GUÍA/NORMA DE SEGURIDAD DE LAS TIC (CCN-STIC-473C)

MANUAL DE USUARIO μPILAR

VERSIÓN 5.3

NOVIEMBRE 2013

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE LA PRESIDENCIA

NIPO: 002-13-053-5

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

PRÓLOGO

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

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

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

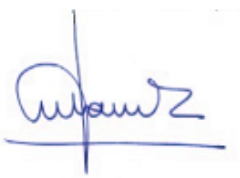
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia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

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

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

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

Noviembre de 2013



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. RESUMEN

A fin de conocer la seguridad que ofrece un sistema, necesitamos modelarlo, identificando y valorando los elementos que lo componen y las amenazas a las que están expuestos. Con estos datos podemos estimar los riesgos a los que el sistema está expuesto.

El riesgo puede mitigarse por medio de salvaguardas. Normalmente, estas medidas reducen el riesgo a un valor residual que, sin ser nulo (seguridad absoluta) sí puede ser aceptable por la organización. Si el riesgo es excesivo, se suele preparar un plan de mejora de la seguridad que siga reduciendo los niveles de riesgo hasta alcanzar valores aceptables.

El análisis de riesgos es la actividad que proporciona la información necesaria para realizar un tratamiento de los riesgos. Se trata de una actividad que se ejecuta una y otra vez, recurriendo a ella cuando el sistema cambia de componentes o cuando cambian las amenazas o se modifican las salvaguardas.

PILAR implementa la metodología Magerit: [http://administracionelectronica.gob.es/].

µPILAR es una versión simplificada de PILAR pensada para sistemas pequeños con un sistema de protección homogéneo. El análisis, con esas premisas, es rápido, aunque sea menos preciso.

A la hora de seleccionar salvaguardas, µPILAR se referencia a algún perfil de seguridad. De esta forma dispondremos de una estimación del grado de cumplimiento del perfil, al tiempo que de una estimación del riesgo residual derivado de las partes no implantadas de dicho perfil.

El objetivo es realizar un análisis de riesgos en menos de 4 horas.

La información recopilada por µPILAR se almacena en el mismo formato que usa PILAR, de forma que los datos pueden analizarse posteriormente de forma más detallada con la herramienta estándar y planificar un tratamiento más preciso.

1.1. LECTURAS RECOMENDADAS

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

View
http://csrc.nist.gov/publications/PubsSPs.html

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

1.2. OTRA DOCUMENTACIÓN

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

2. INSTALACIÓN

2.1. ENTORNO JAVA

Se necesita un

JRE – Entorno de ejecución Java

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

2.2. PILAR (WINDOWS)

Cuando Java esté instalado…

- ejecute `pilarmicro_<version>_<perfil>_<lang>.exe`
- 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
  `pilarmicro.exe`
  donde haya decidido instalar el software.

2.3. PILAR (UNIX, LINUX, …)

Normalmente java ya viene instalado en el sistema.

Cuando Java esté instalado…

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

2.4. PILAR (MAC OS X)

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

- abra `pilarmicro_<version>_<perfil>_<lang>.dmg`
- ejecute la aplicación `INSTALL`, colocando los ficheros donde crea conveniente
- al terminar la instalación, debe encontrar un fichero
  `pilarmicro_<version>.app`

2.5. USO

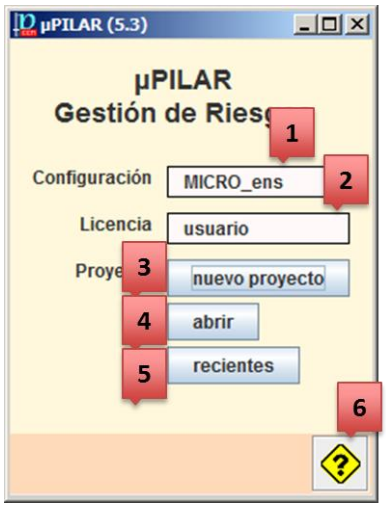
Ejecute `pilarmicro`:

- le pedirá un fichero *Fichero de configuración* (con extensión .CAR) que encontrará en donde haya decidido instalar el programa:
  MICRO_..._es.car

  llevándole a la "*Primera pantalla*.

El fichero *.car* proporciona una serie de información que constituye el contexto de ejecución de PILAR. Puede editarlo con cualquier editor de textos.

