	CSV Las filas desplegadas se copian a un fichero CSV XML Los datos se copian a un fichero XML BASE DE DATOS (si la licencia habilita bases de datos SQL)) Los valores se copian a una base de datos INFORME Se genera un informe RTF o HTML SoA Se genera un informe “Declaración de Aplicabilidad)
04	importar	Carga los valores de un fichero CSV o XML
05	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
06	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.
2	fuentes de información	Haga clic para seleccionar fuentes de información. PILAR recortará el árbol [5] para mostrar sólo las asociadas a alguna de las fuentes de información marcadas.
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 al menú del árbol.
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.
7	fuentes	Haga clic para asociar fuentes de información a la salvaguarda (la marcada y sus descendientes).
8	aplica	Haga clic para conmutar. 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).

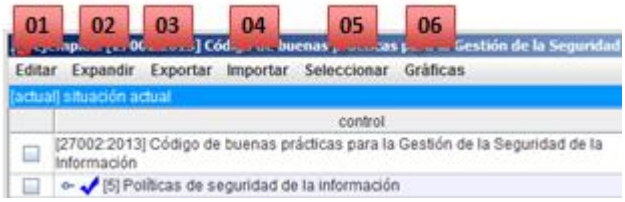
		Vea "*EVL / Fases de referencia y objetivo*
21		Ver "*EVL / Valoración*"
22	semáforo	Compara la valoración en la fase de referencia (ROJA) con la valoración en la fase objetivo (VERDE): ROJO el valor en la fase de referencia está muy lejos del valor objetivo AMARILLO el valor en la fase de referencia 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.

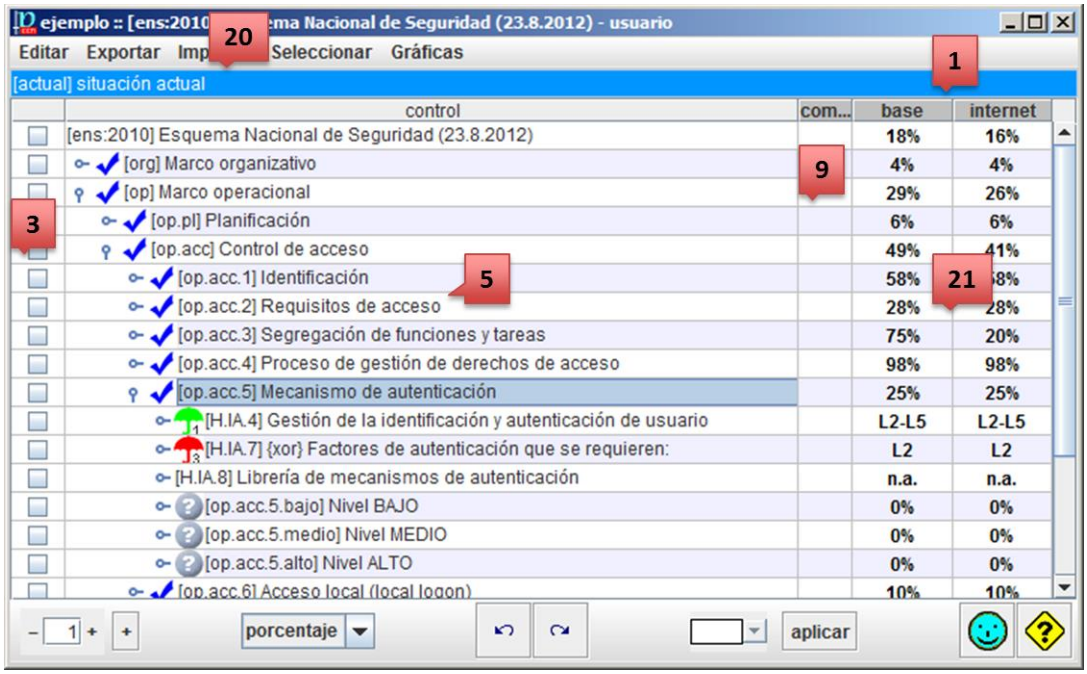
12	dominios	Ver *EVL / dominio*
13		Guarda el proyecto en su fichero o en su base de datos.
23	porcentaje madurez ENS	Controla cómo se presenta el valor en la zona [21] **porcentaje** — porcentaje de cobertura del control (para controles) — madurez de las salvaguardas de PILAR **madurez** — madurez de las salvaguardas y de los controles **cobertura** de **ENS** — porcentaje de cumplimiento de los requisitos al nivel recomendado en la fase ENS; es decir, 100% significa que todos los requisitos se cumplen con una valoración igual o superior a la sugerida por ENS
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

