



**GUÍA/NORMA DE SEGURIDAD DE LAS TIC
(CCN-STIC-470F/2)**

**MANUAL DE USUARIO PILAR
ANÁLISIS DE IMPACTO
CONTINUIDAD DE OPERACIONES**

VERSIÓN 5.3

NOVIEMBRE 2013

Edita:



© Editor y Centro Criptológico Nacional, 2013
NIPO: 002-13-055-6

Fecha de Edición: noviembre de 2013

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

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.

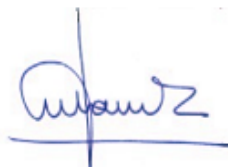
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia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

Noviembre de 2013



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. SOBRE LA CONTINUIDAD	7
1.1. LECTURAS RECOMENDADAS	7
1.2. OTRA DOCUMENTACIÓN.....	8
2. USO TÍPICO	9
2.1. RTO – TIEMPO OBJETIVO DE RECUPERACIÓN	9
2.2. RPO – PUNTO OBJETIVO DE RECUPERACIÓN.....	10
3. INSTALACIÓN.....	12
3.1. ENTORNO JAVA.....	12
3.2. PILAR (WINDOWS)	12
3.3. PILAR (UNIX).....	12
3.4. PILAR (MAC OS X).....	12
3.5. USO	13
3.6. FICHERO DE CONFIGURACIÓN.....	13
3.7. FICHERO DE INFORMACIÓN	13
4. EDITAR / OPCIONES.....	15
4.1. OPCIONES / VALORACIÓN.....	15
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	18
4.12. OPCIONES / FASES ESPECIALES	19
5. INFORMES	20
5.1. POR PATRÓN	20
5.2. INFORMES TEXTUALES	20
5.3. GRÁFICAS	21
5.4. BASES DE DATOS	23
6. NIVELES DE CRITICIDAD – CÓDIGO DE COLORES	24

7. ACEPTAR, CANCELAR, AYUDA.....	25
8. PRIMERA PANTALLA	26
8.1. MODO / PRESENTACIÓN	26
8.2. MODO / TRABAJO	27
9. PANEL DE CONTROL	28
9.1. CONTROLES BÁSICOS	28
9.1.1. MENÚ PROYECTO.....	28
9.1.2. MENÚ FICHERO.....	29
9.1.3. MENÚ BASE DE DATOS	29
9.1.4. IMPORTAR O INTEGRAR	30
9.1.5. MENÚ NIVEL.....	31
9.1.6. MENÚ AYUDA	31
9.2. CONTROLES DEL PROYECTO.....	31
10. PROYECTO	32
10.1. DATOS DEL PROYECTO.....	32
10.2. FUENTES DE INFORMACIÓN	33
10.2.1. EDICIÓN	34
10.3. DOMINIOS DE SEGURIDAD.....	34
10.3.1. EDICIÓN	35
10.3.2. ELIMINACIÓN	36
10.4. ESCALONES DE INTERRUPCIÓN.....	36
10.4.1. FORMATO	37
10.4.2. ESCALAS TÍPICAS	38
10.5. SUBCONJUNTO DE CRITERIOS DE VALORACIÓN	38
10.6. CUANTIFICACIÓN DEL VALOR.....	40
10.7. SUBCONJUNTO DE AMENAZAS	41
10.8. FASES DEL PROYECTO.....	42
10.8.1. COMBINACIÓN Y ELIMINACIÓN DE FASES	43
10.8.2. EDITAR UNA FASE	44
11. ANÁLISIS.....	46
11.1. ACTIVOS / IDENTIFICACIÓN	46
11.1.1. MENÚ CAPAS	48
11.1.2. MENÚ ACTIVOS	49
11.1.3. ACTIVO: ¿ES OBJETO DE AMENAZAS?.....	53

11.1.4.	ACTIVO: ¿ES VISIBLE?.....	53
11.1.5.	ACTIVO: ¿EXISTE?.....	53
11.1.6.	ACTIVO: ¿ESTÁ DISPONIBLE?.....	54
11.1.7.	MENÚ ESTADÍSTICAS.....	54
11.1.8.	OPERACIONES SOBRE UN ACTIVO	54
11.2.	<u>ACTIVOS / EDITAR UN ACTIVO</u>	55
11.3.	<u>ACTIVOS / CLASES DE ACTIVOS</u>	57
11.4.	<u>ACTIVOS / DEPENDENCIAS</u>	59
11.4.1.	MAPA DE DEPENDENCIAS ENTRE CAPAS	64
11.4.2.	GRAFO DE DEPENDENCIAS ENTRE ACTIVOS.....	65
11.4.3.	BUSES: DEPENDENCIAS ENTRE ACTIVOS.....	66
11.4.4.	BLOQUES: DEPENDENCIAS ENTRE ACTIVOS	67
11.4.5.	MAPA DE DEPENDENCIAS ENTRE ACTIVOS.....	68
11.4.6.	DEPENDENCIAS POR DIMENSIÓN DE SEGURIDAD.....	70
11.5.	<u>ACTIVOS / VALORACIÓN</u>	72
11.5.1.	VALORACIÓN DE LOS DOMINIOS DE SEGURIDAD.....	72
11.5.2.	VALORACIÓN ACTIVO POR ACTIVO	75
11.5.3.	VALORACIÓN CUALITATIVA	79
11.5.4.	VALORACIÓN CUANTITATIVA.....	80
11.5.5.	ANULACIÓN DE UNA VALORACIÓN	81
11.5.6.	VALORACIÓN DE LA DISPONIBILIDAD	82
11.6.	<u>AMENAZAS</u>	83
11.6.1.	FACTORES AGRAVANTES ATENUANTES	83
11.6.2.	IDENTIFICACIÓN	85
11.6.3.	VALORACIÓN	88
11.6.4.	TSV – THREAT STANDARD VALUES.....	91
11.7.	<u>IMPACTO Y RIESGO POTENCIALES</u>	92
11.7.1.	IMPACTO Y RIESGO ACUMULADOS	92
11.7.2.	IMPACTO Y RIESGO REPERCUTIDOS	94
11.8.	<u>EQUIPAMIENTO DE RESPALDO</u>	96
11.8.1.	VALORES AGREGADOS	97
11.8.2.	RESPALDO / EDICIÓN	98
11.9.	<u>SALVAGUARDAS</u>	100
11.9.1.	ASPECTO.....	100

11.9.2.	TIPO DE PROTECCIÓN	100
11.9.3.	PESO RELATIVO	100
11.9.4.	INFORMACIÓN ADICIONAL	100
11.9.5.	EN EL ÁRBOL DE SALVAGUARDAS.....	101
11.9.6.	IDENTIFICACIÓN.....	102
11.9.7.	SOA – DECLARACIÓN DE APLICABILIDAD	105
11.9.8.	VALORACIÓN POR DOMINIOS.....	106
11.9.9.	VALORACIÓN POR ACTIVOS	111
11.9.10.	FASE DE REFERENCIA Y FASE OBJETIVO	112
11.9.11.	VALORACIÓN DE LA MADUREZ DE LAS SALVAGUARDAS	113
11.9.12.	OPERACIONES	115
11.9.13.	OPERACIÓN SUGERENCIA	115
11.9.14.	BUSCAR	116
11.9.15.	NORMATIVA DE SEGURIDAD	116
11.9.16.	PROCEDIMIENTOS OPERATIVOS DE SEGURIDAD.....	117
11.10.	<u>IMPACTO Y RIESGO RESIDUALES</u>	117
11.10.1.	TABLA DE IMPACTO Y RIESGO ACUMULADO	117
11.10.2.	IMPACTO ACUMULADO	119
11.10.3.	RIESGO ACUMULADO.....	121
11.10.4.	TABLA DE IMPACTO Y RIESGO REPERCUTIDO	123
11.10.5.	IMPACTO REPERCUTIDO.....	125
11.10.6.	RIESGO REPERCUTIDO	127
12.	DRP – PLANES DE RECUPERACIÓN DE DESASTRES	129
12.1.	<u>PANTALLAS</u>	129
12.1.1.	LA PARTE SUPERIOR.....	129
12.1.2.	LA PARTE INFERIOR.....	130
12.1.3.	ZONA CENTRAL	130
12.1.4.	EJEMPLO	131
12.2.	<u>DRP / ACTUACIONES</u>	132
12.2.1.	ANÁLISIS CUANTITATIVO.....	133
12.3.	<u>EL SIGNIFICADO DE LOS ACTIVOS LISTOS</u>	133

Conceptos

1. SOBRE LA CONTINUIDAD

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.

PILAR 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.

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.
- ISO 22301:2012
Societal security – Business continuity management systems – Requirements
- ISO/IEC 27031:2011
Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity

- ISO/IEC 24762:2008
Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services

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. RTO – TIEMPO OBJETIVO DE RECUPERACIÓN

Es un parámetro importante en la concepción de un plan de continuidad. Concretamente se plantea un tiempo límite para que un cierto servicio vuelva a estar en funcionamiento. A partir de este objetivo, empleado como techo, se van planteando los mecanismos de respaldo y los procesos asociados.

Por ejemplo, nos podemos proponer un RTO de 2 días, que quiere decir que si ocurre un desastre, en menos de 48 horas estaremos de nuevo operativos.

Este parámetro, a veces tiene letra pequeña:

- si un sistema soporta varios servicios, es posible que haya una gradación de tiempos, recuperándose los servicios por etapas
- un servicio puede recuperar rápidamente un nivel mínimo de servicio y luego ir mejorando progresivamente hasta alcanzar los niveles estándar de calidad de servicio
- un servicio puede ser crítico en ciertos días, y menos crítico el resto del tiempo; en estos casos tendremos objetivos RTO diferentes en diferentes periodos

Realmente, el RTO a veces tiene diferentes interpretaciones. Desde que un servicio deja de estar operativo hasta que se restaura, podemos diferenciar 3 fases

1. T1 = desde que el servicio deja de estar operativo hasta que se detecta
2. T2 = desde que se detecta hasta que se toma la decisión de activar el plan de recuperación
3. T3 = desde que se toma la decisión de restaurar el servicio, hasta que se consuma el plan de recuperación.

El tiempo T1 es difícil de determinar por cuanto un servicio puede estar claramente detenido o puede estar trabajando con una calidad disminuida. Un servicio puede caerse durante la noche, y no detectarse hasta que empieza el día.

El tiempo T2 es un tiempo de toma de decisiones. En esta toma de decisiones pesa tanto la detención del servicio como el coste de activar el plan de recuperación. Cuando el origen del problema es externo (por ejemplo, cuando falla un proveedor) aparece la duda de si es mejor esperar a que el proveedor recupere el servicio, o activar el plan de recuperación propio. También hay que tener en cuenta ante un servicio deteriorado, si es mejor mantenerlo en condiciones sub-óptimas, o si es mejor tirarlo completamente y recuperarlo garantizando la calidad del servicio.

Por último, el tiempo T3 es probablemente es menos sujeto a interpretaciones: desde que se le da la orden a los técnicos, hasta que terminan su labor.

El RTO es una decisión de gobierno. Un RTO corto suele ser más costoso que un RTO largo. Suele ser necesario llegar a un equilibrio entre coste asumible y RTO. Es frecuente que este equilibrio vaya cambiando con los años y con la disponibilidad económica de cada momento.

RTOs cortos prácticamente implican mecanismos automáticos de recuperación del servicio. RTOs largos permiten un tratamiento más manual. La diferencia de costes entre la tecnología y del personal marcan fuertemente la decisión que se tome.

PILAR

PILAR es muy flexible en cuanto a lo que queramos hacer con respecto al RTO, ayudando a determinar el valor que nos interesa y a analizar si el sistema cumple nuestro objetivo o no.

PILAR calcula el impacto derivado de recuperar el sistema en un cierto tiempo X. Si este impacto es aceptable, el RTO puede ser superior. Y viceversa, si ese impacto X no es aceptable, buscaremos un RTO inferior.

El RTO deseado se suele elegir a la vista de la valoración del sistema. Ver “Activos / Valoración”. Simplemente, viendo el escalado del impacto, podemos poner una cota de máximo impacto aceptable y el RTO del servicio en cuestión viene dado por el intervalo de interrupción en el que se alcanza esa cota.

Para saber si lo hemos alcanzado, en una cierta fase, analizaremos el impacto residual. Ver “Backup / agregado”.

A veces deseamos diseñar planes de contingencia o de recuperación frente a desastres. En estos casos podemos usar el mismo RTO o tener objetivos de recuperación indexados a la magnitud del desastre. En estos casos usaremos la funcionalidad “plan de recuperación de desastres”.

2.2. RPO – PUNTO OBJETIVO DE RECUPERACIÓN

Es un parámetro importante en la concepción de un plan de continuidad. Concretamente se plantea un tiempo máximo de pérdida de información.

Por ejemplo, si un sistema replica (backup) sus datos cada 24h, un desastre puede llevarnos a perder los datos de las últimas 24h en el peor de los casos¹. O, visto al revés, si no podemos permitirnos el lujo de perder más de X horas de datos, tendremos que organizar las copias de respaldo (backup) de forma que al menos hagamos uno cada X horas.

Este parámetro, a veces tiene letra pequeña:

- si un sistema maneja varios conjuntos de información, es posible que haya una gradación de tiempos, garantizándose diferentes RPOs
- una información puede ser crítica en ciertos días, y menos crítica el resto del tiempo; en estos casos tendremos objetivos RPO diferentes en diferentes periodos

El RPO es una decisión de gobierno. Un RPO corto suele ser más costoso que un RPO largo. Suele ser necesario llegar a un equilibrio entre coste asumible y RPO. Es frecuente que este equilibrio vaya cambiando con los años y con la disponibilidad económica de cada momento.

RPOs cortos prácticamente implican mecanismos automáticos de copias sin detener los servicios. Este planteamiento introduce una cierta complejidad para saber en qué punto tenemos datos consolidados y no meras instantáneas. RPOs largos permiten realizar y trasladar las copias manualmente. La diferencia de costes entre la tecnología y del personal marcan fuertemente la decisión que se tome.

Cuando la información es muy valiosa, a veces conviven objetivos RPO muy cortos (para que no se pierda ninguna información) con RTOs largos, pues el servicio puede detenerse sin mayor problema. Al revés, es menos habitual, pues implicaría reponer un servicio sin la información adecuada.

¹ Algunas metodologías recomiendan duplicar este tiempo. El argumento es que los soportes de información pueden estar dañados, obligando a recurrir a copias previas. Para argumentar al respecto, hay que conocer los detalles de cómo se realizan y conservan las copias de seguridad, dependiendo fuertemente de la tecnología usada. Las copias remotas sobre una red de comunicaciones son mucho más fiables que las copias en soportes con transporte físico a otro lugar.

PILAR

PILAR hace poco respecto del RPO. Realmente, sólo tiene en cuenta el tiempo que cuesta extraer la información tenerla de nuevo disponible. La frecuencia de las copias es un tema de política y procedimientos.

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)

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_es.car`

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

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

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

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

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 alta	F fácil	100
L grande	P probable	A alta	M medio	10
M medio	PP poco probable	M media	D difícil	1
S pequeño	I improbable	B baja	MD muy difícil	0,1
XS muy pequeño	MR muy raro	MB muy baja	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 recalcula 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

cundo una salvaguarda no está valorada en 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

cundo una salvaguarda no está valorada en 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	9°	6°	3°	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	9°	6°	3°	9°	8°	7°

4.8. OPCIONES / SALVAGUARDAS NO EVALUADAS

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

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

es como si la salvaguarda fuera irrelevante en este dominio

salvaguadas 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: salvaguadas / todos los valores de madurez

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

exportar: salvaguadas / 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 salvaguadas 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 salvaguadas. 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 maduras que se presentan como fases especiales; por ejemplo, PILAR. Estas fases no se pueden editar; usted simplemente puede verlas y usarlas como sugerencia de la madurez adecuada para cada salvaguarda.

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.

Equipamiento de respaldo

El informe presenta el equipamiento de respaldo previsto y la madurez del proceso de sustitución, en cada fase.

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 maduras. Es decir: selecciona un umbral de preocupación, y se presentan las salvaguardas por debajo del umbral.

Análisis de impacto

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

Análisis de riesgos

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

5.3. GRÁFICAS

Valor / activo

Muestra directamente un grafo de cómo evoluciona el valor en función del tiempo que el activo está detenido.

Concretamente, muestra el escalado de coste derivado de la interrupción de los activos esenciales.

Es una gráfica que a menudo se emplea para elegir el objetivo de recuperación (*RTO*) de los servicios.

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.

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.

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.

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. NIVELES DE CRITICIDAD – CÓDIGO DE COLORES

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



9 -
8 -
7 - extremadamente crítico
6 - muy crítico
5 - crítico
4 - muy alto
3 - alto
2 - medio
1 - bajo
0 - despreciable

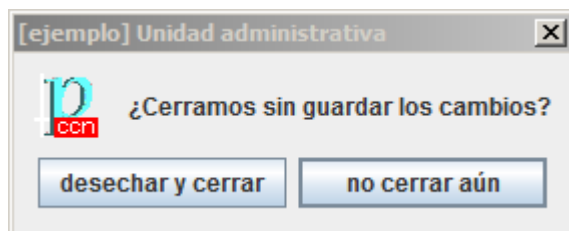
Pantallas

7. ACEPTAR, CANCELAR, AYUDA

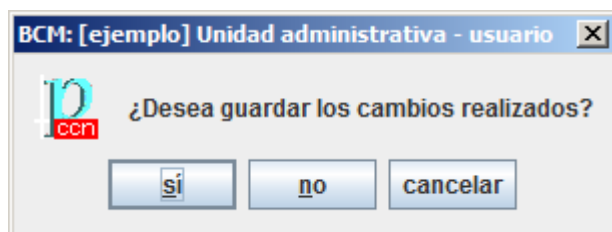
La mayoría de las pantallas incluyen los siguientes botones:

	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 |
| SI | se guardan los cambios y se cierra la ventana |

8. PRIMERA PANTALLA

Para empezar rápidamente

Para ver un análisis de impacto (sólo lectura):

- **modo / presentación**
- **análisis cualitativo [5]**

Para trabajar en un proyecto nuevo o ya existente:

- **modo / trabajo**
- vaya al directorio donde guardó la licencia (fichero .lic) y selecciónela
- **análisis cualitativo**

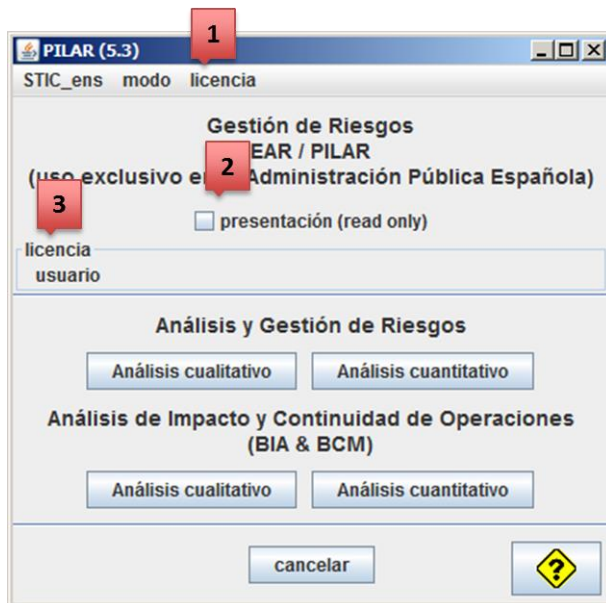
8.1. MODO / PRESENTACIÓN



1	Selecciona un fichero de configuración. Ver " <u>Fichero de configuración</u> ".
2	Modo de presentación: sólo se permite navegar por el proyecto, sin hacer cambios. <u>Modo / trabajo</u> : 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.

6	Inicia un análisis cuantitativo: interrupción y recuperación del servicio.
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



	Ver <u>Menú proyecto</u>
	Ver <u>Menú fichero</u>
	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]
	Preferencias: tipo y tamaño de letra. Opciones: Ver <u>Editar / Opciones</u>
	Ver <u>Menú nivel</u>
	Ver <u>Menú ayuda</u>
	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

	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	 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	 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.

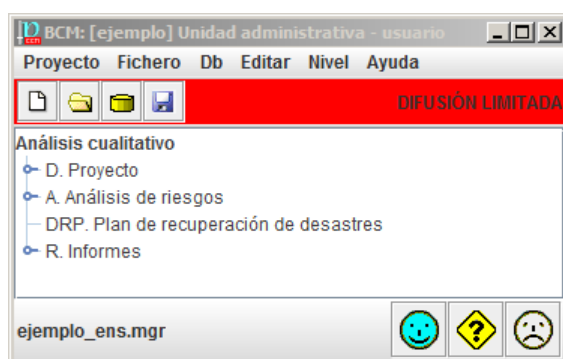
tipo de valor	 importar	 integrar
nuevo dominio de seguridad	se añade	se añade
dominios en P1 & P2 - fuentes de información - factores	- se añade - se añade	- se añade - se añade
nuevo activo	se añade	se añade
activos en P1 & P2 - clases - fuentes de información - dependencias - valores - criterios	- se añade - se añade - se añade - se reemplaza - se reemplaza	- se añade - se añade - se añade - valor máximo - se añade
nueva amenaza	se añade	se añade
amenazas en P1 & P2 valoración	se reemplaza	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 reemplaza - se añade - se reemplaza - se añade - se reemplaza - se reemplaza	- na = na₁ & na₂ - se añade - se añade - se añade - valor máximo - na = na₁ & na₂
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.

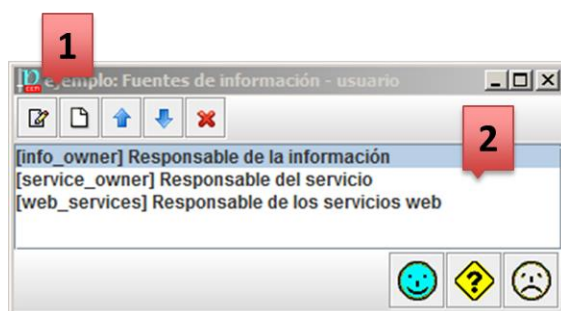
1	La biblioteca. Se selecciona al arrancar. Ver “ <i>Fichero de configuración</i> ”.
2	Código del proyecto. Debería ser único.
3	El nombre del proyecto. Una descripción sucinta.
4	La marca de clasificación, por defecto, de los informes.