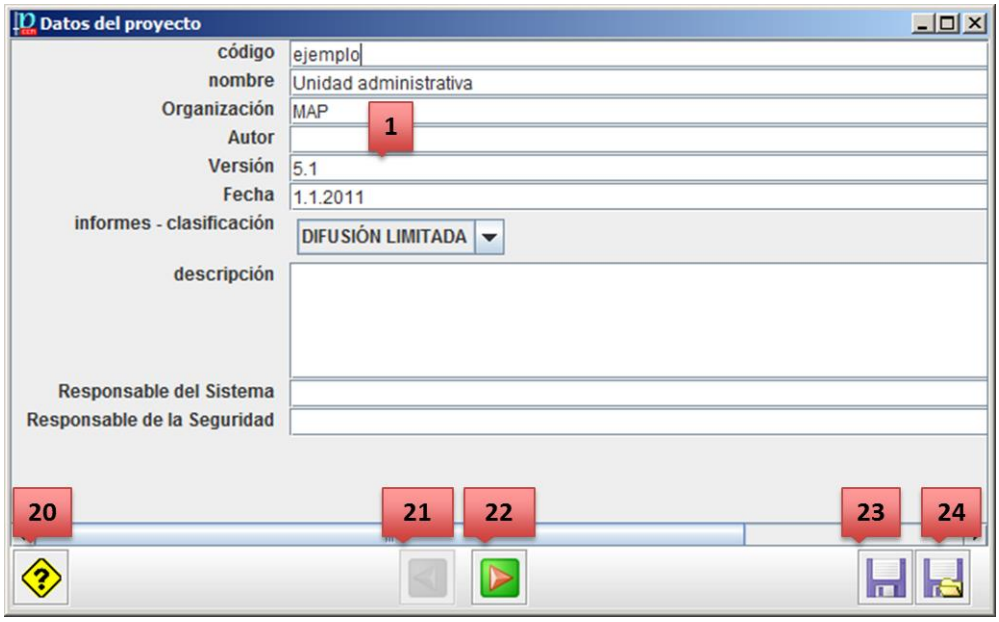
3. PRIMERA PANTALLA



1	configuración	Selecciona un fichero de configuración. Haga clic-clic para seleccionar. Ver "*Fichero de configuración*".
2	licencia	Presenta la licencia actual, incluyendo la fecha de expiración, si tuviera. Haga clic-clic para seleccionar. En el recuadro aparece el titular de la licencia. Si no se dispone de una licencia válida, aparece "sin licencia", en este caso, podrá ver proyectos, pero no modificarlos.
3	nuevo proyecto	Abrimos un proyecto nuevo..
4	abrir	Abre un proyecto que ya existía.
5	recientes	Enlace rápido a proyectos trabajados recientemente.
6		Ayuda en línea.

4. DATOS DEL PROYECTO

Estos datos son meramente administrativos y serán parte de los informes finales.



La mayor parte de los campos deben ser evidentes.

1		Marca por defecto para los informes.
20		Ayuda en línea.
21		Pantalla anterior.
22		Pantalla siguiente.
23		Guarda el proyecto en el fichero.
24		Guarda el proyecto en el fichero que se indique.

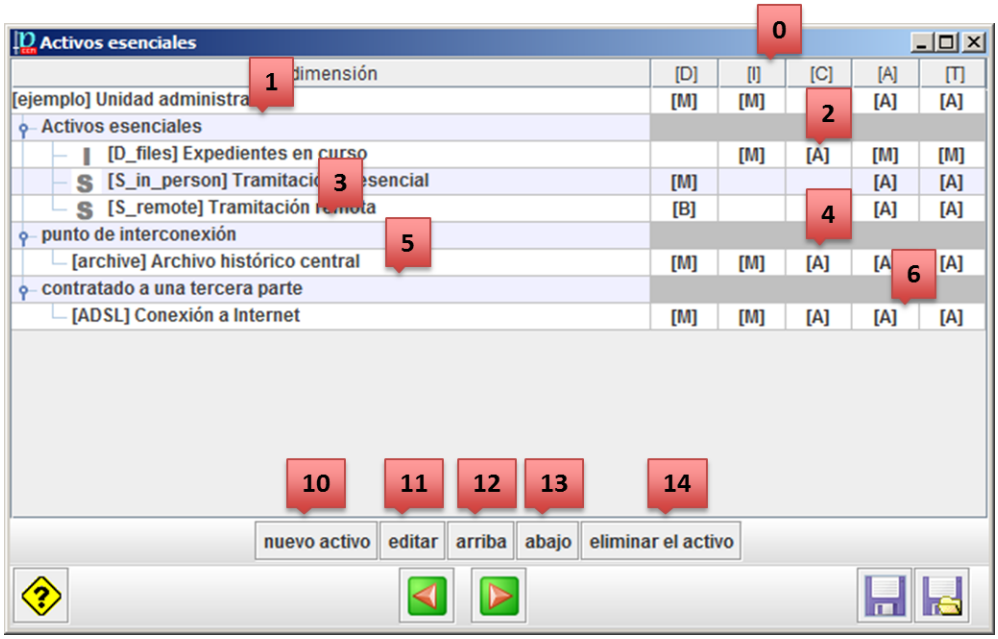
5. ACTIVOS ESENCIALES

En esta pantalla indicaremos cuales son los activos esenciales del sistema, es decir

- la información que se maneja
- el servicio que se presta
- los puntos de interconexión con otros sistemas
- servicios externos (prestados por terceros) en los que se apoya

Para cada uno de estos activos, puede indicar algunos datos administrativos, así como su valoración (nivel de seguridad requerido) en términos de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

La primera vez aparecen 2 activos por defecto: una información y un servicio. Siéntase libre de editarlos, eliminarlos o añadir nuevos activos.