13.7. EVL - VALORACIÓN POR DOMINIOS DE SEGURIDAD

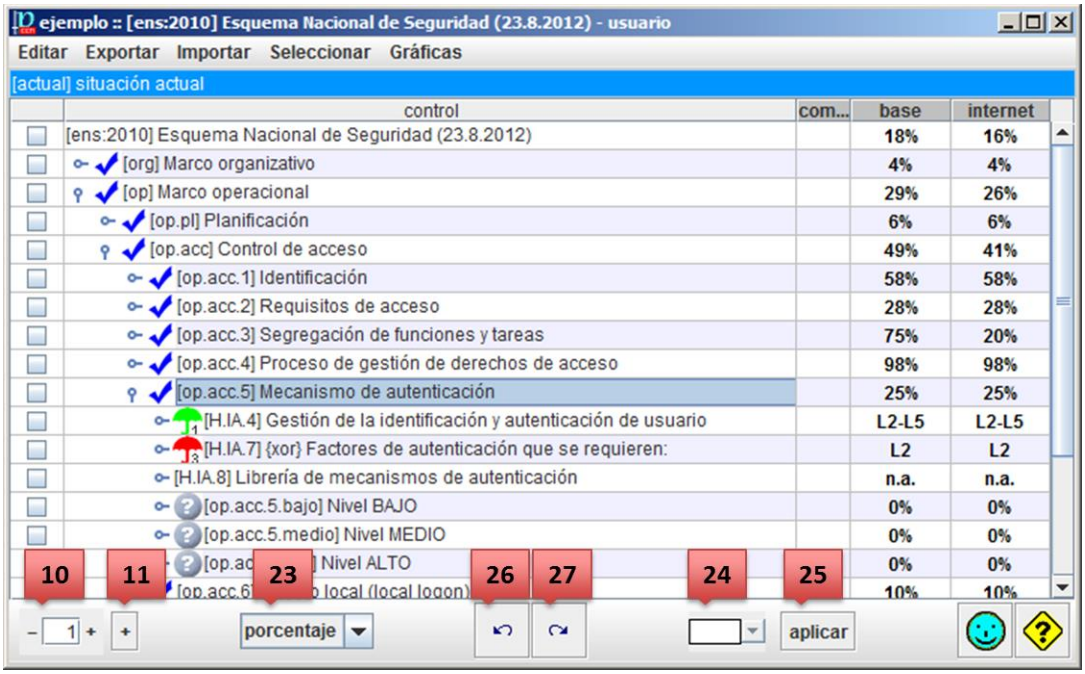


01	editar	buscar busca un cierto texto en el árbol [5] pregunta salta a la siguiente pregunta en el árbol [5]

02	expandir	Expande el árbol hasta el perímetro definido • hasta perímetros definidos en la biblioteca • hasta perfiles definidos por el usuario (ver *Perímetros*
03	exportar	CSV Las filas desplegadas se copian a un fichero CSV XML Los datos se copian a un fichero XML BASE DE DATOS (si la licencia habilita bases de datos SQL)) Los valores se copian a una base de datos INFORME Se genera un informe RTF o HTML SoA Se genera un informe "Declaración de Aplicabilidad)
04	importar	Carga los valores de un fichero CSV o XML
05	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
06	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 al menú del árbol.
9	comentario	Haga clic para asociar un comentario a la salvaguarda.
20		Fases del proyecto. Haga clic para seleccionar la que desea ver.
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