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 “ <i>fichero de información</i> ”.
limpiar	Elimina las filas sin valor.

10.2. FUENTES DE INFORMACIÓN

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



	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
	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:

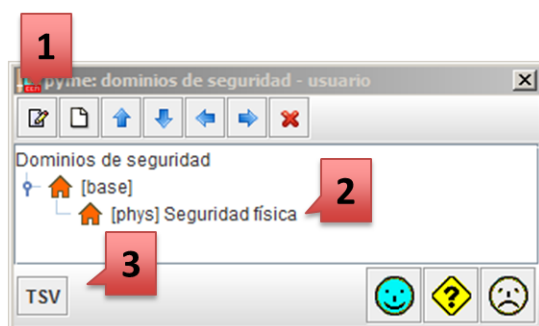
- el código: debe ser único
- el nombre: una descripción sucinta
- una descripción más larga

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 “ <i>Threat Standard Values</i> ”

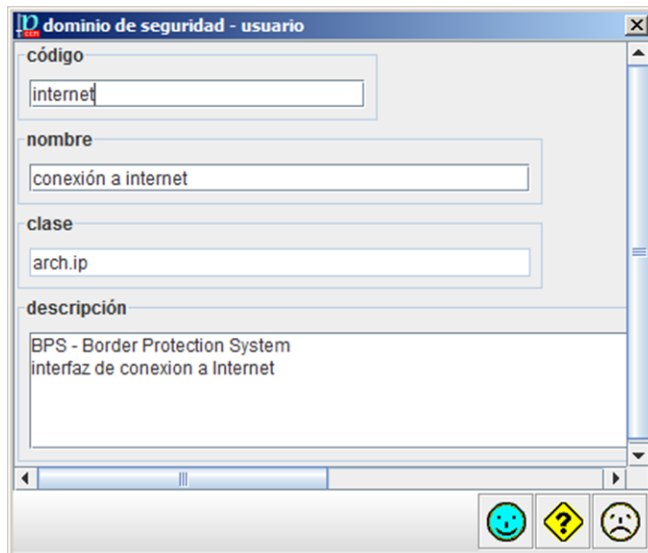
10.3.1.EDICIÓN

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

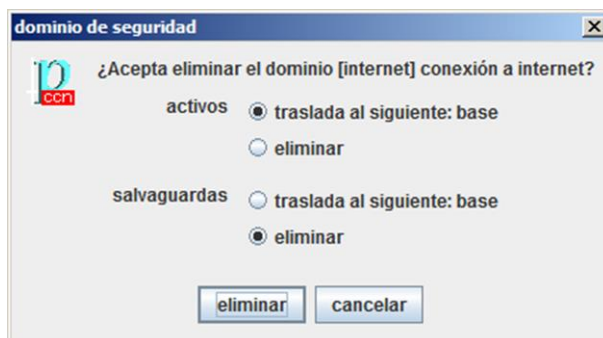
- ENS – sistema adscrito al perfil ENS
- IP – punto de interconexión, perfil IP (CCN-STIC 811)
- una descripción más extensa

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



10.3.2. ELIMINACIÓN

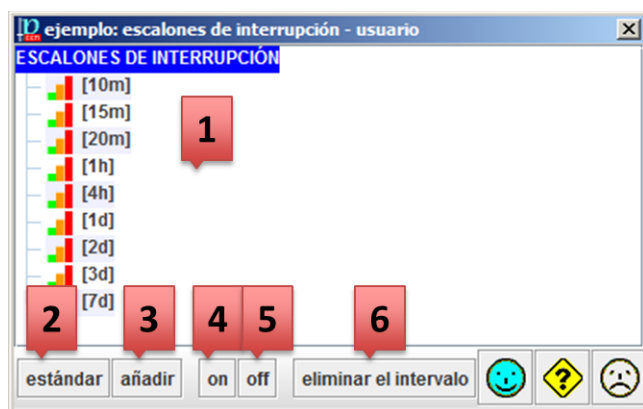
Cuando vaya a eliminar un dominio, PILAR le preguntará qué desea hacer con los datos asociados a ese dominio. Concretamente, debe usted indicar qué hacer con los activos en ese dominio y qué hacer con las salvaguardas evaluadas en ese dominio. Si el dominio no es subdominio de otro, hay poco que hacer: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



10.4. ESCALONES DE INTERRUPCIÓN

Permite determinar los puntos en el tiempo para analizar las interrupciones de servicio.

Ver glosario de términos: [<http://www.pilar-tools.com/es/glossary/index.html>]



1	Intervalos de interrupción que se considerarán en el análisis. PILAR siempre presenta los intervalos ordenados, y usando la forma más compacta de presentación de su duración.
2	Haga clic. PILAR presenta algunas <u>escalas típicas</u>
3	Haga clic para añadir un nuevo intervalo. Vea el <u>formato</u> que usa PILAR Para especificar intervalos.
4	Puede usted mantener el intervalo; pero evitar que PILAR lo presente. ON – sí se presenta
5	OFF – no se presenta (sólo aparece en esta ventana)
6	Se retira el intervalo a todos los afectos.

10.4.1.FORMATO

Internamente, PILAR siempre trabaja con segundos; pero hace un esfuerzo para leer y escribir intervalos más fáciles de leer:

...	segundos
... s	segundos
... m	minutos
... h	horas
... d	días

Se permite cualquier combinación. Por ejemplo

3d207m1

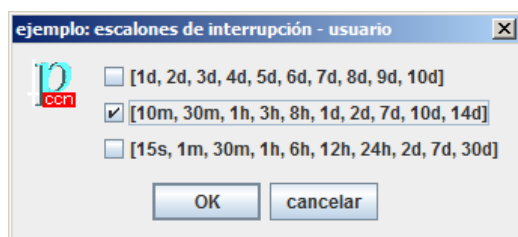
que se lee como “3 días + 207 minutos + 1 segundo”.

Algunos ejemplos más normales:

15s	15 segundos
1m30s	1 minuto + 30 segundos
90s	1 minuto + 30 segundos
2h	2 horas
2h30m	2 horas + 30 minutos
24h	24 horas = 1 día

10.4.2. ESCALAS TÍPICAS

Aunque no hay regla universal, y tiene que ser decidido caso por caso, algunas escalas son habituales:



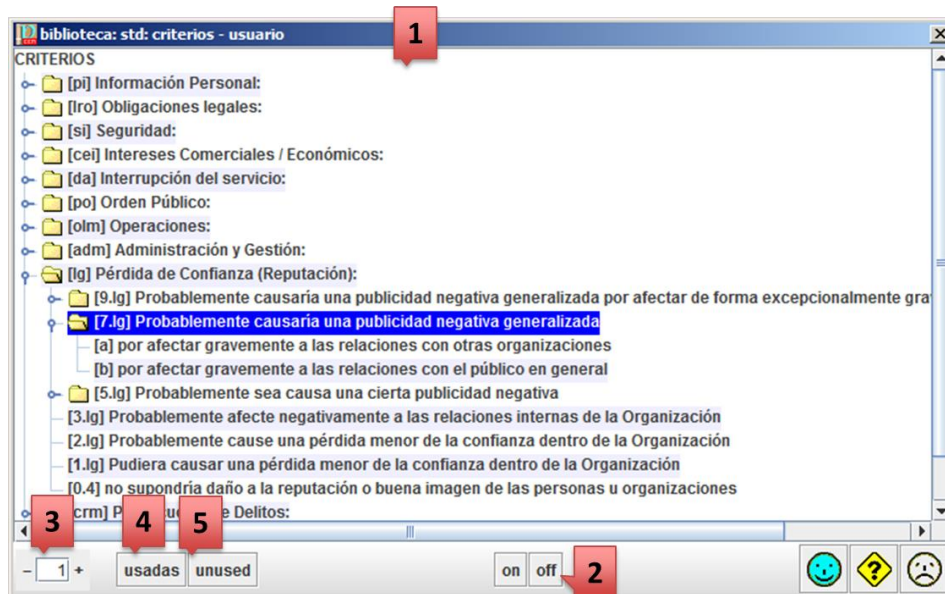
- una escala lineal sobre días sucesivos
1d, 2d, 3d, ..., 10d
suele ser útil para plan de recuperación que no son de tiempo real; o sea, cuando recuperaremos el servicio en horas o días
- una escala exponencial sobre un cierto intervalo
10m, 30m, 1h, 3h, 6h, 1d, 2d, 7d, ...
suele ser útil en sistemas interactivos, en donde se busca una recuperación rápida
- una escala exponencial sobre un amplio intervalo
15s, 1m, 30m, 1h, 6h, 12h, 24h, 2d, 7d, 30d
suele ser útil en sistemas interactivos, en donde se busca una recuperación muy rápida aunque se tiene en cuenta que el sistema pudiera tardar días o semanas en recuperarse

10.5. SUBCONJUNTO DE CRITERIOS DE VALORACIÓN

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

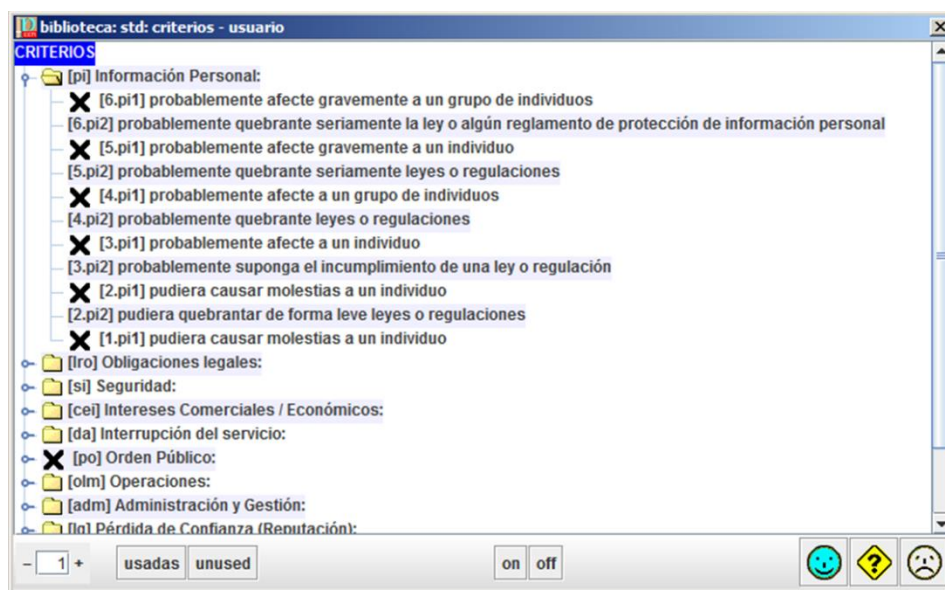
Sin embargo, se puede renunciar a algunos criterios, si no los considera apropiados para su Organización. Seleccione el criterio o grupo de criterios, y use los botones ON / OFF al pie.

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.
3	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 permite asociar niveles de valoración cualitativos a valores cuantitativos a fin de poder alternar entre uno y otro tipo de análisis.

valor	biblioteca	proyecto
[0]	1.000	1.000
[1]	2.150	2.150
[2]	4.650	4.650
[3]	10.000	10.000
[4]	21.500	21.500
[5]	46.500	46.500
[6]	100.000	100.000
[7]	215.000	215.000
[8]	465.000	465.000
[9]	1.000.000	1.000.000
[10]	2.150.000	2.150.000

columna	
valor	muestra el nivel cualitativo. Es fija.
biblioteca	muestra la asociación estándar en la biblioteca. Es fija.
proyecto	muestra la asociación que desea para este proyecto. Puede modificarla a su gusto.
reset	recupera los valores de la biblioteca (columna 2) para el proyecto (columna 3)

Puede elegir cualquier valor para la tercera columna, siempre que esté entre los valores superior e inferior.

Se recomienda para utilizar alguna escala exponencial (o logarítmica).

El RESET se utiliza para copiar los valores de la segunda columna en la tercera.

Después de cambiar la asociación debe cerrar el proyecto y volver a abrirlo, puesto que los cambios se aplican a la ejecución siguiente.

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 realizado. De esta forma puede ser informativo ejecutar un modelo cualitativo en términos cuantitativos.

Paso de valores cuantitativos a niveles cualitativos

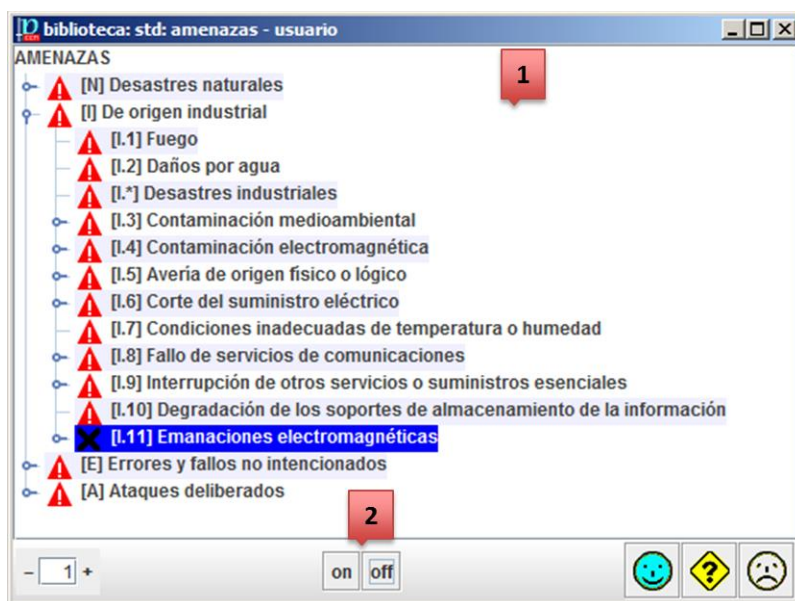
Se utiliza cuando el usuario proporciona solamente la valoración cuantitativa. PILAR puede realizar un análisis cualitativo donde el impacto de un servicio altamente valorado queda realizado. De esta forma puede ser informativo ejecutar un modelo cuantitativo en términos cualitativos.

10.7. SUBCONJUNTO DE AMENAZAS

La biblioteca estándar establece las amenazas disponibles.

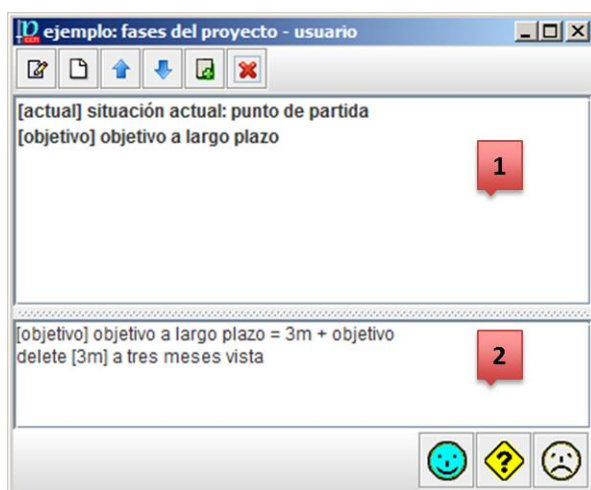
Sin embargo, se puede renunciar a algunas amenazas. Seleccione la amenaza o el grupo de amenazas, y use los botones ON / OFF al pie.

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.



	Árbol con todas las amenazas que pueden afectar a la disponibilidad
	Haga clic para seleccionar / deseleccionar una amenaza o un grupo de amenazas.
	Para seleccionar el nivel de despliegue del árbol.

10.8. FASES DEL PROYECTO



	Haga clic para editar la fase seleccionada. Ver “ <i>Editar una fase</i> ”.
	Haga clic para crear una nueva fase. Ver “ <i>Editar una fase</i> ”.

	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
	Una lista ordenada de fases de evaluación.
	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

The screenshot shows a window titled 'editar objetivo - usuario'. It contains the following fields and callouts:

- 1**: Points to the 'código' field, which has a sub-field 'objetivo'.
- 2**: Points to the 'nombre' field, which has a sub-field 'situación objetivo'.
- 4**: Points to the 'descripción' text area.

At the bottom right, there are three icons: a smiley face, a question mark, and a sad face.

	el código; debe ser único
	el nombre: una descripción sucinta
	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

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

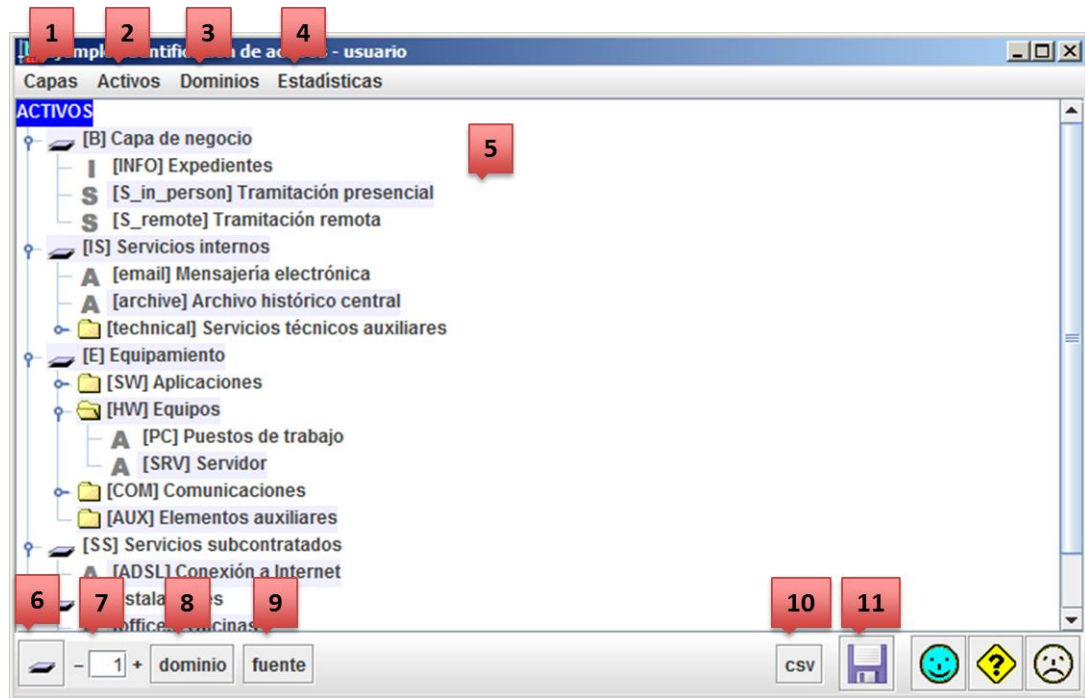
Estos son esenciales para el análisis de riesgos: los activos de verdad.

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 “ <u>Menú capas</u> ”.
2	activos	Ver “ <u>Menú activos</u> ”.
3	dominios	Para editar los dominios de seguridad. Ver “ <u>Dominios de seguridad</u> ”.
4	estadísticas	Ver “ <u>Menú estadísticas</u> ”.
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 “ <u>Editar un activo</u> ”. Haga clic con el botón derecho para operar sobre un activo. Ver “ <u>Operaciones sobre un activo</u> ”-
6		Haga clic para colapsar el árbol al primer nivel.
7		Para seleccionar el nivel de expansión del árbol.

	dominio	Haga clic y seleccione un dominio. PILAR selecciona los activos en dicho dominio.
	fuelle	Haga clic y seleccione una fuente de información. PILAR selecciona los activos asociados a dicha fuente.
	csv	Exporta los datos a un fichero CSV (comma-separated values).
		Guarda el proyecto en su fichero o en su base de datos.

11.1.1.MENÚ CAPAS

	Menú capas
capas estándar	Incorpora las capas definidas en la biblioteca. Ver “ <i>fichero de información</i> ”.
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 “ <u>Editar un activo</u> ”.
nuevo activo / nuevo grupo	Crea un nuevo grupo (un directorio). Ver “ <u>Editar un activo</u> ”.
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 “ <u>Editar un activo</u> ”.
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 “ <i>Editar un activo</i> ”.
combinar activos	Selecione dos o más activos. Esta función los combina, arrojando las clases de unos y otros. Debe editar el nuevo activo y por lo menos cambiar el código, ya que debe ser único. Ver “ <i>Editar un activo</i> ”.
descripción	Salta a la descripción larga del activo seleccionado.
dominio de seguridad	Mueve los activos seleccionados a un dominio de seguridad.
fuentes de información	Asocia una o más fuentes de información a los activos seleccionados.
ordenar / [a..z] ...	Los activos seleccionados se ordenan alfabéticamente, por código.
ordenar / ... [A..Z]	Los activos seleccionados se ordenan alfabéticamente, por nombre.
ordenar / retrocede	Se invierte la última ordenación, regresando al orden original.
activo / grupo / que sea grupo	Cambia los activos seleccionados, de activos normales a grupos.
activo / grupo / que no sea grupo	Cambia los activos seleccionados, de grupos a activos normales.
eliminar / los hijos	Elimina los hijos de los activos seleccionados.
eliminar / el activo	Elimina los activos seleccionados.
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?

Quando 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?

Quando 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

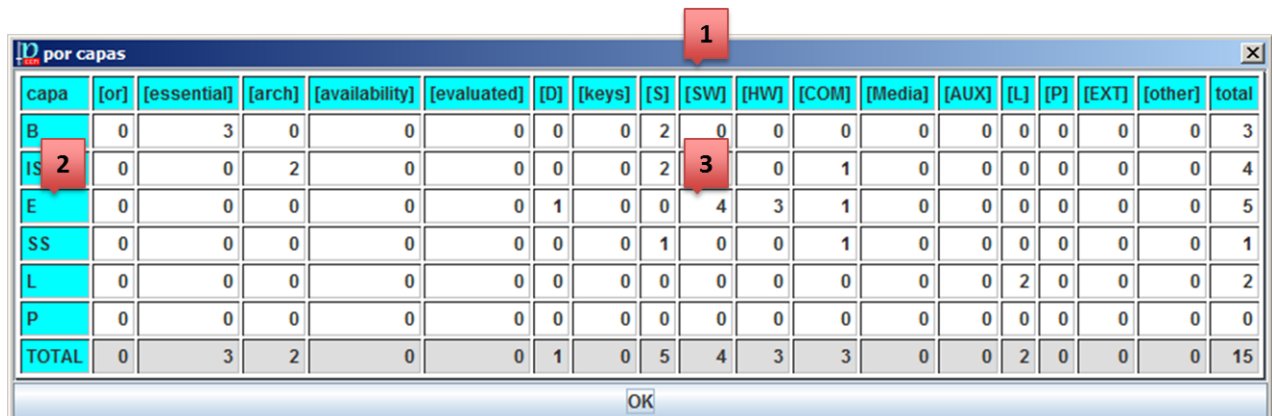
- seleccionar un activo
- menú activos / disponible / ...