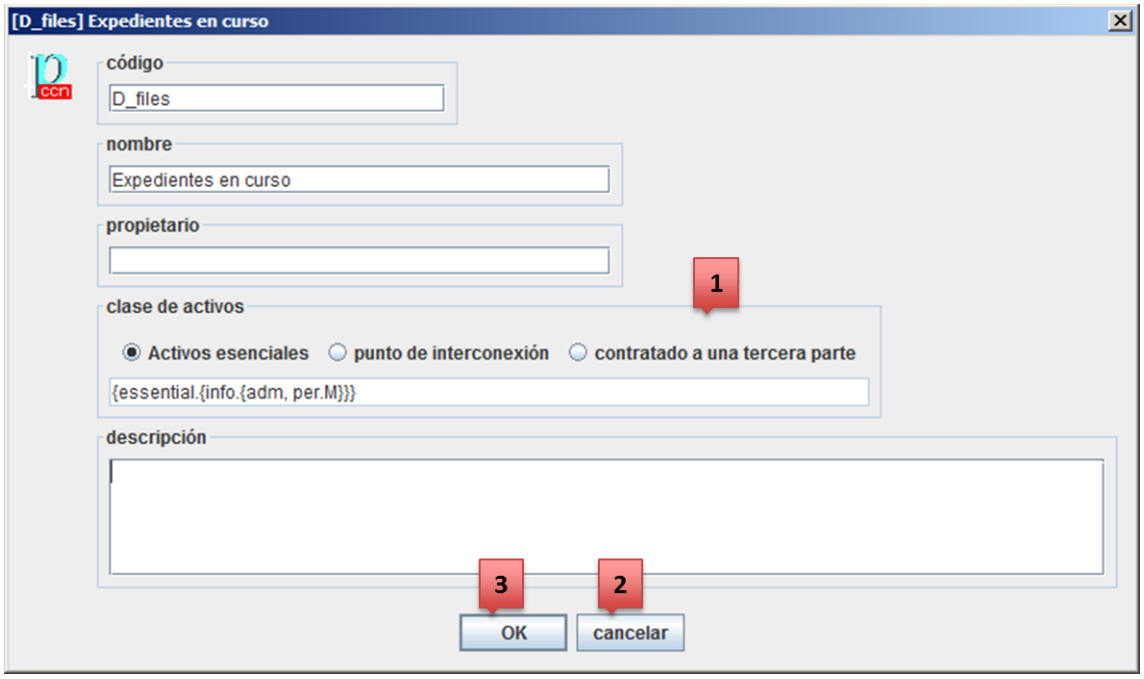
El formato es un poco rígido:

- los activos de información y servicio están siempre en la misma zona del árbol; no obstante, puede recolocarlos usando los botones ARRIBA y ABAJO
- los puntos de interconexión están siempre en la misma zona del árbol; no obstante, puede recolocarlos usando los botones ARRIBA y ABAJO
- los servicios contratados a terceros están siempre en la misma zona del árbol; no obstante, puede recolocarlos usando los botones ARRIBA y ABAJO
- cada activo debe tener un código único
- no pueden haber 2 activos con el mismo código

0		Un columna para cada dimensión de seguridad.
1		Área para los activos esenciales. Seleccione y haga clic en [11], [12], [13] o [14].
2		Área para valorar los activos esenciales. Haga clic-clic para *editar la valoración*
3		Área para los puntos de interconexión. Seleccione y haga clic en [11], [12], [13] o [14].
4		Área para valorar los puntos de interconexión. Los valores se heredan de [2]. Haga clic para marcar que "no aplica", "n.a.".
5		Área para los servicios externos. Seleccione y haga clic en [11], [12], [13] o [14].
6		Área para valorar los servicios externos. Los valores se heredan de [2]. Haga clic para marcar que "no aplica", "n.a.".
10	nuevo	Haga clic para añadir un nuevo activo. Ver "*Asset / edit*".
11	editar	Haga clic para editar el actvo seleccionado en [1], [3], o [5]. Ver "*Asset / edit*".
12	arriba	Haga clic para desplazar hacia arriba el activo seleccionado en [1], [3], o [5].
13	abajo	Haga clic para desplazar hacia abajo el activo seleccionado en [1], [3], o [5].
14	eliminar	Haga clic para eliminar el activo seleccionado en [1], [3], o [5].