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.



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	3	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

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.

	El código, que debe ser único
	Una descripción sucinta: en una línea
	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.
	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 cuenta las clases marcadas en [10]. Ver “ <i>fichero de información</i> ” — limpiar – elimina las líneas sin valor
	Haga clic para asociar un activo a una o más fuentes de información.
	Selecciona el dominio de seguridad al que pertenece el activo.
	Una descripción más extensa. La descripción puede contener hiperenlaces (URLs). Para ir a la página enlazada, haga clic con el botón derecho y después 
	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

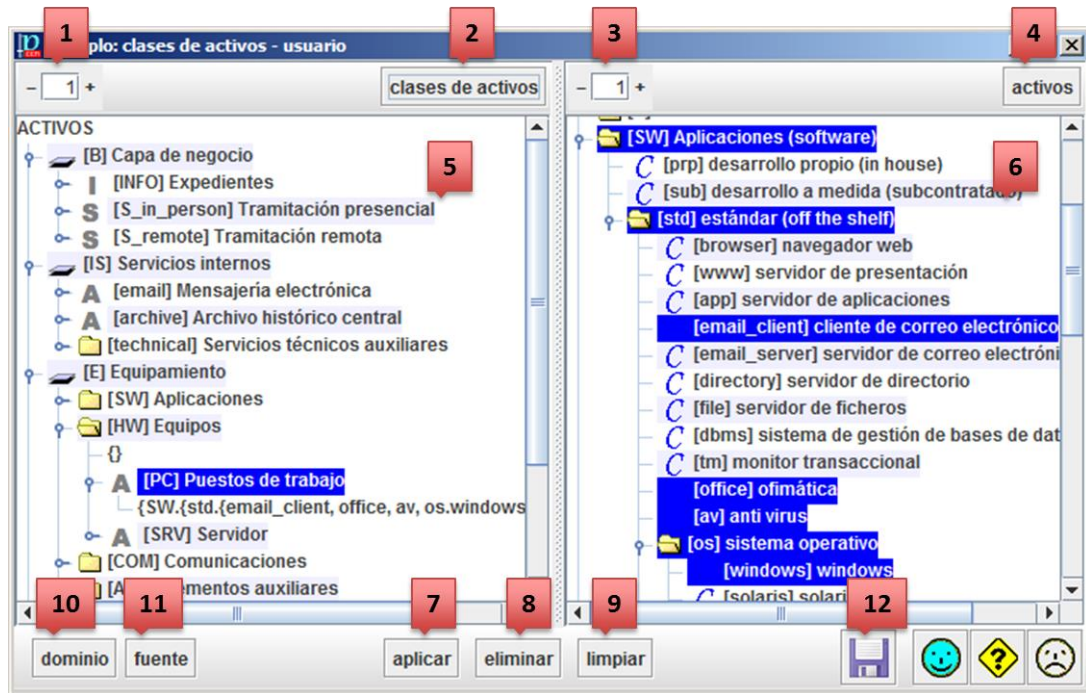
- ▼ ☒ [keys] claves criptográfi...
- ▼ ☒ [info] protección de la Informaci...
- ▼ ☒ [encrypt] encryption k...
 - ☒ [shared_secret] secreto compartido (clave simétri...
 - ☐ [public_encryption] cifrado con clave pública
 - ☐ [public_decryption] descifrado con clave pública
- ▼ ☒ [sign] claves de fir...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

clic derecho + LIMPIAR	clic derecho + ELIMINAR
▼ ☐ [-] [keys] claves criptográfi... ▼ ☐ [-] [info] protección de la Informac... ▼ ☐ [-] [encrypt] encryption k... ☒ [shared_secret] secreto compartido (clave simétri... ☐ [public_encryption] cifrado con clave pública ☐ [public_decryption] descifrado con clave pública ▼ ☒ [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] Certificado 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] Certificado 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 / 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 ...

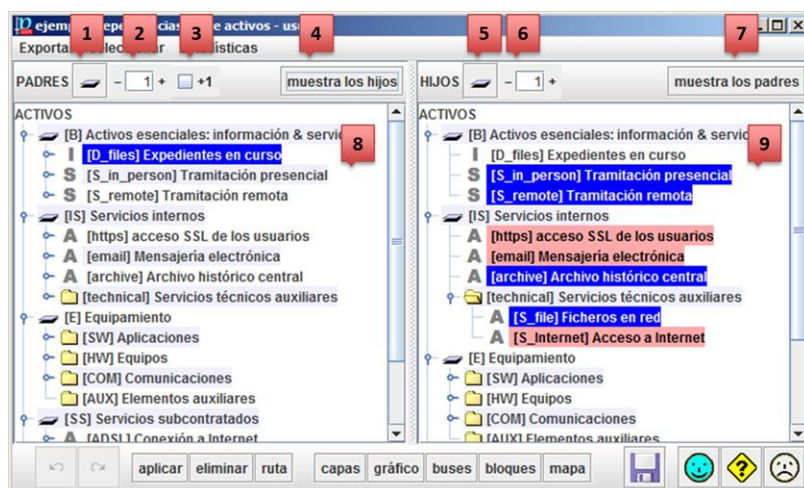
- asocie cada servicio al equipamiento que utiliza: software, hardware, comunicaciones, medios,...

Si ha identificado personal ...

- asocie cada persona a los servicios o al equipo sobre el puede causar daño voluntaria o accidentalmente

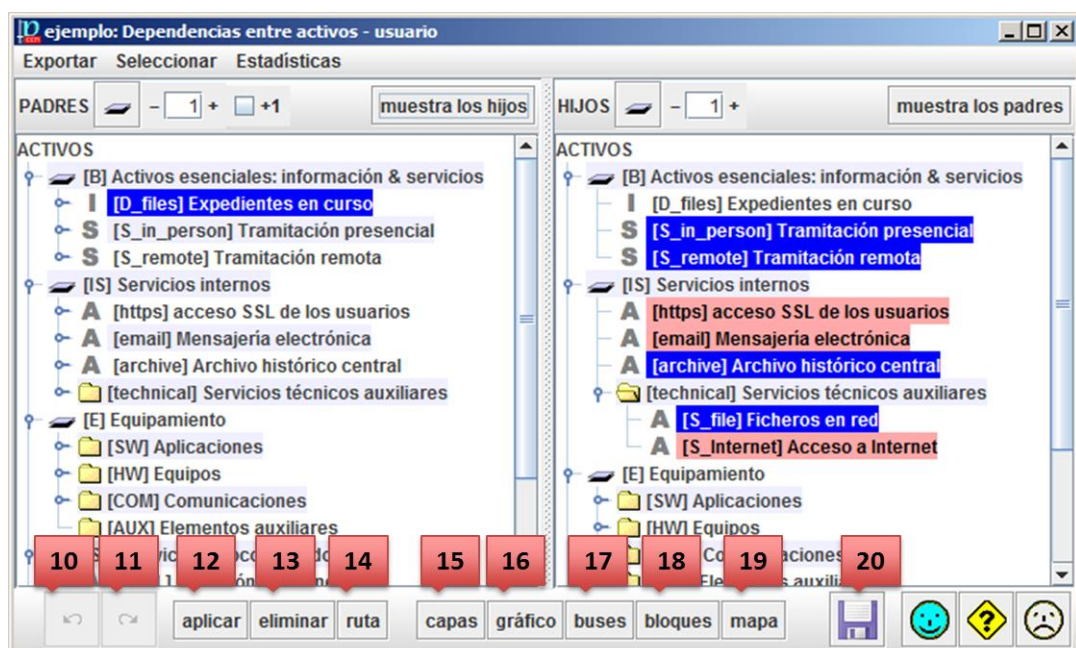
Repita hasta que cada activo por debajo de la capa de negocio se utiliza para algo.

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).

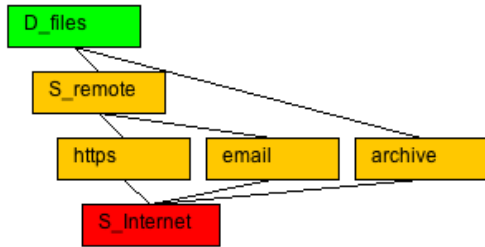


1		Haga clic para colapsar el árbol izquierdo ([8]).
2		Controla el nivel de expansión del árbol izquierdo ([8]).

3	+1	Controla si el árbol izquierdo ([8]) incluye las dependencias. Si está seleccionado [+1], se muestran también los activos de los que depende.
4	mostrar los hijos	— Seleccione un activo en el árbol izquierdo ([8]). — 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		Controla el nivel de expansión del árbol derecho ([9]).
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 “ <u>Activos / Dependencias / Capas</u> ”.
16	gráfico	Abre una ventana con tantas cajitas como activos, mostrando las dependencias entre ellos. Ver “ <u>Activos / Dependencias / Grafo</u> ”.
17	buses	Abre una ventana con tantas cajitas como activos, mostrando las dependencias entre ellos. Ver “ <u>Activos / Dependencias / Buses</u> ”.
18	bloques	Abre una ventana con tantas cajitas como activos, mostrando las dependencias entre activos de cada capa. Ver “ <u>Activos / Dependencias / Bloques</u> ”.
19	mapa	Abre una ventana con tantas cajitas como activos, mostrando las dependencias entre ellos. Ver “ <u>Activos / Dependencias / Mapa</u> ”.
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%.

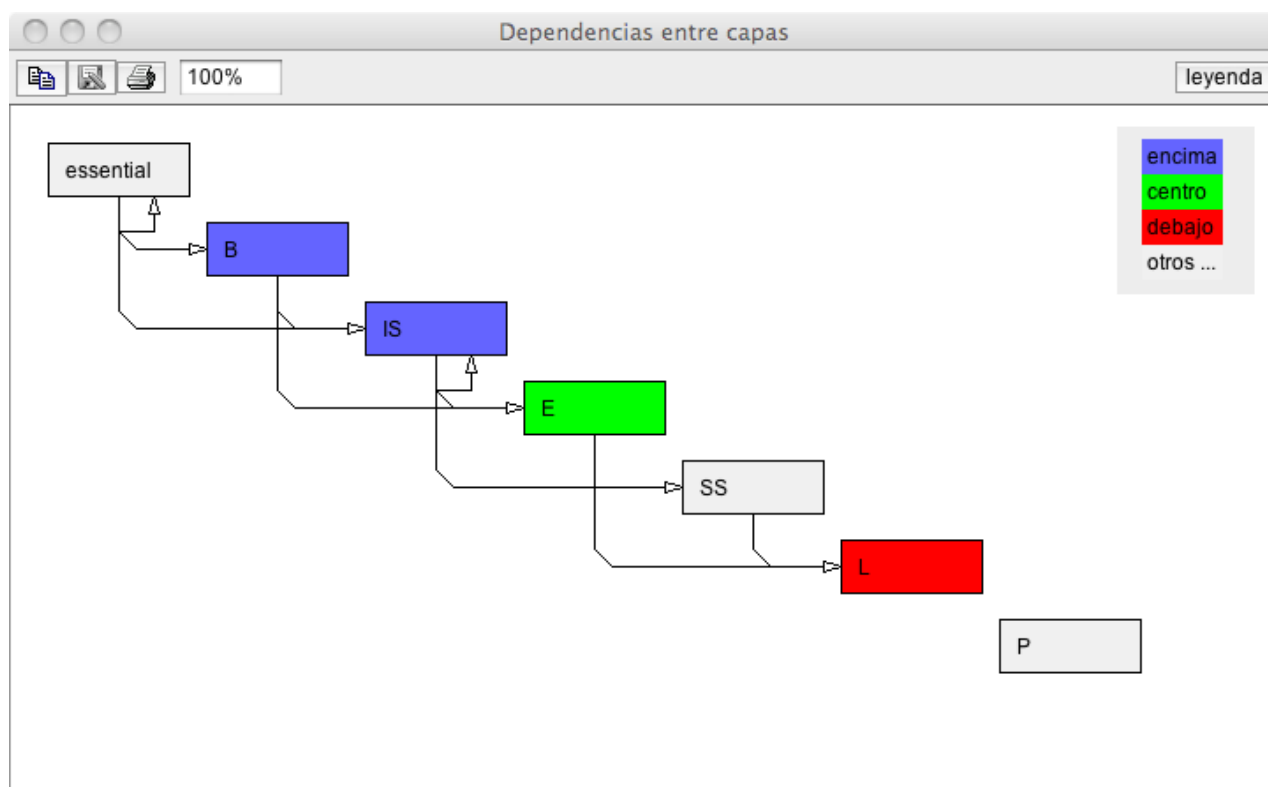
Para fijar un grado entre el 0% y el 100%:

- 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 "ra_add"

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

11.4.1. 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"

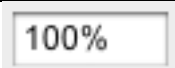
- las capas superiores dependen solamente de capas inferiores
- las capas inferiores dependen solamente de capas superiores
- puede haber dependencias internas en las capas

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 brillante	la capa de la referencia
rojo brillante	capas inferiores directamente relacionadas
gris	no relacionadas

	copiar	copia la imagen al portapapeles para pegarlo en algún otro sitio
	guardar	almacena el dibujo en un fichero gráfico. Los formatos de imagen

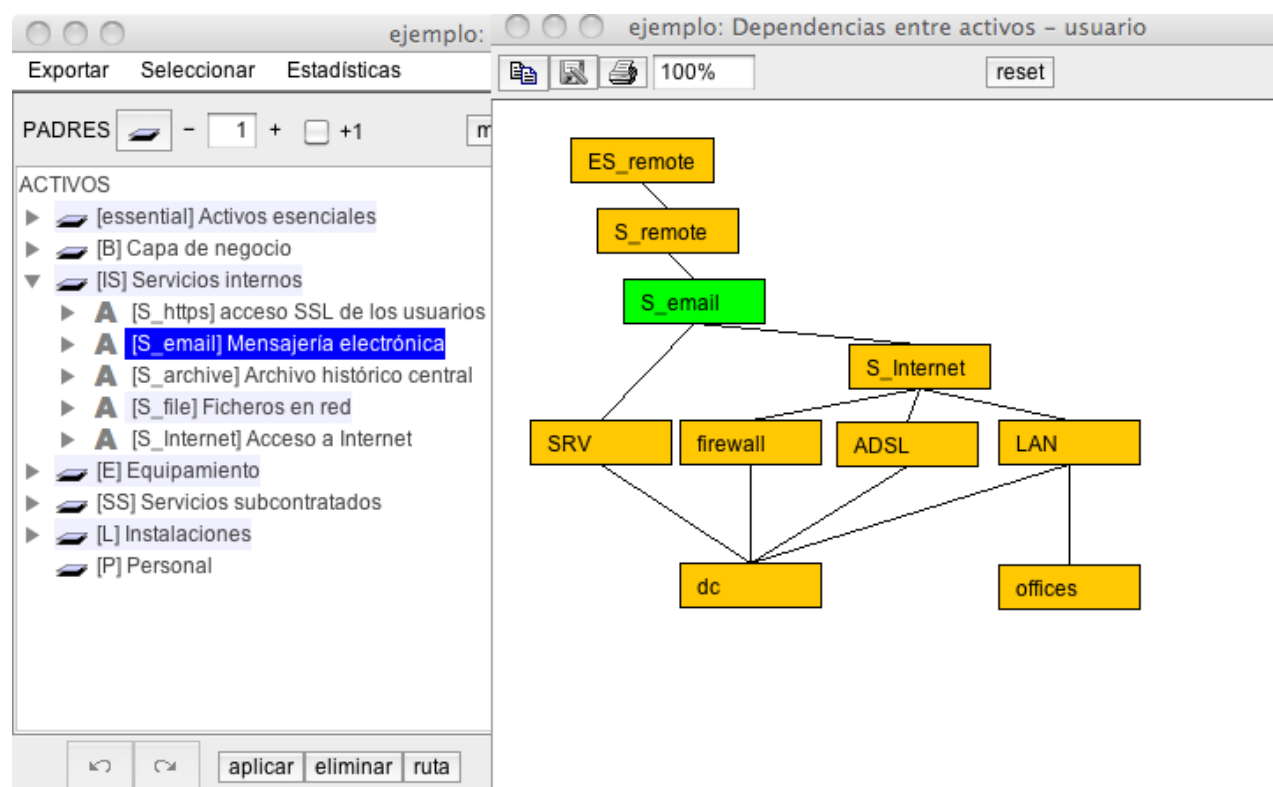
		disponibles dependen de su ordenador; algunos formatos son casi universales jpg, JPEG, png
	imprimir	para enviar el gráfico a una impresora
	escala	para cambiar el tamaño de la imagen
	leyenda	muestra el código de colores

11.4.2. 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
	escala	para cambiar el tamaño de la imagen
	reset	reposiciona las cajas heurísticamente

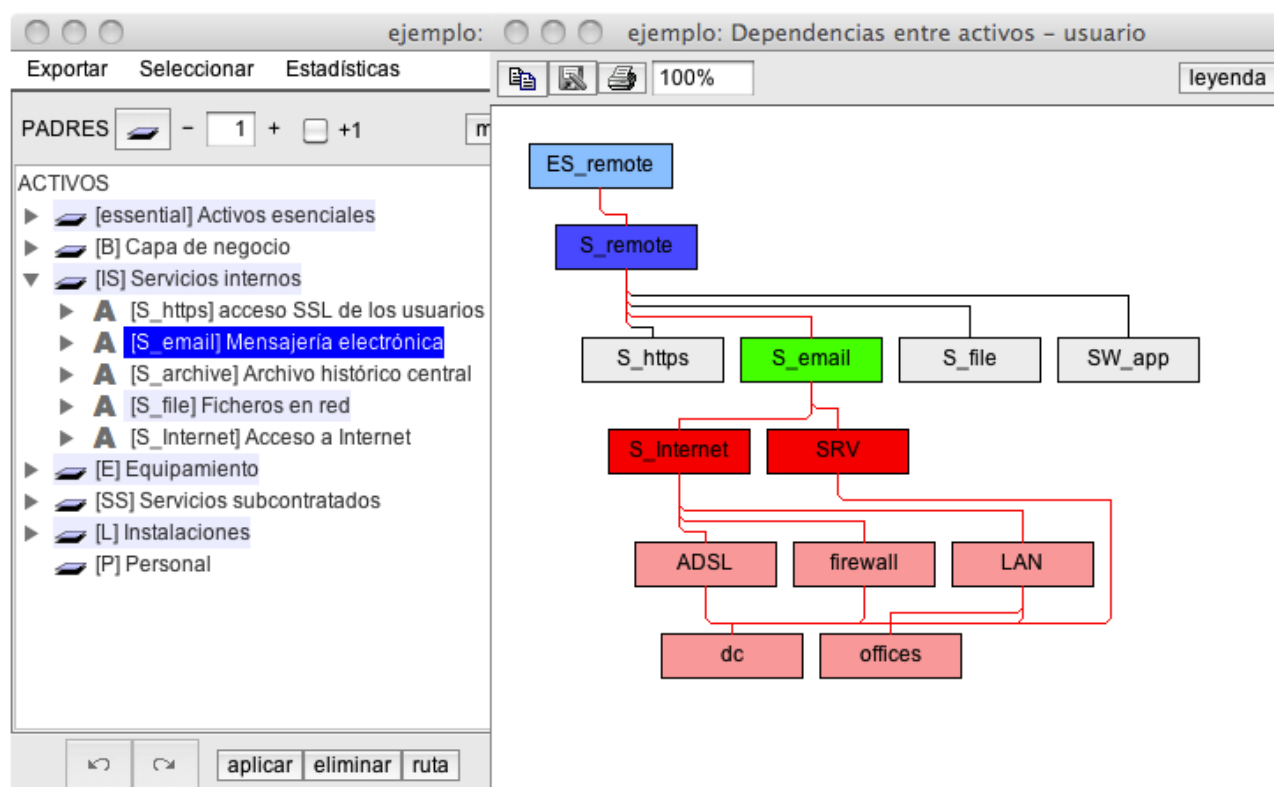
11.4.3. BUSES: DEPENDENCIAS ENTRE ACTIVOS

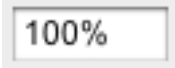
El gráfico muestra las relaciones de dependencia entre activos. Sólo presenta aquellos activos seleccionados en el panel principal y los relacionados con los seleccionados. Si no se selecciona nada, se presentan todos los activos.

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

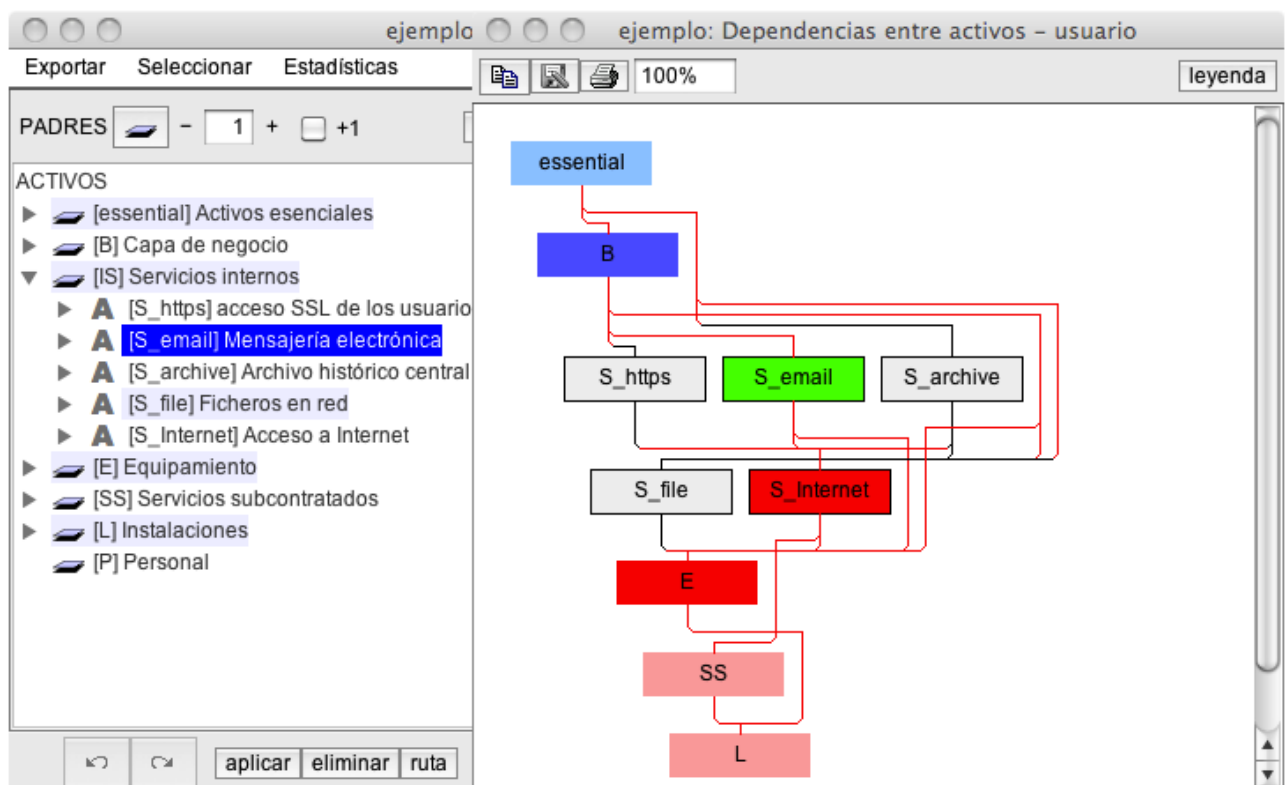
11.4.4.BLOQUES: DEPENDENCIAS ENTRE ACTIVOS

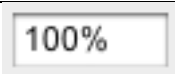
El gráfico muestra las relaciones de dependencia entre activos. Sólo se presentan los activos que se pueden ver en la pantalla principal, respetando lo que está expandido o colapsado en dicha pantalla.

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

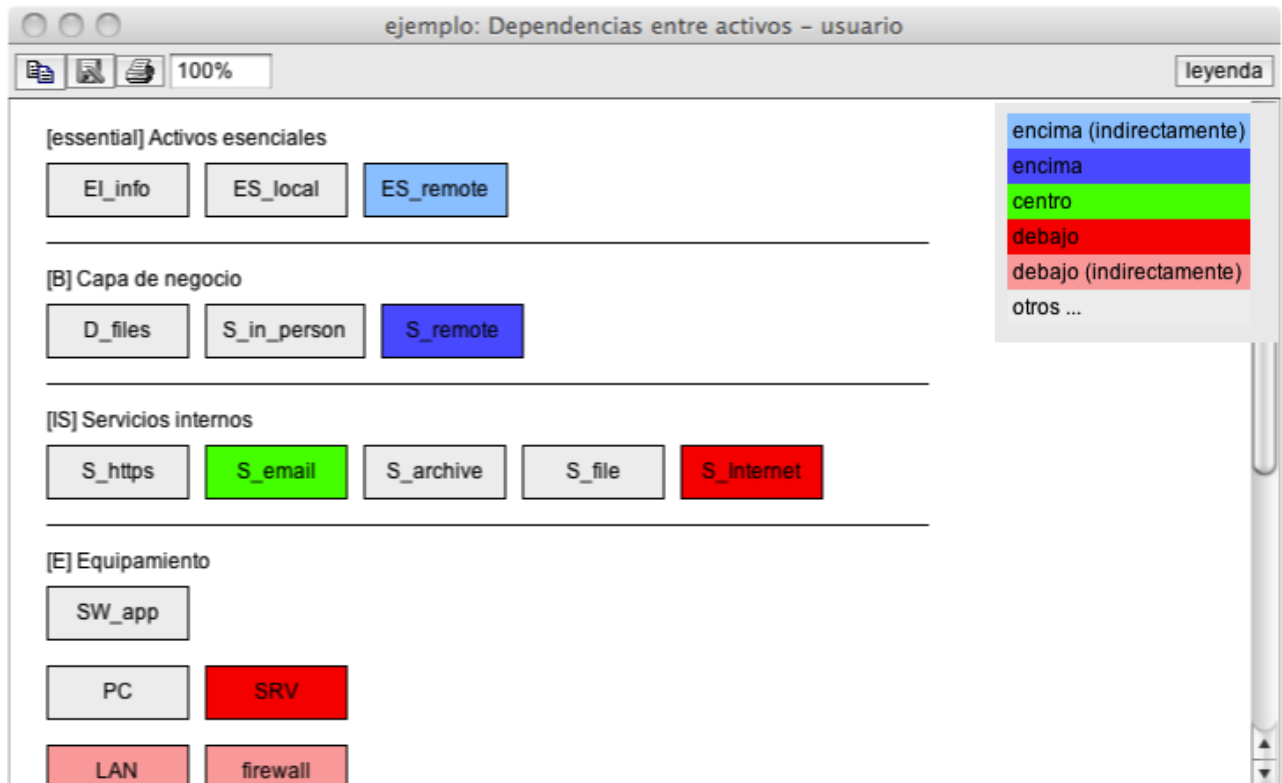
11.4.5. MAPA DE DEPENDENCIAS ENTRE ACTIVOS

Este mapa sirve para estudiar gráficamente las dependencias entre activos.

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

Cuando se selecciona un activo, el mapa se colorea:

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



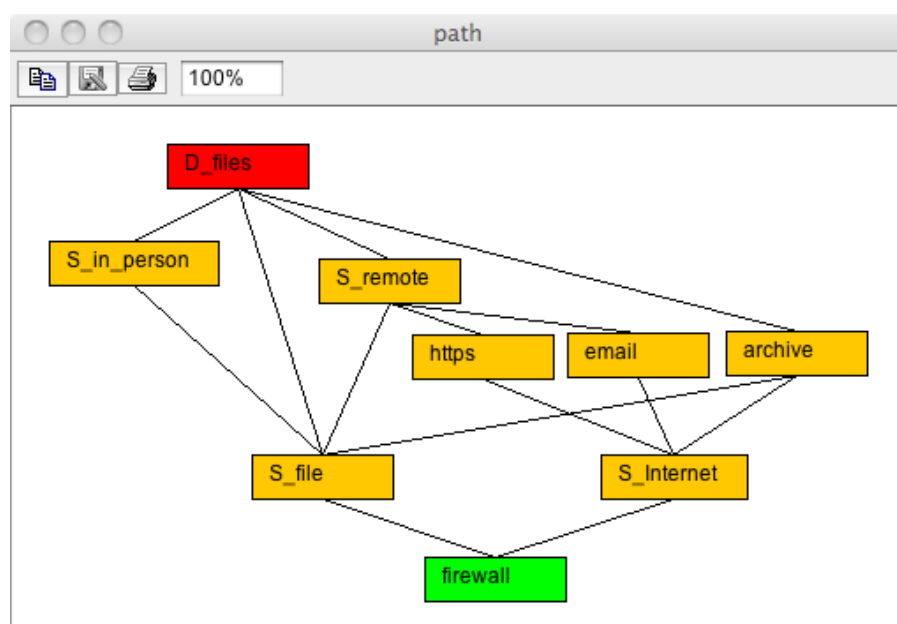
Para modificar las dependencias

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

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

Para describir la vía de dependencia entre un activo y otro

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



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

11.4.6. DEPENDENCIAS POR DIMENSIÓN DE SEGURIDAD

NOTA

PILAR mantiene en esa sección todas las dimensiones por compatibilidad con la herramienta general de análisis de riesgos multidimensional.

En el futuro puede que esta ventana se reduzca a tratar la dimensión de disponibilidad.

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

Dimensión	0	B	M	A	MA	T	Porcentaje
D	☒	☐	☐	☐	☐	☐	0%
I	☐	☐	☐	☐	☐	☒	100%
C	☐	☐	☐	☐	☐	☒	100%
A	☐	☐	☐	☐	☐	☒	100%
T	☐	☐	☐	☐	☐	☒	100%

comentario

ok cancelar

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 transporte 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.

11.5. 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

11.5.1. 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.

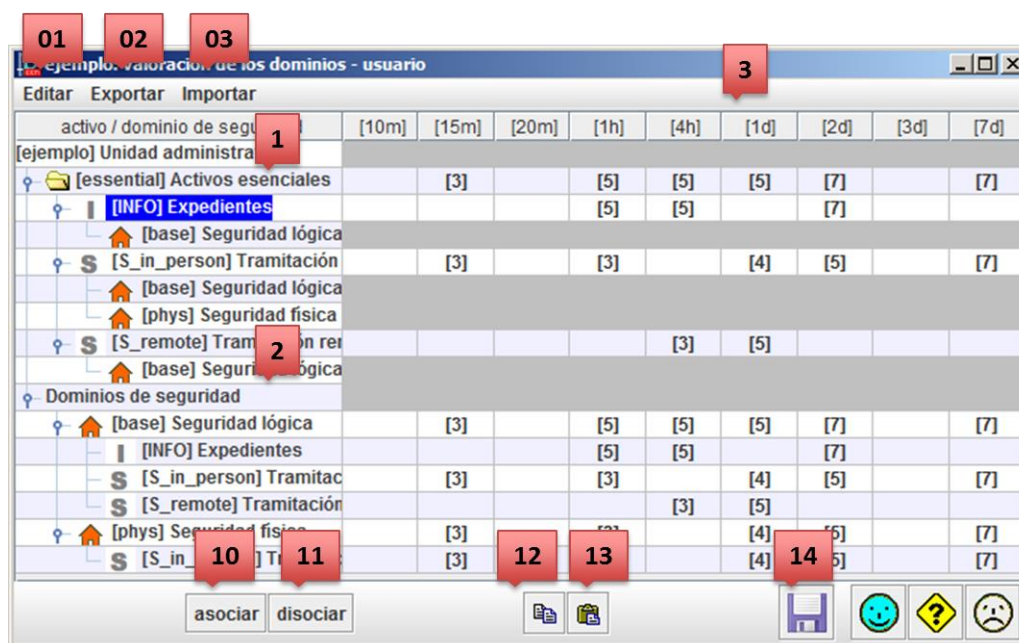
Supongamos que tenemos 2 dominios de seguridad

-  [base] Seguridad lógica
-  [phys] Seguridad física



activo / dominio de seguridad	[10m]	[15m]	[20m]	[1h]	[4h]	[1d]	[2d]	[3d]	[7d]
[ejemplo] Unidad administrativa									
[-] [essential] Activos esenciales		[3]		[5]	[5]	[5]	[7]		[7]
[-] [INFO] Expedientes				[5]	[5]		[7]		
[-] [S_in_person] Tramitación		[3]		[3]		[4]	[5]		[7]
[-] [S_remote] Tramitación remota					[3]	[5]			
[-] Dominios de seguridad									
[-] [base] Seguridad lógica		[3]		[5]	[5]	[5]	[7]		[7]
[-] [phys] Seguridad física		[3]		[3]		[4]	[5]		[7]

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	escalones	Tantas columnas como escalones de interrupción Ver “ <i>Escalones de interrupción</i> ”.
4	valor de los activos	Para cada activo esencial y cada escalón de interrupción, el valor — Ver <i>Activos / Valoración / cualitativo</i> — Ver <i>Activos / Valoración / cuantitativo</i>
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 los 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.

Para empezar rápidamente

¿Cuál es el escalón de interrupción que marca una diferencia significativa en las consecuencias para el negocio o servicio?

Sea [1d] (un día);

- vaya a la celda bajo título [1d], y
- 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.

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.

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

11.5.2. VALORACIÓN ACTIVO POR ACTIVO

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

Para empezar rápidamente

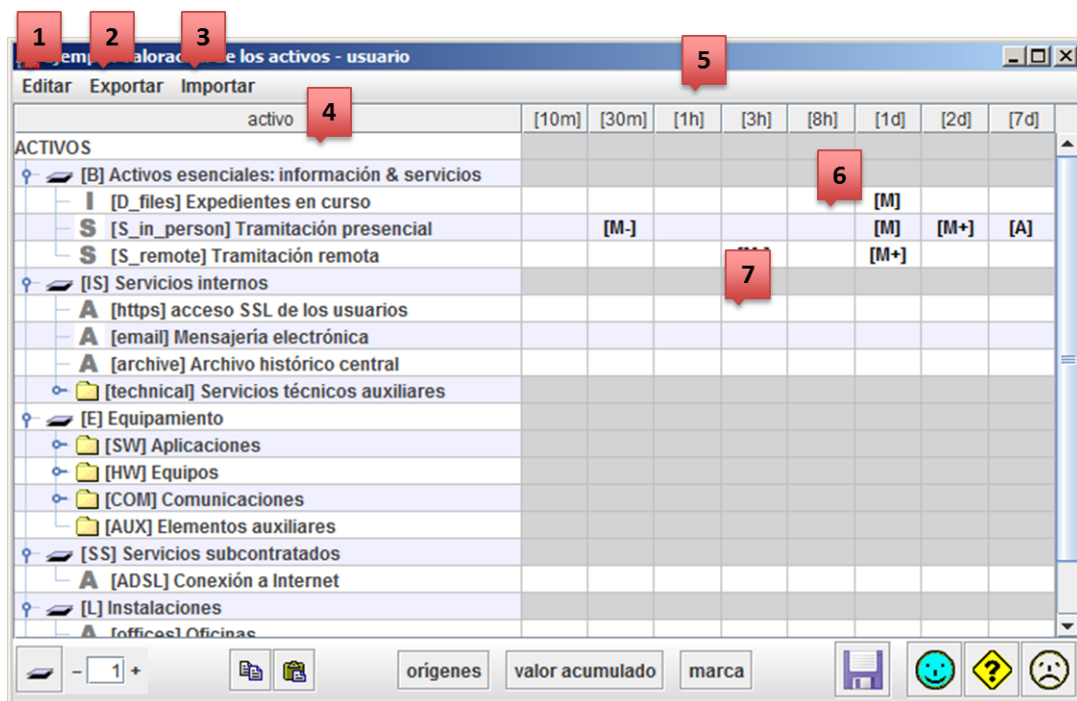
¿Cuál es su principal preocupación respecto de este sistema de información?

- Seleccione un activo (la fila)
- seleccione el intervalo de interrupción que marca una diferencia importante en las consecuencias (columna)
- haga doble clic para seleccionar un valor entre 0 (insignificante) y 10 (absolutamente crítico)
... o algún valor intermedio.

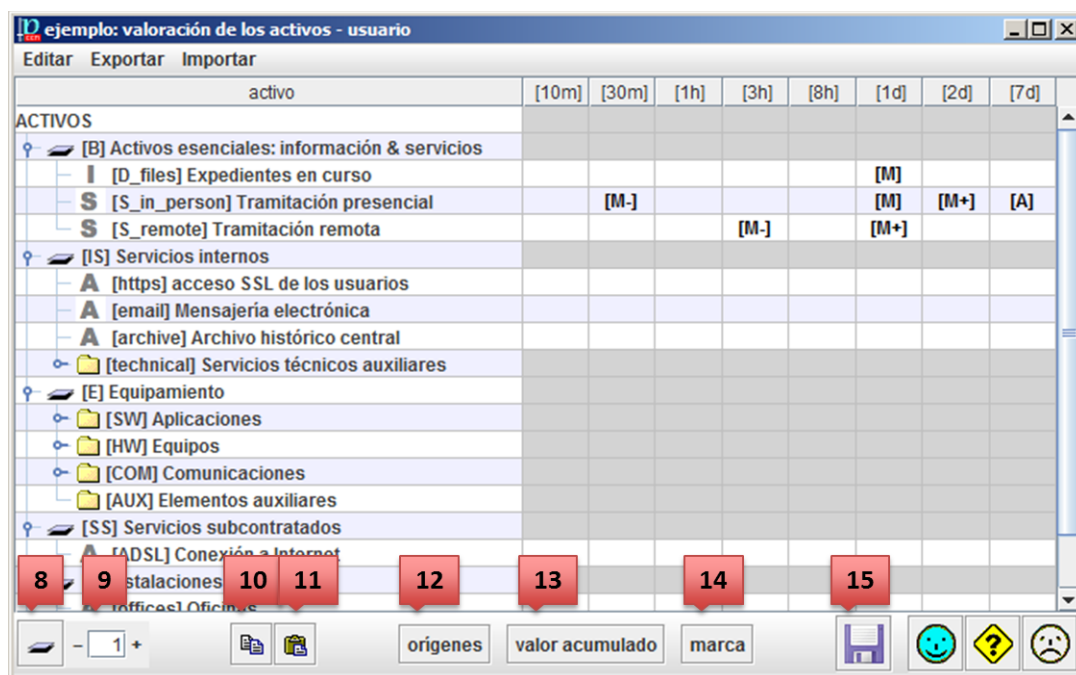
Repita los pasos anteriores con la demás preocupaciones en orden decreciente hasta que considere que el resto de asuntos no son tan importantes.

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 intervalo de interrupción.



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	escalones	Tantas columnas como escalones de interrupción Ver “ <i>Escalones de interrupción</i> ”.																																																														
6	valor	Para cada activo y cada escalón de interrupción. Cuando se presenta el valor propio, el valor aparece sobre fondo blanco																																																														
7		<table><tr><td></td><td></td><td></td><td>[5]</td><td>[5]</td><td></td><td>[7]</td><td></td><td>6</td></tr><tr><td></td><td>[3]</td><td></td><td>[3]</td><td></td><td>[4]</td><td>[5]</td><td></td><td>[7]</td></tr><tr><td></td><td></td><td></td><td></td><td>[3]</td><td>[5]</td><td></td><td></td><td></td></tr></table> Cuando se presenta en valor acumulado, aparece sobre fondo verdoso <table><tr><td></td><td>[3]</td><td>[3]</td><td>[3]</td><td>[3]</td><td>[5]</td><td>[5]</td><td>[5]</td><td>7</td></tr><tr><td></td><td>[3]</td><td>[3]</td><td>[3]</td><td>[3]</td><td>[5]</td><td>[5]</td><td>[5]</td><td>[7]</td></tr></table> Nótese que la acumulación trabaja en dos direcciones: • primero: de izquierda a derecha – el nivel de impacto en un intervalo es el mismo que en el intervalo anterior, salvo que se indique explícitamente un nuevo valor • en segundo lugar: de arriba a abajo – los activos inferiores acumulan los valores de los activos sobre él Cuando el análisis de riesgos es cuantitativo, los valores son cantidades numéricas: <table><tr><td></td><td>10K</td><td>10K</td><td>57K</td><td>67K</td><td>115K</td><td>310K</td><td>310K</td><td>480K</td></tr><tr><td></td><td>10K</td><td>10K</td><td>57K</td><td>67K</td><td>115K</td><td>310K</td><td>310K</td><td>480K</td></tr></table>				[5]	[5]		[7]		6		[3]		[3]		[4]	[5]		[7]					[3]	[5]					[3]	[3]	[3]	[3]	[5]	[5]	[5]	7		[3]	[3]	[3]	[3]	[5]	[5]	[5]	[7]		10K	10K	57K	67K	115K	310K	310K	480K		10K	10K	57K	67K	115K	310K	310K
			[5]	[5]		[7]		6																																																								
	[3]		[3]		[4]	[5]		[7]																																																								
				[3]	[5]																																																											
	[3]	[3]	[3]	[3]	[5]	[5]	[5]	7																																																								
	[3]	[3]	[3]	[3]	[5]	[5]	[5]	[7]																																																								
	10K	10K	57K	67K	115K	310K	310K	480K																																																								
	10K	10K	57K	67K	115K	310K	310K	480K																																																								



8		Haga clic para recoger el árbol de activos
9		Controla el nivel de despliegue del árbol de activos
10		Seleccione una o más celdas. Copie los 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:

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 intervalos de interrupción. Solamente los activos pueden recibir valores; las otras filas están muertas.

Para asignar un valor a un activo

1. seleccione el activo (fila) y el intervalo de interrupción (columna)
2. doble clic

La pantalla permite

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

Los criterios marcados determinan el nivel cualitativo asignado al activo en el intervalo indicado.

Cuando haya terminado ...

- OK para guardar los nuevos datos
- NO SE VALORA para quitarle el valor al activo
- CANCELAR para dejar el activo como estaba

11.5.3. VALORACIÓN CUALITATIVA

Para asignar un valor a un activo

- seleccione un activo (fila) y un escalón (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 la disponibilidad no tiene relevancia ni para ese activo ni propaga su valor a los activos de los que depende. Ver “ <i>Anulación de una valoración</i> ”.
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
----	--

11.5.4. 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

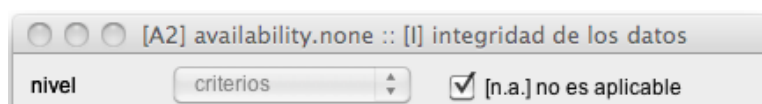
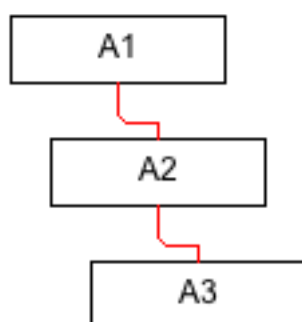
1	Marca el valor cualitativo. Si selecciona “CRITERIOS”, el valor lo decide la marca de mayor valor de los criterios marcados en [4]. Si selecciona un nivel, este será el asignado al activo, independientemente de los criterios marcados.
2	Se marca N.A. cuando la disponibilidad no tiene relevancia ni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

11.5.5. 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.



availability: valoración de los activos – usuario

Editar Exportar Importar

activo	[1d]	[2d]	[3d]	[4d]	[5d]
ACTIVOS					
▼ [E1]					
S [A1]		[3]	[3]	[3]	[3]
A [A2]	[n.a.]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
A [A3]					
▶ [E2]					
▶ [E3]					

- 2 + orígenes valor propio marca

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

11.5.6. VALORACIÓN DE LA DISPONIBILIDAD

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

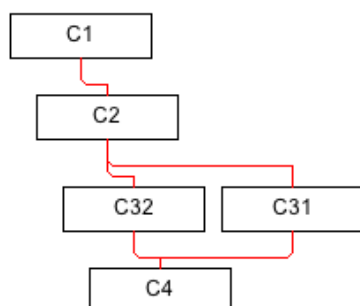
- por *dependencias*
- por *anulación* del valor,
- ajustando algunos calificativos del activo (ver a continuación).