5.1. MODIFICACIÓN DE UN ACTIVO (EDICIÓN)

Cuando edite un activo ya existente o cuando cree uno nuevo, verá una pantalla como la siguiente:

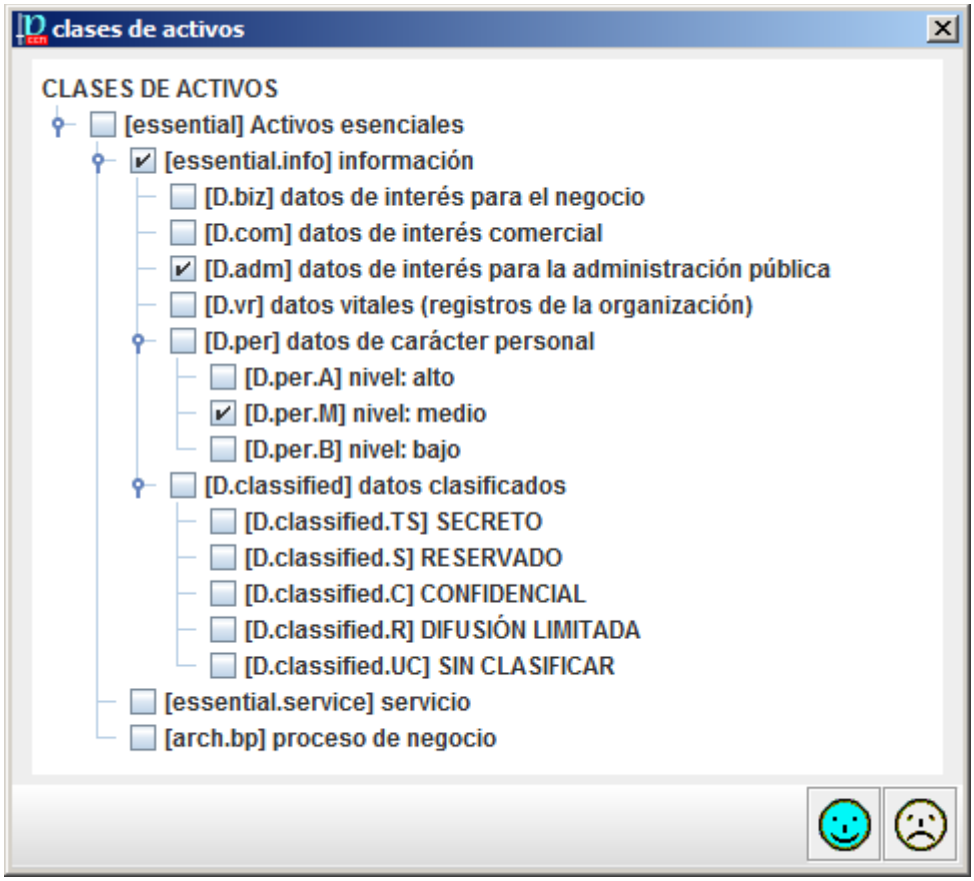


Puede asignarle cualquier código, siempre y cuando sea único. No podrá salir de esta pantalla si el código no es válido.

Puede introducir cualquier nombre, propietario y descripción.

El propietario puede ser una persona, o un role, o un órgano corporativo.

La clase de activo está limitada a las que aparecen en el combo desplegable. El activo se ubicará en a pantalla de activos esenciales según su clase. En activos esenciales, puede refinar la selección:



2 CANCELAR, se cierra la ventana sin guardar los datos.

3 OK, se cierra la ventana, guardando los datos..

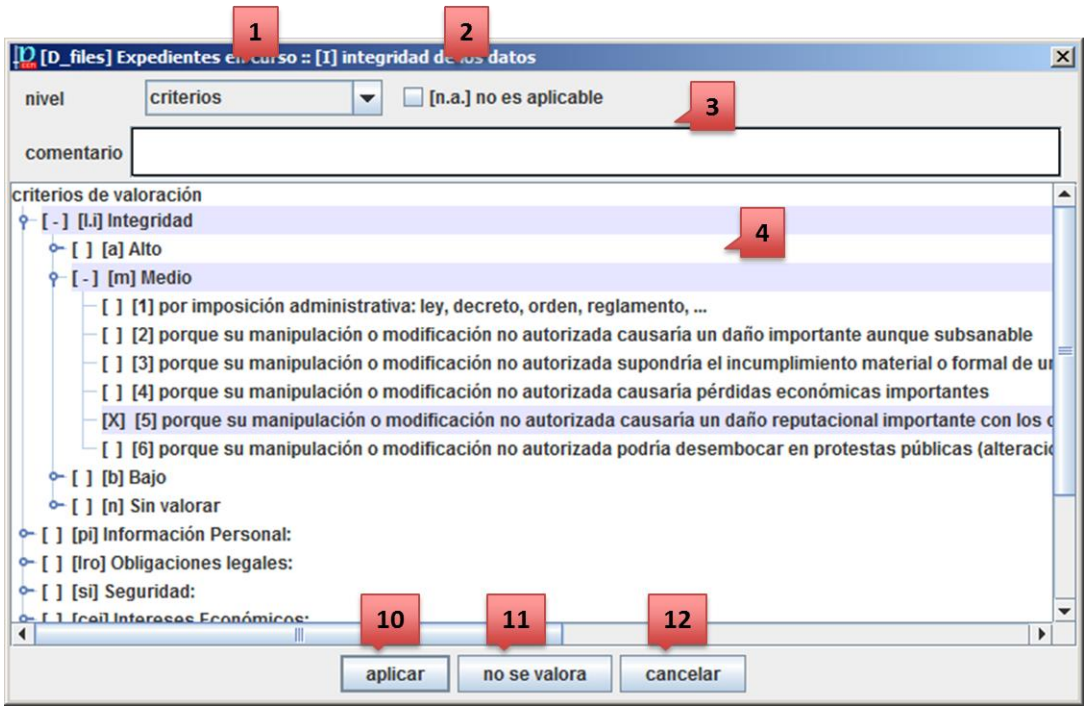
5.2. VALORACIÓN

Para cada activo esencial , información o servicio, puede establecer una valoración; es decir, marcar el nivel requerido en materia de seguridad en las dimensiones de disponibilidad (D), integridad (I), confidencialidad (C), autenticidad (A) y trazabilidad (T). Para establecer un nivel, haga clic-clic en la celda que desea editar y seleccione el criterio o criterios que son de aplicación al caso.

nivel ALTO	7	elevados requisitos de seguridad
nivel MEDIO	4	requisitos medios
nivel BAJO	1	requisitos bajos
sin valorar	0	no hay ninguna necesidad de proteger

Si aplica varios criterios, PILAR se quedará con el de nivel más elevado. Si desea marcar un criterio X en una sección, pero que pilar aplique el nivel Y, seleccione Y en el combo superior denominado "nivel".

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

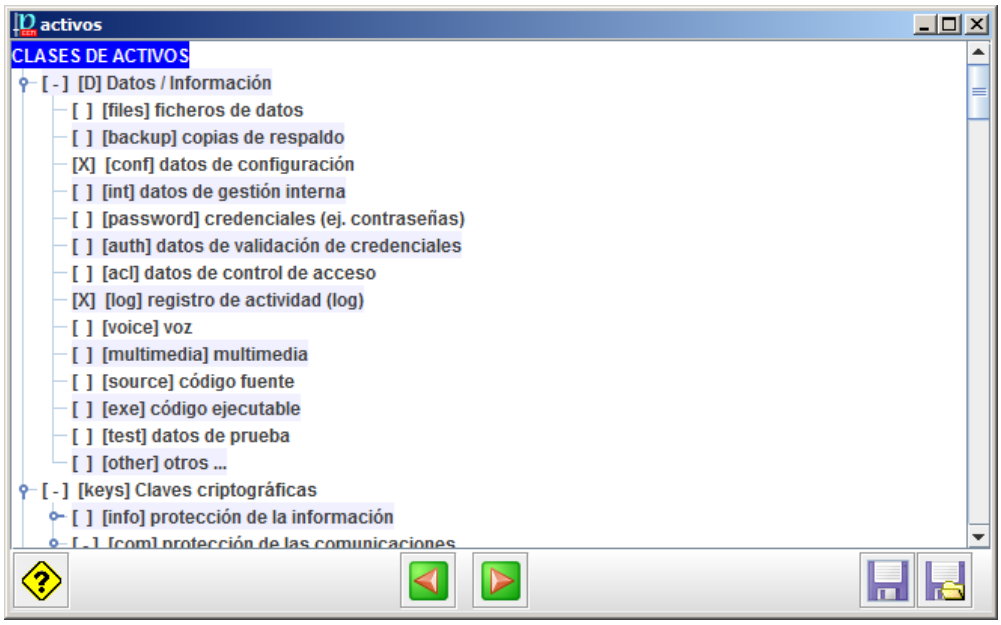


1	Si selecciona "criterios", el valor se decide por el más alto de los marcados en [4]. Si selecciona un valor explícito, este será el valor, independientemente de los criterios marcados.
2	Si la dimensión es irrelevante para el activo, marque N.A.
3	Comentario explicativo.
4	Criterios para valorar activos.
10	Se aplica el valor y se cierra la ventana.
11	Se elimina la valoración y se cierra la ventana.

12	Se cierra la ventana sin tomar los cambios en consideración.

6. OTROS ACTIVOS

Esta pantalla permite declarar otros tipos de activos que constituyen el sistema. Simplemente vaya haciendo clic en aquellas clases que se dan en sus sistema.



Marca las clases que aparecen en el sistema.