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.



availability: valoración de los activos – usuario

Editar Exportar Importar

activo	[1d]	[2d]	[3d]	[4d]	[5d]
ACTIVOS					
▶ [E1]					
▶ [E2]					
▼ [E3]					
S [C1]			[3]	[3]	
A [C2] OR			[3]	[3]	
A [C31]					
A [C32]					
A [C4]			[3]	[3]	

- 2 + orígenes valor propio marca

11.6. AMENAZAS

11.6.1. 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*”).

Factores agravantes | atenuantes - usuario

1 criterios 2 dominios de seguridad

3 aplicar 4 eliminar 5 valor propio 6 marca 7 disco 8 sonrisa 9 interrogación 10 tristeza

Dominios de seguridad
 [base] Seguridad lógica
 [101] () Identificación del atacante
 [101.a] () público en general
 [103] () Beneficio del atacante
 [103.a] (5%) moderadamente interesado
 [104] () Motivación del personal interno
 [104.c] (5%) sobrecargados de trabajo
 [105] () Permisos de los usuarios (derechos)
 [105.a] (10%) se permite el acceso a Internet
 [111] () Conectividad del sistema de información
 [111.d] (30%) conectado a Internet
 [112] {xor} () Ubicación del sistema de información
 [112.a] (-20%) dentro de una zona controlada
 [phys] Seguridad física

[101] () Identificación del atacante
 [101.a] () público en general
 [101.b] (5%) competidor comercial
 [101.c] (5%) proveedor de servicios
 [101.d] (5%) grupos de presión política / activistas /
 [101.e] (5%) periodistas
 [101.f] (8%) criminales / terroristas
 [101.g] (10%) personal interno
 [101.h] (10%) bandas criminales
 [101.i] (10%) grupos terroristas
 [101.j] (20%) servicios de inteligencia
 [102] () Motivación del atacante
 [103] () Beneficio del atacante
 [103.a] (5%) moderadamente interesado
 [103.b] (10%) muy interesado
 [103.c] (20%) extremadamente interesado
 [104] () Motivación del personal interno
 [104.a] (-10%) todo el per está fuertemente m

	critérios	Selecione un dominio de seguridad en [4]. Haga clic en CRITERIOS. PILAR presenta en [5] los criterios que se aplican en el dominio seleccionado.
		Controla el despliegue del árbol de criterios.
	domínios	Selecione un criterio en [5]. Haga clic en DOMINIOS DE SEGURIDAD. PILAR selecciona en [4] los dominios a los que se aplica el criterio.
		Dominios de seguridad
		Criterios
	aplicar	Selecione 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.
	eliminar	Selecione 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.
		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)

11.6.2. 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.

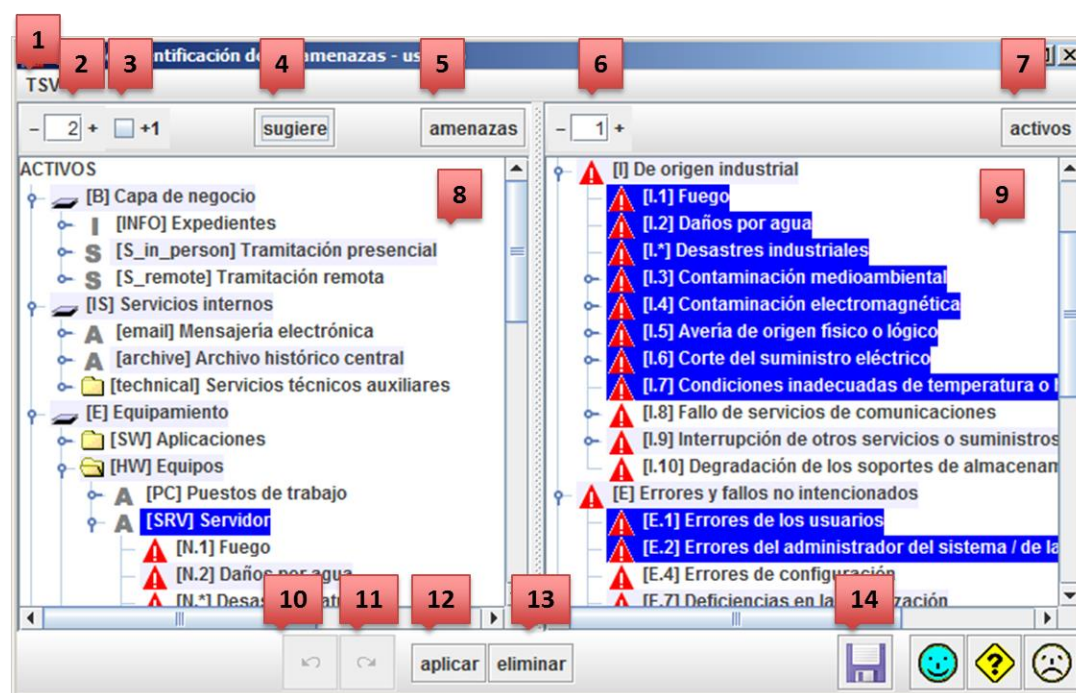
Aún más rápido

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 " <i>Threat Standard Values</i> "
---	-----	---------------------------------------

		Controla el despliegue del árbol de activos.
	+1	Ajusta el efecto de [2]. Si se marca [+1], PILAR muestra también las amenazas asociadas a cada activo.
	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.
	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.
		Controla el despliegue del árbol de amenazas.
	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.
		Activos
		Amenazas
		Revierte la última asociación de activos y amenazas.
		Reaplica la última asociación de activos y amenazas revertida.
	aplicar	— Seleccione uno o más activos a la izquierda ([8]). — Seleccione una o más amenazas a la derecha ([9]). — Haga clic en APLICAR. PILAR asocia las amenazas seleccionadas a los activos seleccionados.
	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.

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

11.6.3. VALORACIÓN

Para empezar rápidamente

Seleccione amenazas automáticas en *Opciones / Amenazas*

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

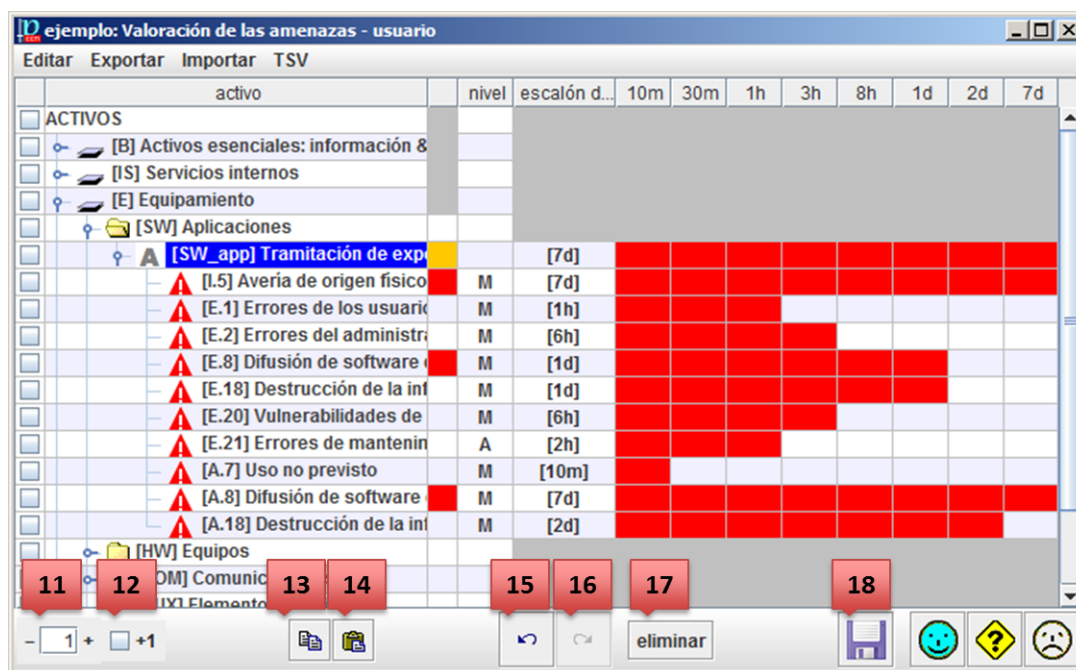


1	editar	opciones – ver <i>Editar / Opciones</i> copiar – ver [13] más abajo pegar – ver [14] más abajo
2	exportar	Genera un fichero CSV o XML
3	importar	Carga un fichero XML
4	TSV cargar aplicar	Ver “ <i>Threat Standard Values</i> ”. Carga un fichero TSV. Aplica los valores del fichero TSV a las filas seleccionadas; o sea, [5] y [6].



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.
5		Esta columna presenta la probabilidad de ocurrencia. El formato se puede ajustar en <i>Opciones / Probabilidad</i>
6		Esta columna presenta el intervalo de tiempo que estará el activo fuera de servicio en el supuesto de que no tengamos nada preparado. Hay que reconocer que es un valor estimado; pero nos servirá de referencia para más tarde.
7		Estas columnas presentan la gráficamente la interrupción causada por la amenaza. Es más estético que útil.
8	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 ([17]).
9		Activos y amenazas

10		Presentación gráfica de la interrupción causada.
----	--	--



11	- 1 +	Controla el despliegue del árbol de activos.
12	+1	Ajusta el despliegue ([11]). Si se marca [+1], PILAR muestra las amenazas asociadas a cada activo.
13		Seleccione una o más celdas en [5] o [6]. Haga clic para copiar los valores.
14		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.
15		Revierte los últimos cambios
16		Aplica de nuevo los últimos cambios revertidos
17	eliminar	— Seleccione una o más filas ([8]). — Haga clic en ELIMINAR. PILAR elimina los valores de las filas seleccionadas.

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

11.6.4. 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

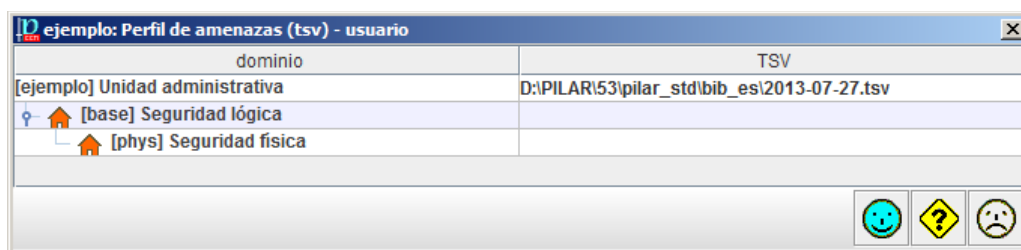
[<http://www.pilar-tools.com/es/tools/pilar/doc.htm>]

aunque también puede abrir el fichero con un editor XML

bib_es / threats.tsv

threats.tsv	significado
<pre><?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></pre>	formato: XML para cada activo de clase HW ... aplica la amenaza E.2 con frecuencia 1.0 y escalón de interrupción de [6h] ... y así sucesivamente ...

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. IMPACTO Y RIESGO POTENCIALES

11.7.1. IMPACTO Y RIESGO ACUMULADOS

Es una pantalla pasiva: sólo muestra resultados.

activo / amenaza	N	EDI	impacto	riesgo
ACTIVOS		120d	[A]	{6,9}
[B] Activos esenciales: información & servicios				
[IS] Servicios internos				
[E] Equipamiento				
[SW] Aplicaciones		7d	[A]	{6,9}
[HW] Equipos		20d	[A]	{6,9}
[PC] Puestos de trabajo		0s		
[SRV] Servidor		20d	[A]	{6,9}
[N.1] Fuego	B	[15d]	[A]	{5,6}
[N.2] Daños por agua	B	[7d]	[A]	{5,6}
[N.*] Desastres naturales	B	[20d]	[A]	{5,6}
[I.1] Fuego	M	[15d]	[A]	{6,4}
[I.2] Daños por agua	M	[7d]	[A]	{6,4}
[I.*] Desastres industriales	M	[15d]	[A]	{6,4}
[I.3] Contaminación medioambiental	M	[7d]	[A]	{6,8}
[I.4] Contaminación electromagnética	M	[2d]	[M+]	{5,1}
[I.5] Avería de origen físico o lógico	M	[2d]	[M+]	{5,1}
[I.6] Corte del suministro eléctrico	M	[10m]		{0}
[I.7] Condiciones inadecuadas de temperatura o humedad	M	[20d]	[A]	{6,8}
[I.10] Degradación de los soportes de almacenamiento	M	[20d]	[A]	{6,8}

1	selección	no se usa
---	-----------	-----------

2	activos	Árbol de activos y amenazas. Haga clic-clic para colapsar / expandir el árbol.
3	probabilidad	Ver “ <i>Opciones / Probabilidad</i> ”
4	EDI Escalón De Interrupción	Consecuencia de la amenaza sobre el activo
5	impacto	El impacto de la amenaza sobre el activo
6	riesgo	El riesgo de la amenaza sobre el activo

	activo / amenaza	N	EDI	impacto	riesgo
☐	ACTIVOS		120d	[A]	{6,9}
☐	[B] Activos esenciales: información & servicios				
☐	[IS] Servicios internos				
☐	[E] Equipamiento				
☐	[SW] Aplicaciones		7d	[A]	{6,9}
☐	[HW] Equipos		20d	[A]	{6,9}
☐	[PC] Puestos de trabajo		0s		
☐	[SRV] Servidor		20d	[A]	{6,9}
☐	[N.1] Fuego	B	[15d]	[A]	{5,6}
☐	[N.2] Daños por agua	B	[7d]	[A]	{5,6}
☐	[N.*] Desastres naturales	B	[20d]	[A]	{5,6}
☐	[I.1] Fuego	M	[15d]	[A]	{6,4}
☐	[I.2] Daños por agua	M	[7d]	[A]	{6,4}
☐	[I.*] Desastres industriales	M	[15d]	[A]	{6,4}
☐	[I.3] Contaminación medioambiental	M	[7d]	[A]	{6,8}
☐	[I.4] Contaminación electromagnética	M	[2d]	[M+]	{5,1}
☐	[I.5] Avería de origen físico o lógico	M	[2d]	[M+]	{5,1}
☐	[I.6] Corte del suministro eléctrico	M	[10m]		{0}
☐	[I.7] Condiciones inadecuadas de temperatura o humedad	M		[A]	{6,8}
☐	[I.8] Pérdida de los soportes de almacenamiento	M		[A]	{6,8}

10	- 1 +	Controla el despliegue del árbol de activos ([2])
11	+1	Ajusta el despliegue [10]. Si se selecciona [+1], PILAR presenta las amenazas sobre el activo.
12	dominio	Seleccione un dominio de seguridad. PILAR seleccionará los activos ([2]) en ese dominio.
13	fuelle	Seleccione una o más fuentes de información. PILAR seleccionará los activos ([2]) asociados a esa fuente.

14	leyenda	Ver <i>Riesgos / Niveles de criticidad / código de colores</i>
15	exportar html csv xml db	Extrae los valores de la tabla — a un fichero HTML — a un fichero CSV — a un fichero XML — a una base de datos externa (si la licencia lo permite)

11.7.2.IMPACTO Y RIESGO REPERCUTIDOS

activo / amenaza	N	EDI	impacto	riesgo
[D_files] Expedientes en curso		[120d]	[A]	{6,9}
[S_in_person] Tramitación presencial		[120d]	[M]	{5,7}
[S_in_person] Tramitación presencial		[120d]	[A]	{6,9}
[S_in_person] Tramitación presencial		[2d]	[M+]	{5,2}
[SW.SW_app] Tramitación de expedientes		[7d]	[A]	{6,9}
[HW.SRV] Servidor		[20d]	[A]	{6,9}
[N.1] Fuego	B	[15d]	[A]	{5,6}
[N.2] Daños por agua	B	[7d]	[A]	{5,6}
[N.*] Desastres naturales	B	[20d]	[A]	{5,6}
[I.1] Fuego	M	[15d]	[A]	{6,4}
[I.2] Daños por agua	M	[7d]	[A]	{6,4}
[I.*] Desastres industriales	M	[15d]	[A]	{6,4}
[I.3] Contaminación medioambiental	M	[7d]	[A]	{6,8}
[I.4] Contaminación electromagnética	M	[2d]	[M+]	{5,1}
[I.5] Avería de origen físico o lógico	M	[2d]	[M+]	{5,1}
[I.6] Corte del suministro eléctrico	M	[10m]		{0}
[I.7] Condiciones inadecuadas de temperatura o humedad	M	[20d]	[A]	{6,8}
[I.10] Degradación de los soportes de almacenamiento de	M	[20d]	[A]	{6,8}
[E.1] Errores de los usuarios	M	[1h]	[M-]	{3,5}
[E.2] Errores del administrador del sistema / de la seguridad	M	[6h]	[M-]	{3,5}

1	selección	no se usa
2	activos	Árbol de activos y amenazas. Incluye los activos superiores, con valor propio, y los activos inferiores, con valor acumulado, sobre los que se materializan las amenazas que luego repercuten sobre los activos superiores. Haga clic-clic para colapsar / expandir el árbol.
3	probabilidad	Ver “ <i>Opciones / Probabilidad</i> ”
4	EDI Escalón De	Consecuencia de la amenaza sobre el activo

	Interrupción	
5	impacto	El impacto de la amenaza sobre el activo. Se presentan valores repercutidos sobre los activos superiores y acumulados sobre los inferiores.
6	riesgo	El riesgo de la amenaza sobre el activo. Se presentan valores repercutidos sobre los activos superiores y acumulados sobre los inferiores.

ejemplo: riesgo repercutido - usuario

	activo / amenaza	N	EDI	impacto	riesgo
☐	ACTIVOS		[120d]	[A]	{6,9}
☐	[D_files] Expedientes en curso		[120d]	[M]	{5,7}
☐	[S_in_person] Tramitación presencial		[120d]	[A]	{6,9}
☐	[S_in_person] Tramitación presencial		[2d]	[M+]	{5,2}
☐	[SW.SW_app] Tramitación de expedientes		[7d]	[A]	{6,9}
☐	[HW.SRV] Servidor		[20d]	[A]	{6,9}
☐	[N.1] Fuego	B	[15d]	[A]	{5,6}
☐	[N.2] Daños por agua	B	[7d]	[A]	{5,6}
☐	[N.*] Desastres naturales	B	[20d]	[A]	{5,6}
☐	[L.1] Fuego	M	[15d]	[A]	{6,4}
☐	[L.2] Daños por agua	M	[7d]	[A]	{6,4}
☐	[L.*] Desastres industriales	M	[15d]	[A]	{6,4}
☐	[L.3] Contaminación medioambiental	M	[7d]	[A]	{6,8}
☐	[L.4] Contaminación electromagnética	M	[2d]	[M+]	{5,1}
☐	[L.5] Avería de origen físico o lógico	M	[2d]	[M+]	{5,1}
☐	[L.6] Corte del suministro eléctrico	M	[10m]		{0}
☐	[L.7] Condiciones inadecuadas de temperatura o humedad	M	[20d]	[A]	{6,8}
☐	[L.10] Degradación de los soportes de almacenamiento de	M	[20d]	[A]	{6,8}
☐	[] Soportes de los usuarios	M		[M-]	{3,5}
☐	[] Soportes del administrador d	M		[M-]	{3,5}

10 12 13 14 15

- 1 + dominio fuente leyenda html csv xml db

10	- 1 +	Controla el despliegue del árbol de activos ([2])
12	dominio	Seleccione un dominio de seguridad. PILAR seleccionará los activos ([2]) en ese dominio.
13	fuelle	Seleccione una o más fuentes de información. PILAR seleccionará los activos ([2]) asociados a esa fuente.
14	leyenda	Ver <i>Riesgos / Niveles de criticidad / código de colores</i>
15	exportar html csv xml db	Extrae los valores de la tabla — a un fichero HTML — a un fichero CSV — a un fichero XML — a una base de datos externa (si la licencia lo permite)

11.8. EQUIPAMIENTO DE RESPALDO

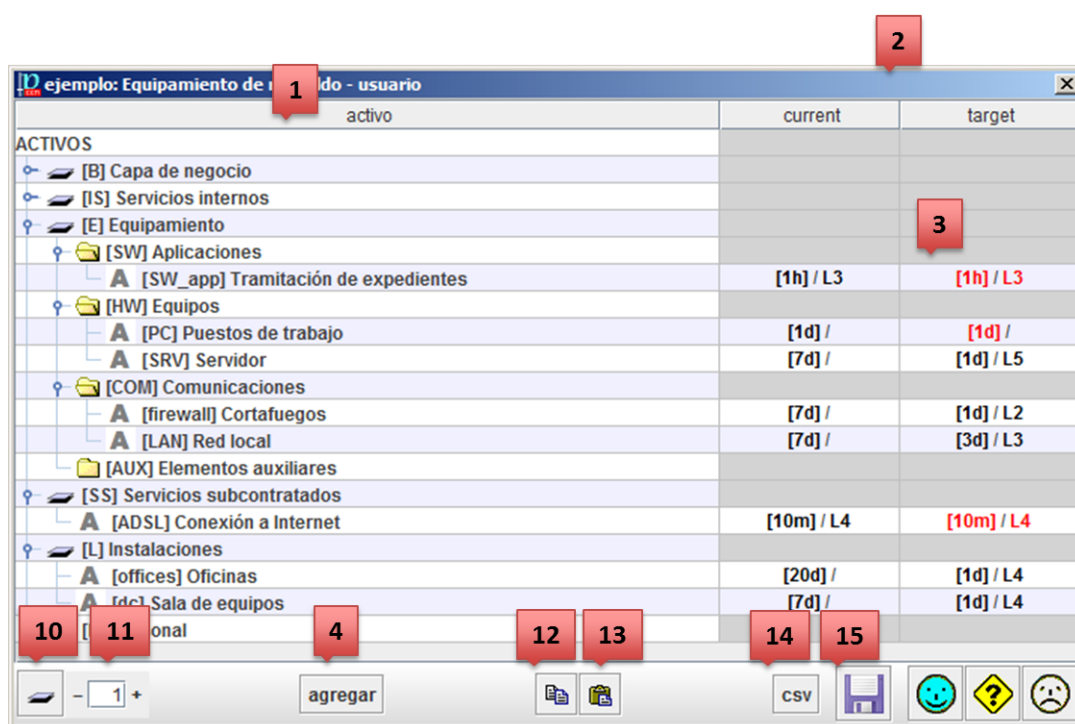
Si disponemos de medios alternativos preparados para reemplazar a los medios habituales en caso de desastre, podremos contar con limitar el impacto de un incidente a niveles aceptables.

En esta pantalla se introducen los tiempos de entrada en servicio de los medios alternativos. Estos tiempos pueden diferir de una fase a la siguiente típicamente porque mejoramos la capacidad de respuesta de la Organización.

- La existencia de un equipo de respaldo a partir de una fase y hasta que cambiemos, se indica en NEGRO.
- Si una fase no se indica ningún dato, se utiliza el valor de una fase anterior (ROJO).
- Si ninguna fase tiene valor alguno, significa que no hay equipo del respaldo.

También se introduce, asociado a cada mecanismo de respaldo, la madurez del proceso que soporta la sustitución del activo.

- Si una fase no indica madurez, se utiliza el valor de una fase anterior (ROJO).



1	activos	Árbol de activos. Haga clic en la manivela o clic-clic en el texto para expandir / comprimir el árbol.
2	fases	Una columna por fase del proyecto

	valores	[escalón de interrupción] / madurez del proceso de entrada en operación. Haga clic-clic para <u>editar los valores</u> Los valores explícito se muestran en letra negra. Si una celda carece de valor explícito, PILAR muestra en rojo en valor que se arrastra de la fase anterior (si las fases están interconectadas; ver “ <u>Opciones / Fases del proyecto</u> ”).
	agregar	PILAR presenta las consecuencias sobre los activos esenciales de los tiempos de recuperación de los activos de los que depende. Ver “ <u>Backup / agregado</u> ”
		Haga clic para colapsar el árbol ([1]) a nivel de capas
		Controla el despliegue del árbol de activos ([1])
		Seleccione una o más celdas en [3]. Haga clic para copiar los valores.
		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.
	CSV	Exporta los datos a un fichero en formato CSV
		Guarda el proyecto en su fichero o en su base de datos.

11.8.1. VALORES AGREGADOS

Pilar calcula las consecuencias para los activos esenciales del backup que hayamos previsto para el equipamiento del que depende cada uno.

Se presentan los datos calculados sobre fondo verdoso.

ejemplo: Equipamiento de respaldo - usuario

activo	current	target
ACTIVOS		
[B] Capa de negocio		
[I] [INFO] Expedientes	1d/L4	1d/L4
[S_in_person] Tramitación presencial	20d/_L3	3d/_L5
[S_remote] Tramitación remota	20d/_L4	3d/_L5
[IS] Servicios internos		
[A_email] Mensajería electrónica	[4h] / L2	[4h] / L2
[A_archive] Archivo histórico central	[10m] /	[10m] /
[technical] Servicios técnicos auxiliares		
[A_S_file] Ficheros en red	20d/_L0	3d/_L5
[A_S_Internet] Acceso a Internet	20d/_L4	3d/L0-L4
[E] Equipamiento		
[SW] Aplicaciones		
[A_SW_app] Tramitación de expedientes	[1h] / L3	[1h] / L3
[HW] Equipos		
[A_PC] Puestos de trabajo	[1d] /	[1d] /
[A_SRV] Servidor	[7d] /	[1d] / L5
[COM] Comunicaciones		
[A_firewall] Cortafuegos	[7d] /	[1d] / L2
[A_11_AMI Red local]	[7d] /	[3d] / L3

agregar csv [1] [emojis]

Se calculan valores agregados para

- activos esenciales, información o servicios
- puntos de acceso al servicio ([null.sap])

Para ello

- se tiene en cuenta el peor tiempo de recuperación de los activos de los que depende
- el mejor tiempo de respuesta de las opciones OR

y se muestra el rango de valores de madurez de los elementos involucrados.

PILAR requiere datos de tiempo de recuperación para todos los activos involucrados, salvo que haya nodos OR, en cuyo caso pueden haber opciones no valoradas que PILAR ignora.

Por simplificar la entrada de datos, PILAR también acepta que no se valoren

- activos esenciales
- activos OR
- puntos de acceso a servicios [null.sap]

Esta pantalla nos permite saber si satisfacemos nuestros objetivos RTO para servicios.

11.8.2. RESPALDO / EDICIÓN

Haciendo clic-clic o haciendo clic con el botón derecho, pasará a una ventana donde puede introducir o modificar la información relativa al equipamiento de respaldo.

Si lo hace sobre un activo suelto, los datos se aplican al activo en cuestión. Si lo hace sobre un grupo de activos, sobre una capa o sobre el árbol completo, los datos se aplican uniformemente a todos los activos que queden englobados.

1	tiempo	Aquí se introduce el tiempo que tardaremos en reponer el activo; es decir, el cierre de la interrupción. Ver “ <u>escalones / formato</u> ”.
2	madurez	Madurez del proceso de entrada en servicio del equipo de respaldo. Ver “ <u>Opciones / Madurez</u> ”.
3	comentario	Explicación informal. Haciendo clic con el botón derecho, puede Selecciona un texto. Puede cortarlo para pegarlo después. Puede copiarlo para pegarlo después. Puede pegar lo que haya cortado o copiado. Puede interpretarlo como una URL.
4	opciones	Es informativo, indicando el mecanismo de que se dispone para alcanzar el tiempo previsto de recuperación.
10	cancelar	Cierra la ventana sin modificar los valores anteriores

11	no hay respaldo	Cierra la ventana eliminando los valores de tiempo y madurez; es decir, no hay respaldo para este activo en esta fase
12	aplicar	Cierra la ventana, reteniendo los datos introducidos

11.9. SALVAGUARDAS

11.9.1. ASPECTO

Aspecto que trata la salvaguardas

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

11.9.2. 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

11.9.3. PESO RELATIVO

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

11.9.4. INFORMACIÓN ADICIONAL

Una ventana separada presenta información adicional relativa a la salvaguarda



11.9.5. 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

11.9.6. IDENTIFICACIÓN

Para empezar rápidamente

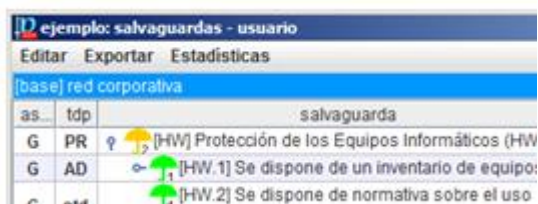
- Seleccione el botón RECOMENDACIÓN en la barra inferior.
- OK.

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.

11.9.6.1. Menús barra superior

**Menú EDITAR**

Ver “Salvaguardas / Buscar”.

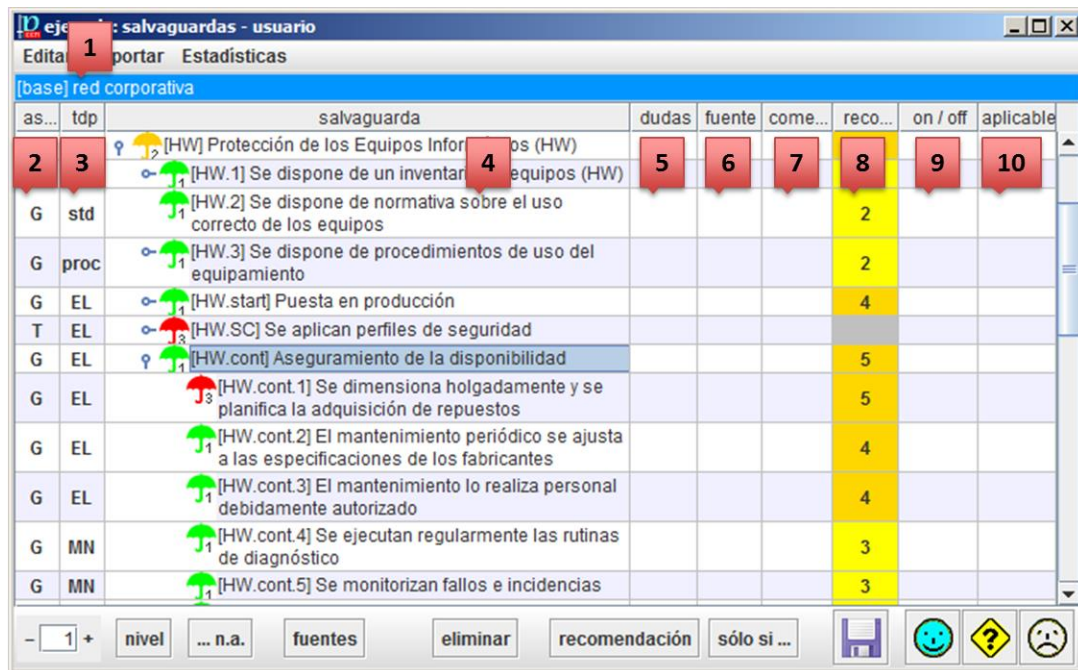
Menú EXPORTAR

Genera un informe: “SoA – Declaración de Aplicabilidad”.

Menú ESTADÍSTICAS

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

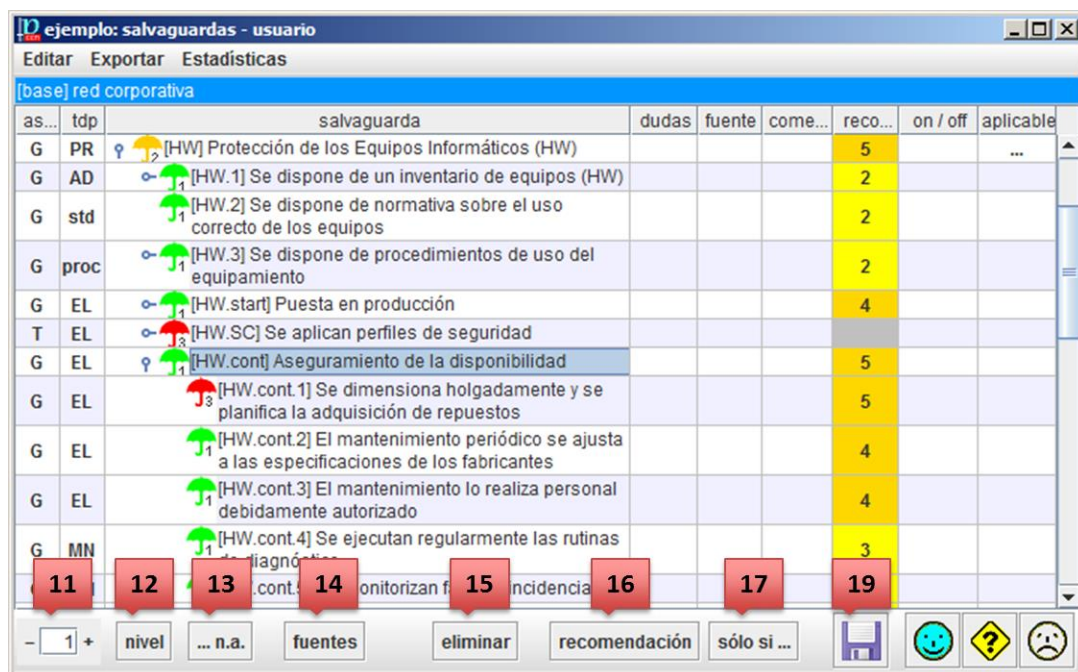
11.9.6.2. Pantalla principal, cuerpo



1	dominio de seguridad	Pueden haber diferentes salvaguadas en diferentes dominios. Haga clic para seleccionar el dominio en el que vamos a trabajar.
2	aspecto	Ver “ <u>Salvaguadas / Aspecto</u> ”.
3	tdp	Ver “ <u>Salvaguadas / Tipo de protección</u> ”.
4		Árbol de salvaguadas. Haga clic-clic para colapsar / expandir el árbol. Clic con el botón derecho para acceder a <u>Salvaguadas / tree</u>
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 salvaguada (la marcada y sus descendientes).
7	comentario	Haga clic para asociar un comentario a la salvaguada.

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.

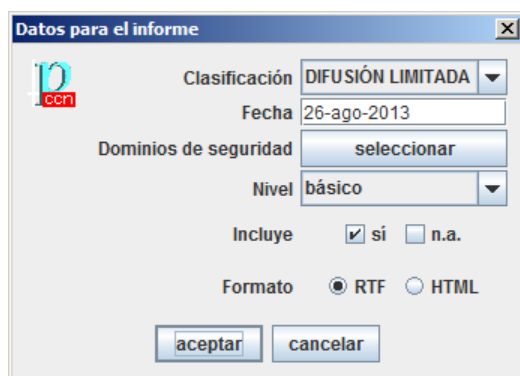
11.9.6.3. Barra inferior de herramientas



11	- 1 +	Controla el despliegue del árbol de salvaguardas.
12	nivel	PILAR tiene 3 niveles predefinidos de expansión. BÁSICO expande las secciones principales, sin detalles. EXPERTO expande hasta el último detalle. MEDIO se queda entre BÁSICO y EXPERTO.
13	... n.a.	Expande el árbol lo suficiente para que se vean todos los n.a.
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.
18	SoA	Genera un informe: “ <i>SoA – Declaración de Aplicabilidad</i> ”.
19		Guarda el proyecto en su fichero o en su base de datos.

11.9.7. 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 <i>Datos del proyecto</i> . Aquí se puede poner una marca más restrictiva.
Fecha	La fecha por defecto es HOY.
Dominios de seguridad	Puede seleccionar un subconjunto de los dominios para el informe. Mientras no indique lo contrario, se imprimen todos.
Nivel	BÁSICO salvaguardas más importantes, sin mucho detalle EXPERTO máximo nivel de detalle MEDIO algo intermedio entre BÁSICO y EXPERTO
Incluye	Puede incluir sólo las salvaguardas que aplican, sólo las que no, o ambas categorías.
Format0	El formato RTF es útil para documentos. El formato HTML es útil para intranets.

11.9.8. VALORACIÓN POR DOMINIOS

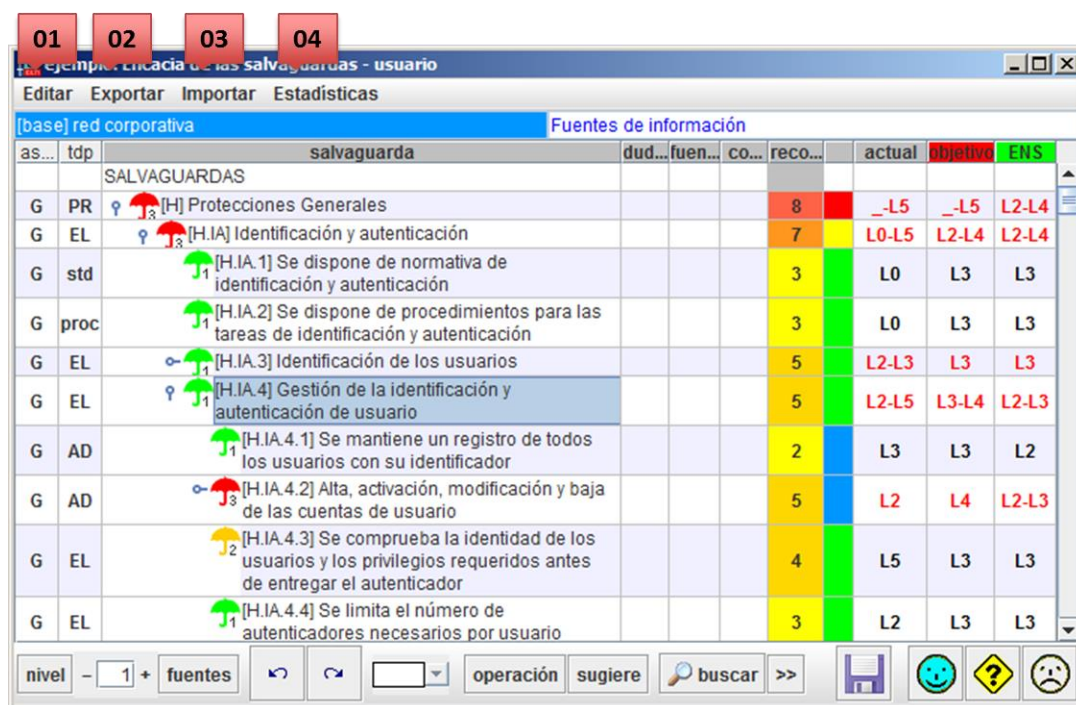
Para empezar rápidamente

- 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).

11.9.8.1. 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 “<u>Salvaguardas / Buscar</u>”
02	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 <u>Salvaguardas / Fases de referencia y objetivo</u>

03	importar	Lee los niveles de madures de un fichero, CSV o XML.
04	estadísticas	Genera una tabla resumen con al número de salvaguardas evaluadas en cada dominio de seguridad.

11.9.8.2. 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 “ <u>Salvaguardas / Aspecto</u> ”.
4	tdp	Ver “ <u>Salvaguardas / Tipo de protección</u> ”.
5		Árbol de salvaguardas. Haga clic-clic para colapsar / expandir el árbol. Clic con el botón derecho para acceder a <u>Salvaguardas / tree</u>

	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.
	fuentes	Haga clic para asociar fuentes de información a la salvaguarda (la marcada y sus descendientes).
	comentario	Haga clic para asociar un comentario a la salvaguarda.
	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.
	semáforo	Ver “ <u>Salvaguardas / Fases de referencia y objetivo</u> ”.
		Fases del proyecto
		Ver “ <u>Valoración de salvaguardas por dominios</u> ”.

11.9.8.3. Barra inferior de herramientas



13	nivel	PILAR tiene 3 niveles predefinidos de expansión. BÁSICO expande las secciones principales, sin detalles. EXPERTO expande hasta el último detalle. MEDIO se queda entre BÁSICO y EXPERTO.
14	- 1 +	Controla el despliegue del árbol de salvaguuardas.
15	fuentes	Seleccione una o más fuentes de información. PILAR seleccionará todas las salvaguuardas a las que está asociada.
16		Revierte los últimos cambios
17		Rehace los últimos cambios revertidos
18		Con el combo puede elegir una madurez para las <u>Salvaguuardas / Valoración / Operaciones</u>
19	operación	Ver “ <u>Salvaguuardas / Valoración / Operaciones</u> ”.
20	sugiere	Ver “ <u>Salvaguuardas / Sugiere</u> ”.

21		Ver “ <u>Salvaguadas / Buscar</u> ”.
22	>>	Ver “ <u>Salvaguadas / Buscar</u> ”.
23		Guarda el proyecto en su fichero o en su base de datos.

11.9.9. VALORACIÓN POR ACTIVOS

Esta pantalla permite el especificar si la evaluación de las salvaguadas 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		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 ().

	editar	Haga clic para editar valores de madurez específicos del activo
		Haga clic para colapsar el árbol a nivel de capas
		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 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”.



as...	tdp	salvaguarda	du...	fue...	co...	re...	act...	obj...	PIL
SALVAGUARDAS									
G	PR	[H] Protecciones Generales				8	---	---	---
G	EL	[H.IA] Identificación y autenticación				7	---	---	---
G	std	[H.IA.1] Se dispone de normativa de identificación y autenticación				3	---	---	L3
G	proc	[H.IA.2] Se dispone de procedimientos para las tareas de identificación y autenticación				3	---	---	L3
G	EL	[H.IA.3] Identificación de los usuarios				5	---	---	---
G	EL	[H.IA.4] Gestión de la identificación y autenticación de usuario				5	---	---	---
G	EL	[H.IA.5] Cuentas especiales (administración)				5	---	---	---
G	EL	[H.IA.5.1] Hay cuentas específicas para administradores del sistema				4	L5	L5	L3
G	EL	[H.IA.5.2] Hay cuentas específicas para administradores de seguridad				5	L5	L5	L3
G	EL	[H.IA.5.3] Hay cuentas específicas para actividades de auditoría				3	L5	L5	L3
G	EL	[H.IA.5.4] Las cuentas especiales están sujetas a							

11.9.10. 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

11.9.11. 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 “*Salvuardas / Valoración / Operaciones*”
- puede usar las operaciones copiar y pegar del menú EDITAR ([01]) para trasladar el valor de unas celdas a otras

En salvuardas de tipo XOR, podemos indicar cual es 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 salvuardas que realmente son un enlace a otra salvaguarda, no podremos establecer una valoración: hay que ir al sitio enlazado.

11.9.12. OPERACIONES

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

APLICAR

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

RELLENAR

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

PREDECIR

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

SIMPLIFICAR

elimina valores que pueden ser heredados, bien del dominio inferior, bien de la fase anterior;
es útil cuando estamos moviendo las fases arriba y abajo para buscar el orden óptimo de ejecución

MÍNIMOS

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

RECOMENDACIÓN

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

11.9.13. OPERACIÓN SUGERENCIA

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

ejemplo: Eficacia de las salvaguardas - usuario

Editar Exportar Importar Estadísticas

[base] Seguridad lógica Fuentes de información

as...	tdp	salvaguarda	du...	fue...	co...	re...	act...	obj...	PIL...
F	CR	[AUX.power.6.4] Redundancia				5	L0	L1...	L3
F	CR	[AUX.power.6.4.1] Sistema de alimentación ininterrumpida (SAI) que permite el funcionamiento de los equipos críticos, hasta su correcto cierre y apagado				3	L0	L3	L3
F	CR	[AUX.power.6.4.2] Sistema de alimentación redundante que garantiza el funcionamiento de los equipos críticos, y la continuidad de las operaciones				5	L0	L1	L3
F	CR	[AUX.power.6.4.3] Acometida redundante (dos suministradores)				5	L0	L1	L3
F	PR	[AUX.AC] Climatización				6	L0...	L3	L3...
F	FI	[AUX.wires] Protección del cableado					L0	L4	n.a.