[X] significa que hay presentes uno más activos de esta clase

[–] significa que hay presentes uno más activos de una subclase de esta

[ ] significa que en el sistema no hay ningún activo de esta clase, ni de ninguna sus subclase

Para seleccionar o eliminar una clase

- haga clic en ella

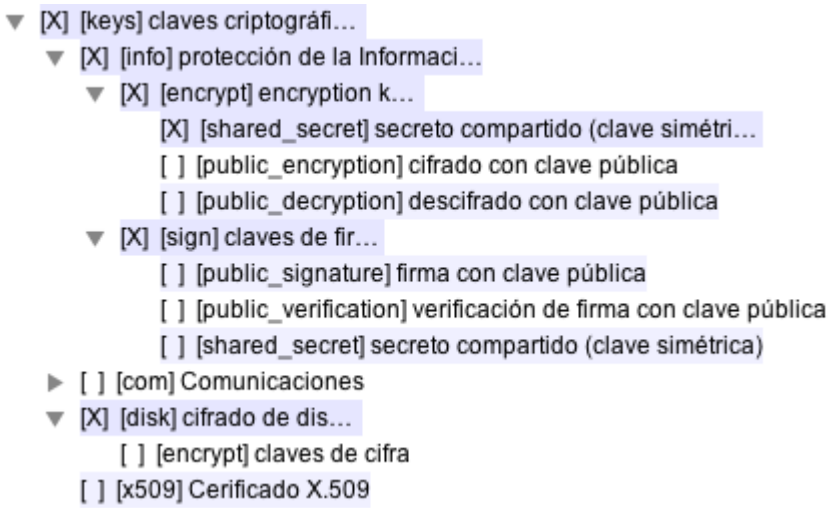
Para limpiar una clase (es decir, para eliminar las clases que tienen subclases marcadas)

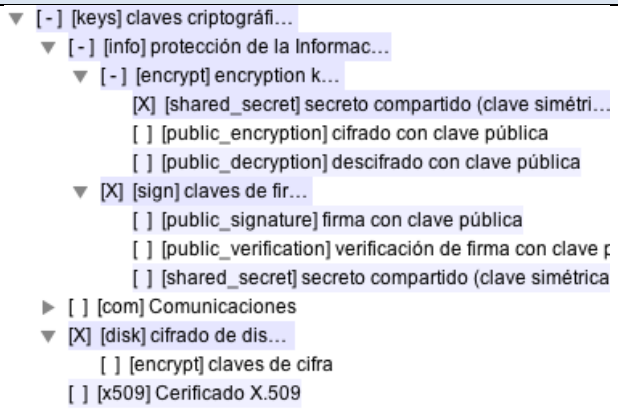
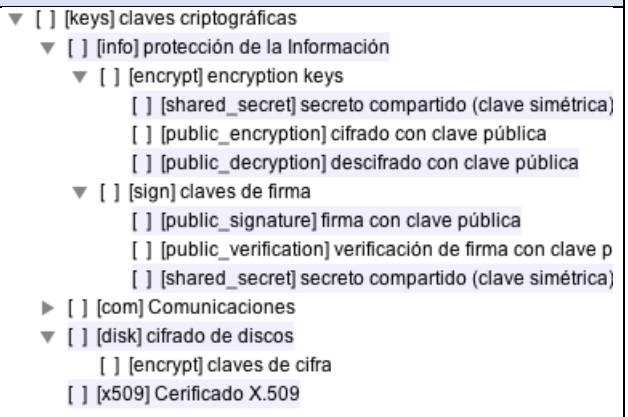
- seleccione la clase
- clic con el botón derecho
- clic en LIMPIAR

Para eliminar una clase (es decir, para eliminar una clases y sus subclases)

- seleccione la clase
- clic con el botón derecho
- clic en ELIMINAR

Ejemplo



clic derecho + LIMPIAR	clic derecho + ELIMINAR
	

Para guardar una copia del proyecto en el disco

- clic en el botón GUARDAR

Para guardar una copia en un fichero con otro nombre

- clic en el botón GUARDAR COMO

Para regresar a la pantalla anterior

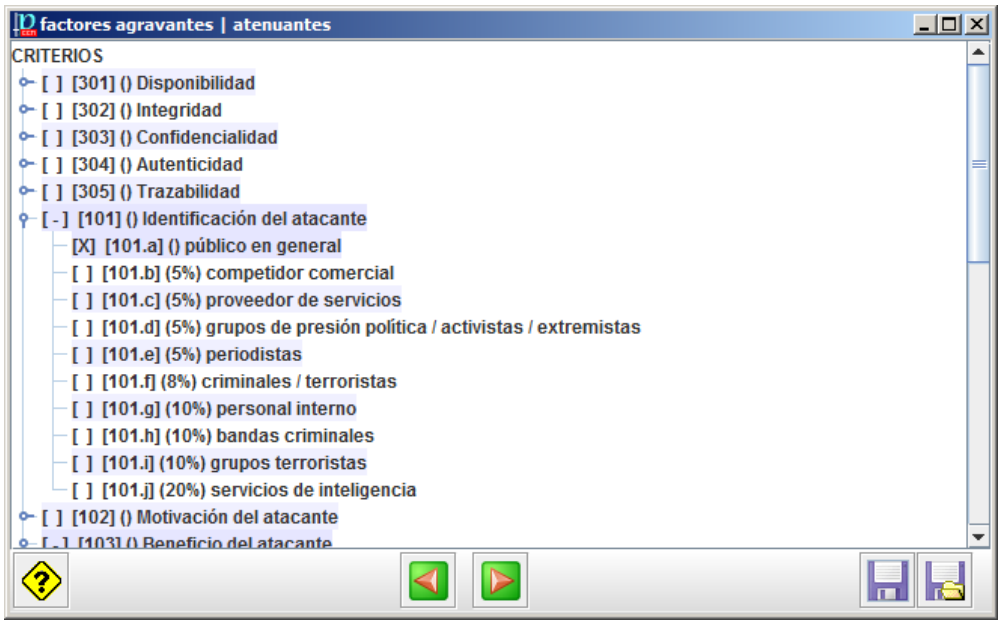
- clic en el botón con la fecha a la izquierda