[HW.cont.a.1] Equipo de alta disponibilidad con sistema de almacenamiento RAID

[AUX.power.6.4.2] Sistema de alimentación redundante que garantiza el funcionamiento de los equipos críticos, y la contin

[AUX.power.6.4.3] Acometida redundante (dos suministradores)

[H.IR.4.1] Se previene la fuga de información

[H.IR.4.2] Se garantiza la integridad de la información

nivel - 1 + fuentes

operación sugiere buscar >>

11.9.14. 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

11.9.15. NORMATIVA DE SEGURIDAD

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

Ver “Valoración de salvaguardas por dominios”.

11.9.16. 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”.

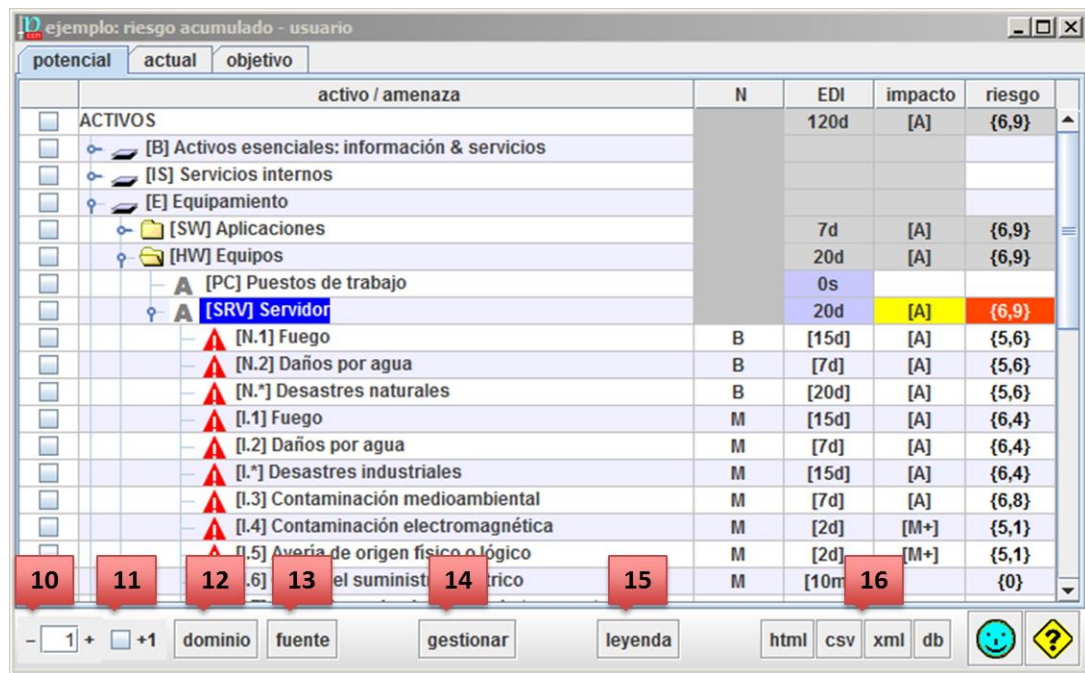
11.10. IMPACTO Y RIESGO RESIDUALES

11.10.1. TABLA DE IMPACTO Y RIESGO ACUMULADO

activo / amenaza	N	EDI	impacto	riesgo
ACTIVOS		120d	[A]	{6,9}
[B] Activos esenciales: información & servicios				
[IS] Servicios internos				
[E] Equipamiento				
[SW] Aplicaciones		7d	[A]	{6,9}
[HW] Equipos		20d	[A]	{6,9}
[PC] Puestos de trabajo		0s		
[SRV] Servidor		20d	[A]	{6,9}
[N.1] Fuego	B	[15d]	[A]	{5,6}
[N.2] Daños por agua	B	[7d]	[A]	{5,6}
[N.*] Desastres naturales	B	[20d]	[A]	{5,6}
[I.1] Fuego	M	[15d]	[A]	{6,4}
[I.2] Daños por agua	M	[7d]	[A]	{6,4}
[I.*] Desastres industriales	M	[15d]	[A]	{6,4}
[I.3] Contaminación medioambiental	M	[7d]	[A]	{6,8}
[I.4] Contaminación electromagnética	M	[2d]	[M+]	{5,1}
[I.5] Avería de origen físico o lógico	M	[2d]	[M+]	{5,1}
[I.6] Corte del suministro eléctrico	M	[10m]		{0}

1	selección	Selecciona qué activos serán objeto de tratamiento en [14]. Haga clic en la cabecera de la columna para borrar la selección actual.
2	fases	Una pestaña para cada fase del proyecto. Haga clic para seleccionar la fase.
3	activos	Árbol de activos y amenazas. Haga clic-clic para colapsar / expandir el árbol.
4	probabilidad	Ver “ <u>Opciones / Probabilidad</u> ”
5	EDI	EDI - escalón de interrupción Consecuencia de la amenaza sobre el activo

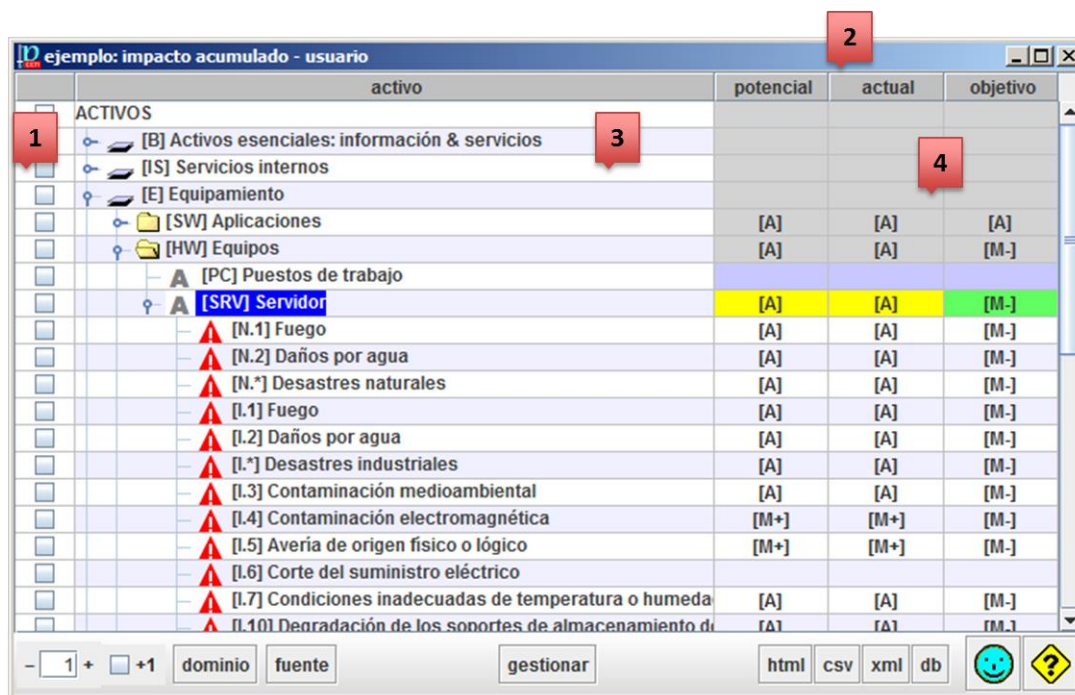
6	impacto	El impacto de la amenaza sobre el activo
7	riesgo	El riesgo de la amenaza sobre el activo



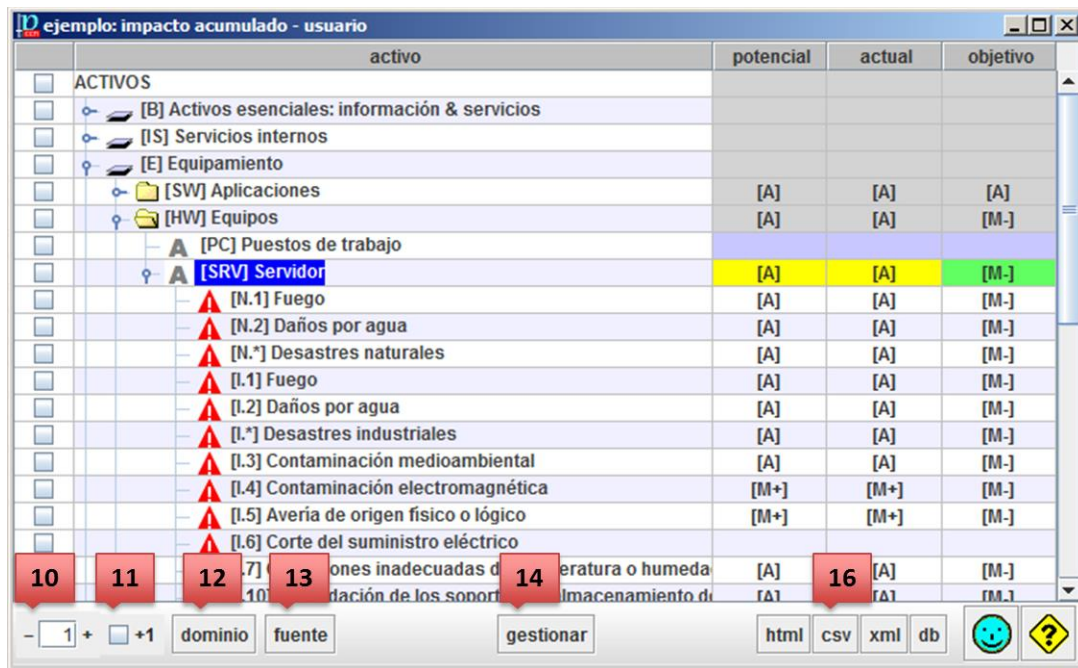
10	- 1 +	Controla el despliegue del árbol de activos ([3])
11	+1	Ajusta el despliegue [10]. Si se selecciona [+1], PILAR presenta las amenazas sobre el activo.
12	dominio	Seleccione un dominio de seguridad. PILAR seleccionará los activos ([3]) en ese dominio.
13	fuelle	Seleccione una o más fuentes de información. PILAR seleccionará los activos ([3]) asociados a esa fuente.
14	gestiona	Para las filas seleccionadas ([1]), PILAR recolecta los riesgos asociados y salta a la ventana de <i>valoración de salvaguardas</i> , teniendo en cuenta sólo dichos riesgos.
15	leyenda	Ver <i>Riesgos / Niveles de criticidad / código de colores</i>

16	exportar html csv xml db	Extrae los valores de la tabla — a un fichero HTML — a un fichero CSV — a un fichero XML — a una base de datos externa (si la licencia lo permite)
----	--------------------------------------	---

11.10.2. IMPACTO ACUMULADO



1	selección	Selecciona qué activos serán objeto de tratamiento en [14]
2	fases	Una columna para cada fase del proyecto.
3	activos	Árbol de activos y amenazas. Haga clic-clic para colapsar / expandir el árbol.
4	valores de impacto	Para cada activo y en cada fase del proyecto.



10	- 1 +	Controla el despliegue del árbol de activos ([3])
11	+1	Ajusta el despliegue [10]. Si se selecciona [+1], PILAR presenta las amenazas sobre el activo.
12	dominio	Seleccione un dominio de seguridad. PILAR seleccionará los activos ([3]) en ese dominio.
13	fuelle	Seleccione una o más fuentes de información. PILAR seleccionará los activos ([3]) asociados a esa fuente.
14	gestiona	Para las filas seleccionadas ([1]), PILAR recolecta los riesgos asociados y salta a la ventana de <i>valoración de salvaguardas</i> , teniendo en cuenta sólo dichos riesgos.
16	exportar html csv xml db	Extrae los valores de la tabla — a un fichero HTML — a un fichero CSV — a un fichero XML — a una base de datos externa (si la licencia lo permite)

11.10.3. RIESGO ACUMULADO

activo	potencial	actual	objetivo
ACTIVOS			
[B] Activos esenciales: información & servicios			
[IS] Servicios internos			
[E] Equipamiento			
[SW] Aplicaciones	{6,9}	{5,6}	{4,4}
[HW] Equipos	{6,9}	{6,2}	{3,0}
[PC] Puestos de trabajo			
[SRV] Servidor	{6,9}	{6,2}	{3,0}
[N.1] Fuego	{5,6}	{4,8}	{0,78}
[N.2] Daños por agua	{5,6}	{4,9}	{0,78}
[N.*] Desastres naturales	{5,6}	{4,9}	{0,78}
[I.1] Fuego	{6,4}	{5,7}	{0,95}
[I.2] Daños por agua	{6,4}	{5,8}	{0,96}
[I.*] Desastres industriales	{6,4}	{5,8}	{0,96}
[I.3] Contaminación medioambiental	{6,8}	{5,8}	{1,2}
[I.4] Contaminación electromagnética	{5,1}	{4,1}	{1,2}
[I.5] Avería de origen físico o lógico	{5,1}	{4,1}	{1,2}
[I.6] Corte del suministro eléctrico	{0}	{0}	{0}
[I.7] Condiciones inadecuadas de temperatura o humedad	{6,8}	{5,7}	{1,1}
[I.10] Degradación de los soportes de almacenamiento de	{6,8}	{6,0}	{1,1}

1	selección	Selecciona qué activos serán objeto de tratamiento en [14]
2	fases	Una columna para cada fase del proyecto.
3	activos	Árbol de activos y amenazas. Haga clic-clic para colapsar / expandir el árbol.
4	valores de riesgo	Para cada activo y en cada fase del proyecto.

ejemplo: riesgo acumulado - usuario

	activo	potencial	actual	objetivo
☐	ACTIVOS			
☐	[B] Activos esenciales: información & servicios			
☐	[IS] Servicios internos			
☐	[E] Equipamiento			
☐	[SW] Aplicaciones	{6,9}	{5,6}	{4,4}
☐	[HW] Equipos	{6,9}	{6,2}	{3,0}
☐	[PC] Puestos de trabajo			
☐	[SRV] Servidor	{6,9}	{6,2}	{3,0}
☐	[N.1] Fuego	{5,6}	{4,8}	{0,78}
☐	[N.2] Daños por agua	{5,6}	{4,9}	{0,78}
☐	[N.*] Desastres naturales	{5,6}	{4,9}	{0,78}
☐	[I.1] Fuego	{6,4}	{5,7}	{0,95}
☐	[I.2] Daños por agua	{6,4}	{5,8}	{0,96}
☐	[I.*] Desastres industriales	{6,4}	{5,8}	{0,96}
☐	[I.3] Contaminación medioambiental	{6,8}	{5,8}	{1,2}
☐	[I.4] Contaminación electromagnética	{5,1}	{4,1}	{1,2}
☐	[I.5] Avería de origen físico o lógico	{5,1}	{4,1}	{1,2}
☐	[I.6] Corte del suministro eléctrico	{0}	{0}	{0}
☐	[I.7] Condiciones inadecuadas de temperatura y humedad	{6,8}	{5,7}	{1,1}
☐	[I.10] Interrupción de suministro de energía	{6,8}	{6,0}	{1,1}

10 11 12 13 14 15 16

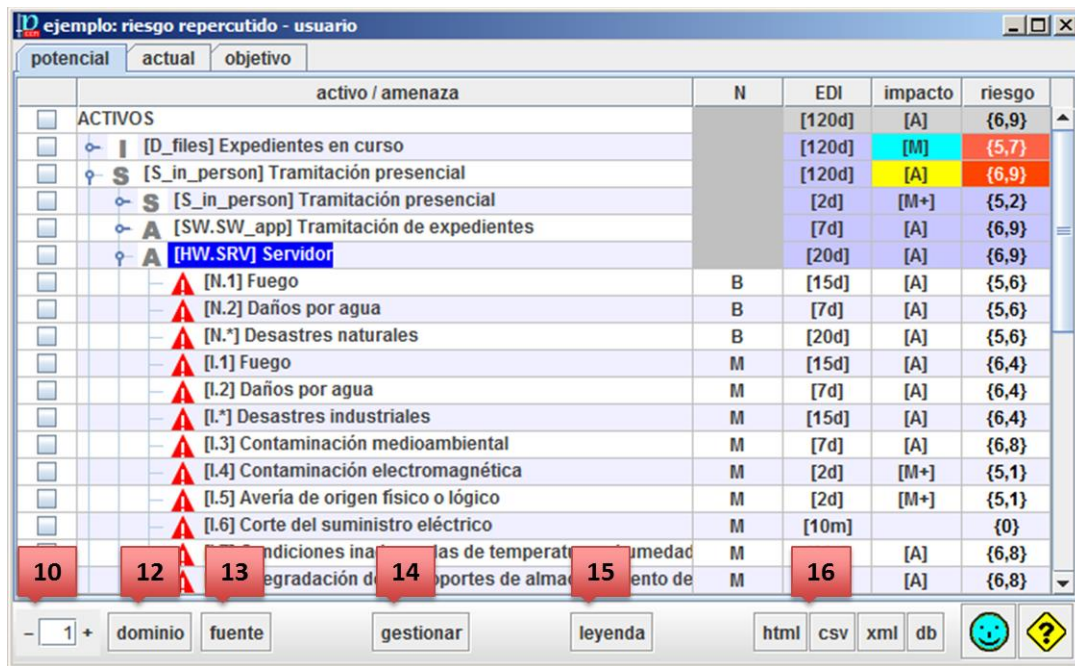
- 1 + +1 dominio fuente gestionar leyenda html csv xml db

10	- 1 +	Controla el despliegue del árbol de activos ([3])
11	+1	Ajusta el despliegue [10]. Si se selecciona [+1], PILAR presenta las amenazas sobre el activo.
12	dominio	Seleccione un dominio de seguridad. PILAR seleccionará los activos ([3]) en ese dominio.
13	fuelle	Seleccione una o más fuentes de información. PILAR seleccionará los activos ([3]) asociados a esa fuente.
14	gestiona	Para las filas seleccionadas ([1]), PILAR recolecta los riesgos asociados y salta a la ventana de <u>valoración de salvaguardas</u> , teniendo en cuenta sólo dichos riesgos.
15	leyenda	Ver <u>Riesgos / Niveles de criticidad / código de colores</u>
16	exportar html csv xml db	Extrae los valores de la tabla — a un fichero HTML — a un fichero CSV — a un fichero XML — a una base de datos externa (si la licencia lo permite)

11.10.4. TABLA DE IMPACTO Y RIESGO REPERCUTIDO

potencial	actual	objetivo	activo / amenaza	N	EDI	impacto	riesgo
1			ACTIVOS		[120d]	[A]	{6,9}
			[D_files] Expedientes en curso		[120d]	[M]	{5,7}
			[S_in_person] Tramitación presencial		[120d]	[A]	{6,9}
			[S_in_person] Tramitación presencial		[2d]	[M+]	{5,2}
			[SW.SW_app] Tramitación de expedientes		[7d]	[A]	{6,9}
			[HW.SRV] Servidor		[20d]	[A]	{6,9}
			[N.1] Fuego	B	[15d]	[A]	{5,6}
			[N.2] Daños por agua	B	[7d]	[A]	{5,6}
			[N.*] Desastres naturales	B	[20d]	[A]	{5,6}
			[I.1] Fuego	M	[15d]	[A]	{6,4}
			[I.2] Daños por agua	M	[7d]	[A]	{6,4}
			[I.*] Desastres industriales	M	[15d]	[A]	{6,4}
			[I.3] Contaminación medioambiental	M	[7d]	[A]	{6,8}
			[I.4] Contaminación electromagnética	M	[2d]	[M+]	{5,1}
			[I.5] Avería de origen físico o lógico	M	[2d]	[M+]	{5,1}
			[I.6] Corte del suministro eléctrico	M	[10m]		{0}
			[I.7] Condiciones inadecuadas de temperatura o humedad	M	[20d]	[A]	{6,8}
			[I.10] Degradación de los soportes de almacenamiento de	M	[20d]	[A]	{6,8}

1	selección	Selecciona qué activos serán objeto de tratamiento en [14]
2	fases	Una pestaña para cada fase del proyecto.
3	activos	Árbol de activos y amenazas. Presenta tanto los activos superiores, con valor propio, como los activos inferiores de los que depende. Haga clic-clic para colapsar / expandir el árbol.
4	probabilidad	Ver “ <i>Opciones / Probabilidad</i> ”
5	escalón de interrupción	Consecuencia de la amenaza sobre el activo
6	impacto	El impacto de la amenaza sobre el activo
7	riesgo	El riesgo de la amenaza sobre el activo

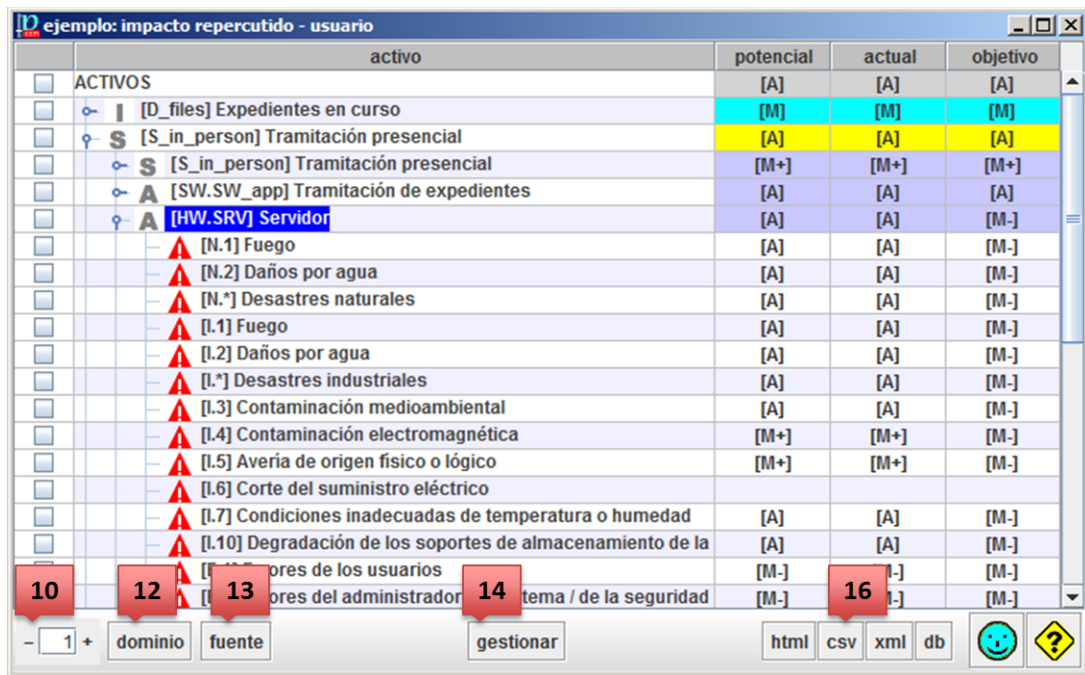


10	- 1 +	Controla el despliegue del árbol de activos ([3])
12	dominio	Seleccione un dominio de seguridad. PILAR seleccionará los activos ([3]) en ese dominio.
13	fuelle	Seleccione una o más fuentes de información. PILAR seleccionará los activos ([3]) asociados a esa fuente.
14	gestiona	Para las filas seleccionadas ([1]), PILAR recolecta los riesgos asociados y salta a la ventana de <u>valoración de salvaguardas</u> , teniendo en cuenta sólo dichos riesgos.
15	leyenda	Ver <u>Riesgos / Niveles de criticidad / código de colores</u>
16	exportar html csv xml db	Extrae los valores de la tabla — a un fichero HTML — a un fichero CSV — a un fichero XML — a una base de datos externa (si la licencia lo permite)

11.10.5. IMPACTO REPERCUTIDO

	activo	potencial	actual	objetivo
1	ACTIVOS	[A]	[A]	[A]
	└─ [D_files] Expedientes en curso	[M]	[M]	[M]
	└─ S [S_in_person] Tramitación presencial	[A]	[A]	[A]
	└─ S [S_in_person] Tramitación presencial	[M+]	[M+]	[M+]
	└─ A [SW.SW_app] Tramitación de expedientes	[A]	[A]	[A]
	└─ A [HW.SRV] Servidor	[A]	[A]	[M-]
	└─ [N.1] Fuego	[A]	[A]	[M-]
	└─ [N.2] Daños por agua	[A]	[A]	[M-]
	└─ [N.*] Desastres naturales	[A]	[A]	[M-]
	└─ [I.1] Fuego	[A]	[A]	[M-]
	└─ [I.2] Daños por agua	[A]	[A]	[M-]
	└─ [I.*] Desastres industriales	[A]	[A]	[M-]
	└─ [I.3] Contaminación medioambiental	[A]	[A]	[M-]
	└─ [I.4] Contaminación electromagnética	[M+]	[M+]	[M-]
	└─ [I.5] Avería de origen físico o lógico	[M+]	[M+]	[M-]
	└─ [I.6] Corte del suministro eléctrico			
	└─ [I.7] Condiciones inadecuadas de temperatura o humedad	[A]	[A]	[M-]
	└─ [I.10] Degradación de los soportes de almacenamiento de la	[A]	[A]	[M-]
	└─ [E.1] Errores de los usuarios	[M-]	[M-]	[M-]
	└─ [E.2] Errores del administrador del sistema / de la seguridad	[M-]	[M-]	[M-]

1	selección	Selecciona qué activos serán objeto de tratamiento en [14]
2	fases	Una columna para cada fase del proyecto.
3	activos	Árbol de activos y amenazas. Presenta tanto los activos superiores, con valor propio, como los activos inferiores de los que depende. Haga clic-clic para colapsar / expandir el árbol.
4	valores de impacto	Para cada activo y en cada fase del proyecto.



10	- 1 +	Controla el despliegue del árbol de activos ([3])
12	dominio	Seleccione un dominio de seguridad. PILAR seleccionará los activos ([3]) en ese dominio.
13	fuelle	Seleccione una o más fuentes de información. PILAR seleccionará los activos ([3]) asociados a esa fuente.
14	gestiona	Para las filas seleccionadas ([1]), PILAR recolecta los riesgos asociados y salta a la ventana de <i>valoración de salvaguardas</i> , teniendo en cuenta sólo dichos riesgos.
16	exportar html csv xml db	Extrae los valores de la tabla — a un fichero HTML — a un fichero CSV — a un fichero XML — a una base de datos externa (si la licencia lo permite)

11.10.6. RIESGO REPERCUTIDO


activo	potencial	actual	objetivo
ACTIVOS	{6,9}	{6,4}	{4,5}
[D_files] Expedientes en curso	{5,7}	{5,1}	{2,3}
[S_in_person] Tramitación presencial	{6,9}	{6,4}	{4,5}
[S_in_person] Tramitación presencial	{5,2}	{4,5}	{3,1}
[SW.SW_app] Tramitación de expedientes	{6,9}	{5,6}	{4,4}
[HW.SRV] Servidor	{6,9}	{6,2}	{3,0}
[N.1] Fuego	{5,6}	{4,8}	{0,78}
[N.2] Daños por agua	{5,6}	{4,9}	{0,78}
[N.*] Desastres naturales	{5,6}	{4,9}	{0,78}
[I.1] Fuego	{6,4}	{5,7}	{0,95}
[I.2] Daños por agua	{6,4}	{5,8}	{0,96}
[I.*] Desastres industriales	{6,4}	{5,8}	{0,96}
[I.3] Contaminación medioambiental	{6,8}	{5,8}	{1,2}
[I.4] Contaminación electromagnética	{5,1}	{4,1}	{1,2}
[I.5] Avería de origen físico o lógico	{5,1}	{4,1}	{1,2}
[I.6] Corte del suministro eléctrico	{0}	{0}	{0}
[I.7] Condiciones inadecuadas de temperatura o humedad	{6,8}	{5,7}	{1,1}
[I.10] Degradación de los soportes de almacenamiento de la	{6,8}	{6,0}	{1,1}
[E.1] Errores de los usuarios	{3,5}	{2,9}	{1,3}
[E.2] Errores del administrador del sistema / de la seguridad	{3,5}	{2,9}	{1,3}

1	selección	Selecciona qué activos serán objeto de tratamiento en [14]
2	fases	Una columna para cada fase del proyecto.
3	activos	Árbol de activos y amenazas. Presenta tanto los activos superiores, con valor propio, como los activos inferiores de los que depende. Haga clic-clic para colapsar / expandir el árbol.
4	valores de riesgo	Para cada activo y en cada fase del proyecto.

	activo	potencial	actual	objetivo
☐	ACTIVOS	{6,9}	{6,4}	{4,5}
☐	[D_files] Expedientes en curso	{5,7}	{5,1}	{2,3}
☐	[S_in_person] Tramitación presencial	{6,9}	{6,4}	{4,5}
☐	[S_in_person] Tramitación presencial	{5,2}	{4,5}	{3,1}
☐	[A [SW.SW_app] Tramitación de expedientes	{6,9}	{5,6}	{4,4}
☐	[A [HW.SRV] Servidor	{6,9}	{6,2}	{3,0}
☐	[N.1] Fuego	{5,6}	{4,8}	{0,78}
☐	[N.2] Daños por agua	{5,6}	{4,9}	{0,78}
☐	[N.*] Desastres naturales	{5,6}	{4,9}	{0,78}
☐	[I.1] Fuego	{6,4}	{5,7}	{0,95}
☐	[I.2] Daños por agua	{6,4}	{5,8}	{0,96}
☐	[I.*] Desastres industriales	{6,4}	{5,8}	{0,96}
☐	[I.3] Contaminación medioambiental	{6,8}	{5,8}	{1,2}
☐	[I.4] Contaminación electromagnética	{5,1}	{4,1}	{1,2}
☐	[I.5] Avería de origen físico o lógico	{5,1}	{4,1}	{1,2}
☐	[I.6] Corte del suministro eléctrico	{0}	{0}	{0}
☐	[I.7] Condiciones inadecuadas de temperatura o humedad	{6,8}	{5,7}	{1,1}
☐	[I.10] Degradación de los soportes de almacenamiento de la	{6,8}	{6,0}	{1,1}
☐	[I.11] Errores de los usuarios	{3,5}	{2,9}	{1,3}
☐	[I.12] Errores del administrador del sistema / de la seguridad	{3,5}	{2,9}	{1,3}

- 1 + dominio fuente gestionar leyenda html csv xml db

10	- 1 +	Controla el despliegue del árbol de activos ([3])
12	dominio	Seleccione un dominio de seguridad. PILAR seleccionará los activos ([3]) en ese dominio.
13	fuelle	Seleccione una o más fuentes de información. PILAR seleccionará los activos ([3]) asociados a esa fuente.
14	gestiona	Para las filas seleccionadas ([1]), PILAR recolecta los riesgos asociados y salta a la ventana de <u>valoración de salvaguardas</u> , teniendo en cuenta sólo dichos riesgos.
15	leyenda	Ver <u>Riesgos / Niveles de criticidad / código de colores</u>
16	exportar html csv xml db	Extrae los valores de la tabla — a un fichero HTML — a un fichero CSV — a un fichero XML — a una base de datos externa (si la licencia lo permite)

12. DRP – PLANES DE RECUPERACIÓN DE DESASTRES

Después de un incidente serio (desastre), puede que tenga que reconstruir el sistema.

Esta pantalla ayuda a diseñar un plan de recuperación.

En un sistema complejo, pueden ser necesarios varios planes:

- dependiendo de qué activos se pierden
- dependiendo de qué servicios necesitan reconstrucción urgente
- dependiendo de las necesidades actuales: ej. final del período de pagos a empleados y proveedores
- ...

En estas pantallas no se tienen en cuenta las salvaguardas. Solamente se analiza el supuesto de que todo trabaja según el plan.

12.1. PANTALLAS

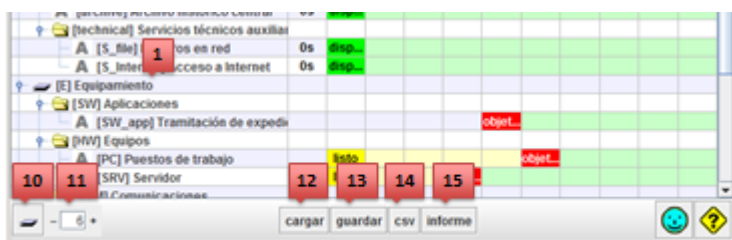
La pantalla es relativamente compleja.

12.1.1. LA PARTE SUPERIOR



1	activos	Árbol de activos. Haga clic en la manivela o clic-clic en el texto para expandir / comprimir el árbol.
2	tiempos	Para recopilar lo que hacemos respecto de un activo. Ver “ DRP / actuaciones ”
3	intervalos	Una columna para cada intervalo de interrupción
4	valores de impacto	PILAR presenta 2 filas con la evolución del impacto: — primera fila: el impacto si no hacemos nada — segunda fila: impacto residual tras aplicar el plan La segunda fila nos permite saber si alcanzamos el RTO objetivo que nos hayamos propuesto para este escenario.

12.1.2.LA PARTE INFERIOR



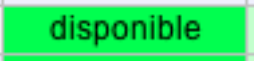
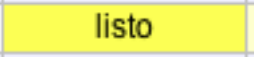
1	activos	Árbol de activos. Haga clic en la manivela o clic-clic en el texto para expandir / comprimir el árbol.
10		Haga clic para colapsar el árbol [1] al primer nivel, capas.
11		Controla el despliegue del árbol de activos ([1])
12	cargar	Carga un plan de recuperación de un fichero ya existente (extensión .drp)
13	guardar	Guarda el plan de recuperación en un fichero (extensión .drp). Los planes de recuperación de desastre NO se guardan con el proyecto. El usuario los guarda y restaura en archivos separados.
14	csv	Exporta el plan de recuperación a un fichero CSV
15	informe	Exporta el plan de recuperación a un fichero textual

12.1.3.ZONA CENTRAL

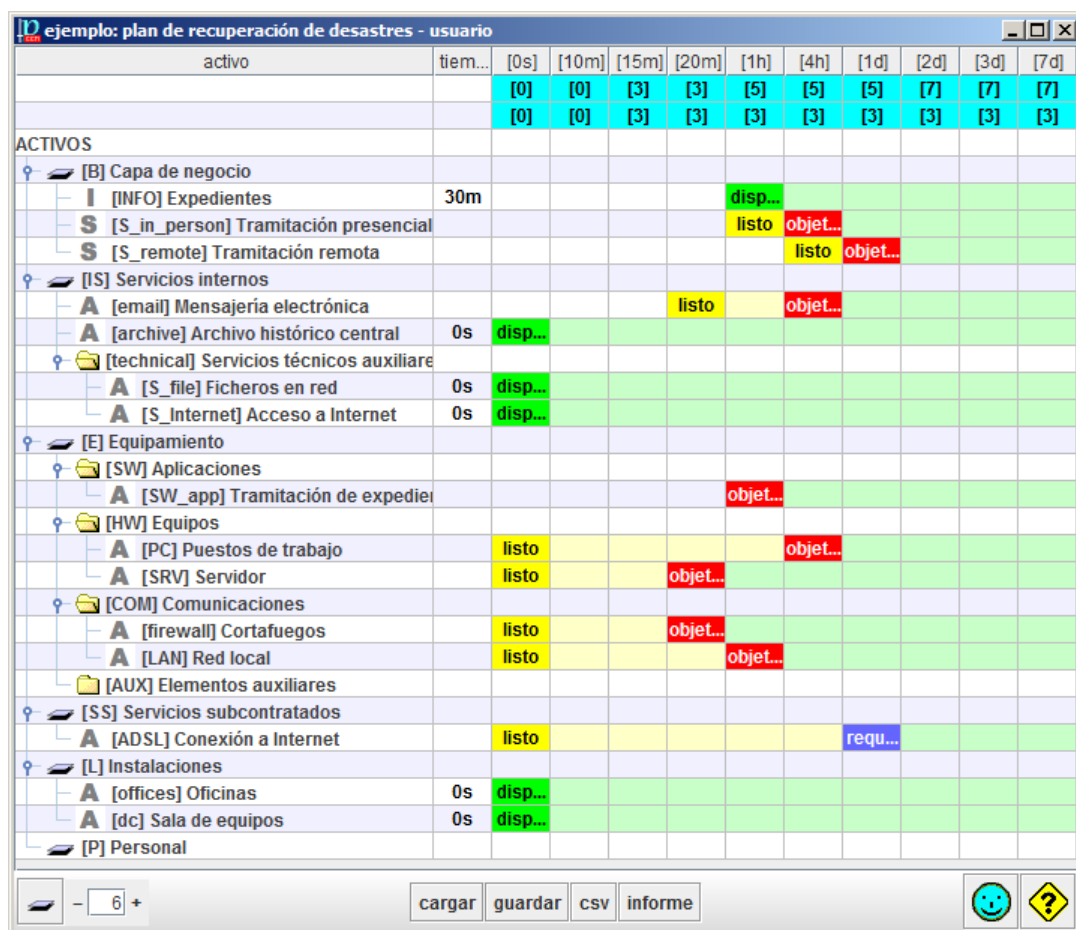
Contiene las actuaciones previstas con cada activo.

En cada celda, determinada por un activo (del árbol izquierdo) y un intervalo de tiempo (columnas), podemos

etiqueta	significado
	Haga clic en una celda para marcarse un objetivo: “mi objetivo es que este activo esté funcionado en este intervalo de tiempo”. Esto tiene una traducción en la fila superior que muestra el impacto residual, por lo que la forma de trabajar es marcarse objetivos lo bastante ambiciosos como para que el impacto sea aceptable.

	Como consecuencia de haber marcado un objetivo, PILAR analiza qué activos son necesarios para soportar el objetivo, y los marca.
	Usted puede decir, en la columna de tiempos, lo que hace. Si, por ejemplo, indica que tiene un plan para recuperar un activo en 30 minutos, PILAR marca que ese activo está disponible a partir de la columna [30m].
	Cuando un activo está disponible, todos los activos que dependen de él se dice que están listos, lo que quiere decir que tienen la plataforma preparada para que los instalemos.
	Podemos decir que los objetivos imponen “hacia abajo” requisitos, mientras que la disponibilidad habilita “hacia arriba” lo que está listo. Un plan está completo cuando no quedan activos marcados como “requeridos”.

12.1.4.EJEMPLO



activo	tiempo...	[0s]	[10m]	[15m]	[20m]	[1h]	[4h]	[1d]	[2d]	[3d]	[7d]
		[0]	[0]	[3]	[3]	[5]	[5]	[5]	[7]	[7]	[7]
		[0]	[0]	[3]	[3]	[3]	[3]	[3]	[3]	[3]	[3]
ACTIVOS											
[B] Capa de negocio											
[INFO] Expedientes	30m					disp...					
[S_in_person] Tramitación presencial						listo	objet...				
[S_remote] Tramitación remota						listo	objet...				
[IS] Servicios internos											
[A_email] Mensajería electrónica					listo		objet...				
[A_archive] Archivo histórico central	0s	disp...									
[technical] Servicios técnicos auxiliares											
[A_S_file] Ficheros en red	0s	disp...									
[A_S_Internet] Acceso a Internet	0s	disp...									
[E] Equipamiento											
[SW] Aplicaciones											
[A_SW_app] Tramitación de expedientes						objet...					
[HW] Equipos											
[A_PC] Puestos de trabajo		listo					objet...				
[A_SRV] Servidor		listo			objet...						
[COM] Comunicaciones											
[A_firewall] Cortafuegos		listo			objet...						
[A_LAN] Red local		listo			objet...						
[AUX] Elementos auxiliares											
[SS] Servicios subcontratados											
[A_ADSL] Conexión a Internet		listo						requ...			
[L] Instalaciones											
[A_offices] Oficinas	0s	disp...									
[A_dc] Sala de equipos	0s	disp...									
[P] Personal											

Nos hemos marcado como objetivos esenciales

- que el servicio [S_in_person] esté funcionando en 4 horas (RTO = 4h)
- que el servicio [S_remote] esté funcionando en 1 día (RTO = 1d)

En el escenario que analizamos, damos por hecho que

- las instalaciones no han sufrido daños y están disponibles en todo momento.
 - que los datos tiene una copia de backup recuperable en 30 minutos
 - que el archivo histórico sigue disponible
 - que los servicios técnicos auxiliares están disponibles
- esta es una forma “curiosa” de indicar que son activos inmateriales, que sólo sirven para estructurar el árbol de activos transfiriendo requisitos hacia abajo y disponibilidad hacia arriba

Nos hemos marcado como objetivos operacionales (plan de reconstrucción)

- que en 20m tendremos operativos el servidor y el cortafuegos
- que en 1h el sw de aplicación estará funcionando
- que en 4h tendremos listos los puestos de trabajo

El plan no está completo, porque para poner en marcha el segundo servicio aún no hemos resuelto el problema de la conexión ADSL a Internet.

12.2. DRP / ACTUACIONES

La columna denominada “tiempos” ([2]) nos permite indicar qué es lo que vamos a hacer.

Por ejemplo, para la información del ejemplo anterior:

tiempo 30m

comentario objetivo de recuperación de datos

equipamiento de respaldo

- ▶ [] [S] Servicios (S)
- ▼ [-] [D] Datos / Información (D)
 - ▼ [-] [D.e.-] Copias de respaldo en soporte electrónico
 - [X] [D.e.-lcl] copia local
 - [] [D.e.-ext] copia externa en instalaciones propias
 - [] [D.e.-cont] copia externa en instalaciones contratadas
 - ▶ [] [D.paper] Copias de respaldo en papel
 - ▶ [] [D.man] Procesamiento manual

Otro ejemplo, para las instalaciones del ejemplo anterior:

[dc] Sala de equipos

tiempo 0s

comentario escenario en el que no se han perdido las instalaciones

A partir del tiempo indicado, PILAR marca como DIPONIBLE la celda correspondiente en la pantalla principal, y recalcula el impacto residual en las primeras filas de la tabla.

12.2.1. ANÁLISIS CUANTITATIVO

Si está trabajando en modo cuantitativo, puede añadir información de cuánto cuesta aplicar el procedimiento de reposición del activo (coste económico del mecanismo de recuperación). Por ejemplo:

tiempo
 coste
 comentario
 equipamiento de respaldo
 ▶ ☐ [S] Servicios (S)
 ▼ ☒ [D] Datos / Información (D)
 ▼ ☒ [D.e-] Copias de respaldo en soporte electrónico
 ☒ [D.e-.lcl] copia local
 ☐ [D.e-.ext] copia externa en instalaciones propias
 ☐ [D.e-.cont] copia externa en instalaciones contratadas
 ▶ ☐ [D.paper] Copias de respaldo en papel
 ▶ ☐ [D.man] Procesamiento manual

PILAR añade ese coste al impacto residual, indicando que aunque por una parte atajamos el coste de la interrupción restaurando el activo, por otra la restauración en sí también tiene un coste.

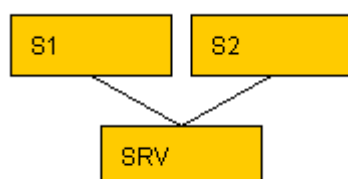
tiempo	[0s]	[10m]	[15m]	[20m]	[1h]	[4h]	[1d]	[2d]	[3d]	[7d]
	0	0	10K	10K	57K	67K	115K	310K	310K	480K
	3K	3K	13K	13K	13K	13K	13K	13K	13K	13K
30m					disponi...					

12.3. EL SIGNIFICADO DE LOS ACTIVOS LISTOS

Los activos OBJETIVO son los objetivos explicitados por el usuario de la herramienta. Los activos REQUERIDOS son los activos inferiores que se necesitan según el grafo de dependencias.

Los activos LISTOS son esos activos para los cuales sus activos inferiores o son OBJETIVO o son REQUERIDOS o están DISPONIBLES.

Un ejemplo puede ayudar a entenderlo mejor. Sean dos servicios que dependen de un servidor compartido:



Éstas son las consecuencias de seleccionar cada activo como OBJETIVO:

ACTIVOS				
▼ [capa]				
A [S1] servicio #1		objetivo	listo	listo
A [S2] servicio #2		listo	objetivo	listo
A [SRV] servidor compartido		requerido	requerido	objetivo