Para pasar a la siguiente pantalla

- clic en el botón con la fecha a la derecha

7. FACTORES AGRAVANTES O ATENUANTES

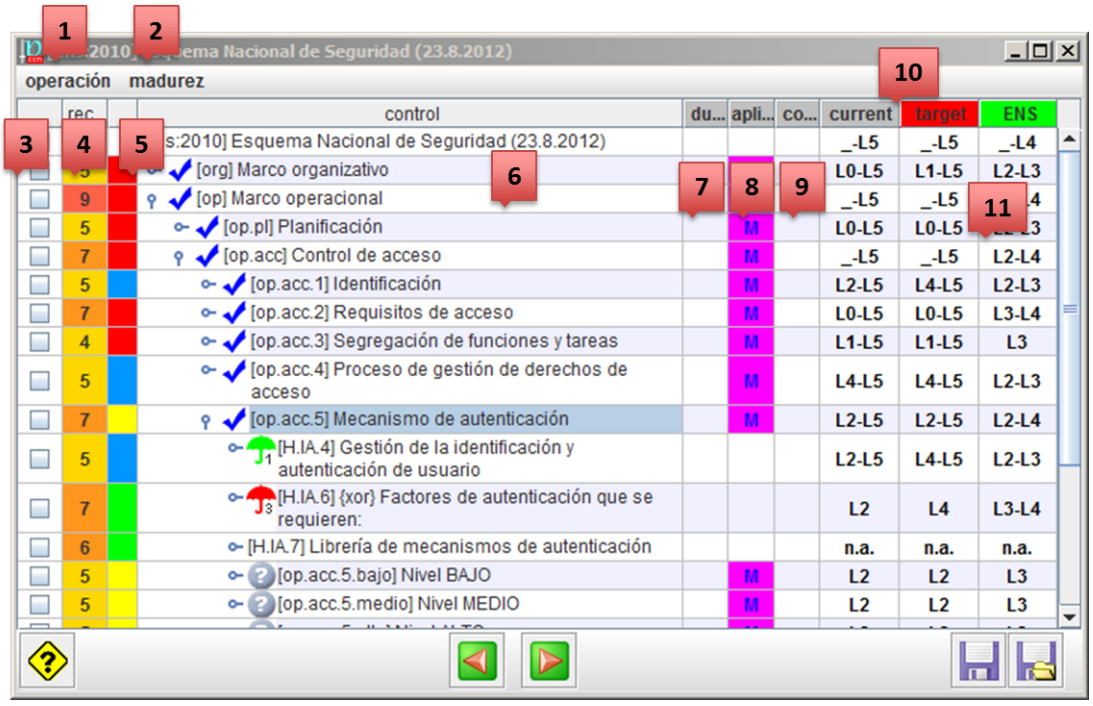
Pantalla que se usa para marcar algunas características del sistema que pueden suponer una vulnerabilidad.



Marque los criterios que considere de aplicación.

8. PERFIL DE SEGURIDAD

Esta pantalla presenta el cumplimiento de un determinado perfil de seguridad.



1	operación	*operation / merge* *operation / draw*
2	porcentaje	En [11] PILAR presenta: **porcentaje** — porcentaje de cumplimiento de los controles — madurez de las salvaguardas **madurez** — madurez de controles y salvaguardas **cobertura de PILAR** — porcentaje de cumplimiento de la recomendación de PILAR para el ENS; es decir, 100% significa que la madurez es igual o superior a la recomendada por PILAR
3		Selecciona filas para *operation / draw* Haga clic en las cajitas para añadir o retirar de la selección. Haga clic con MAYÚSCULAS para seleccionar un rango. Haga clic en la cabecera de la columna para vaciar la selección.
4	recomendación	Un valor en el rango [null .. 10] estimado por PILAR teniendo en cuenta los activos declarados, la valoración en cada dimensión de seguridad y el nivel de riesgo afrontado por esta medida o control.

		La celda queda gris (null) si PILAR no encuentra ninguna razón para recomendar la medida. (o) - PILAR piensa que es excesivo ("overkill"). (u) - PILAR piensa que es insuficiente ("underkill").
5	traffic light	Compra la valoración en la fase de referencia (ROJA) con la valoración en la fase objetivo (VERDE) y muestra un color: ROJO el valor en la fase de referencia es muy inferior al del objetivo AMARILLO el valor en la fase de referencia es inferior al del objetivo VERDE el valor en la fase de referencia es igual al del objetivo AZUL el valor en la fase de referencia es superior al del objetivo Ver "*Fases de referencia y objetivo*".
6		Árbol de controles Presenta los controles que componen el perfil en forma de árbol jerárquico. Cuando terminan los controles formales, PILAR sigue desplegando las salvaguardas asociadas a ellos, o preguntas específicas. Haga clic para expandir / colapsar una rama del árbol. Haga clic con el botón derecho para acceder a "*EVL / tree*".
7	dudas	Para marcar puntos de duda; es decir, si cuando está rellenado la tabla de valores aparecen dudas que deben ser respondidas por alguien más, marque esta columna, simplemente para recordar que faltan datos. Haga clic para cambiar el estado de duda. La marca "flota" a los controles superiores para destacar el problema cuando está anidado.
8	aplica	Ver *EVL / Applicability*
9	comentario	Se usa para asociar comentarios a los controles o salvaguardas. Haga clic para editar un comentario. Cuando hay un comentario asociado, se marca como (*). El cuerpo del comentario puede ser cualquier texto. Además, puede usted introducir URLs para lanzar automáticamente un navegador web; esto es útil, por ejemplo, si se dispone de un sistema de gestión documental en la intranet.

10	fases	Fses del proyecto. Haga clic con el botón izquierdo para seleccionar la fase de referencia (ROJA). Haga clic con el botón derecho para seleccionar la fase objetivo (VERDE). Ver "*Fases de referencia y objetivo*".
11		Ver "*EVL / Valuation*

8.1. IMPORTACIÓN DE VALORES DE OTRO PROYECTO

Si ya ha evaluado otro sistema en el mismo entorno, puede importar aquellas valoraciones en este proyecto. Esta situación es típica de entornos donde se analizan varios sistemas pequeños que están sometidos todos al mismo entorno de protección.

Haga clic para seleccionar otro proyecto (.mgr).

PILAR lee del otro proyecto

- valores para los perfiles de seguridad
- valores para las salvaguardas (ver "*Salvaguardas*")

8.2. EN EL ÁRBOL DE CONTROLES

Haga clic con el botón derecho …

When you right-click on the EVL tree, you may …

copiar

Se copia al portapapeles el código y el nombre de la fila

copiar la ruta

Se copia al portapapeles el código y el nombre de la fila y de sus superiores (el camino que trae a esta file

texto completo

Aparece una ventana con el código y el nombre de la fila

camino completo

Aparece una ventana con el código y el nombre de la fila y de sus superiores (el camino que trae a esta file

descripción

Si el control dispone de información adicional, se presenta. Depende de cada perfil.

cerrar el padre

Se colapsa el árbol a nivel del padre de esta fila.

cerrar los hermanos

Se colapsa el árbol al nivel de esta fila., así como de sus hermanos.

ir ar

para enlaces, , nos lleva al control enlazado.

8.3. EVL - APLICABILIDAD

Para cada control ( ), cada pregunta ( ), y cada salvaguarda ( ) puede indicar si es de aplicación, o no, haciendo clic en la columna APLICA.

Por ejemplo, si tenemos portátiles, pero no tele-trabajo:

[11.7] Equipos móviles y tele-trabajo		...
[11.7.1] Equipos móviles		
[HW.PCD] Informática móvil		
[11.7.2] Teletrabajo		n.a.
[S.TW] Teletrabajo		n.a.

"n.a." significa que la fila no es de aplicación. Los puntos suspensivos significan que hay algo dentro que no aplica.

Cuando selecciona un control y lo marca "n.a.", todos los controles bajo el marcado pasan a "n.a.". Las salvaguardas no están rígidamente conectadas, y aunque un control no aplique, puede que las salvaguardas relacionadas sean de aplicación, o no; tendrá que marcarlo manualmente.

Puede tener diferentes combinaciones de controles y salvaguardas que que son de aplicación, o no.

Por ejemplo

[SI-6] Security Functionality Verification		
[H59] Security functions verification		...
[H591] on start-up		
[H592] on a regular basis		n.a.
[H593] upon command by authorised administrator		n.a.
[H594] {or} when anomalies are discovered ...		...
[H5941] notifies system administrator		
[H5942] shuts the system down		n.a.
[H5943] restarts the system		n.a.

[IA-8] Identification and Authentication (Non- Organizational Users)			n.a.	
[H133] Guest accounts are subject to strict control			n.a.	
[E22] Access method(s)				
[E23] Control and use of unique identifiers				

8.4. CONTROLES DE OBLIGADO CUMPLIMIENTO

Algunos perfiles de seguridad imponen la obligación de cumplir ciertos controles. Es un tema de cumplimiento normativo, a veces dependiente de alguna condición (por ejemplo, que el sistema tenga interconexiones). Cuando estas obligaciones se conocen, PILAR colorea la celda de aplicabilidad.

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

Si un control de obligado cumplimiento se marca como “n.a.”, PILAR mantiene el coloreado de la celda para recordarle que debe justificar la exclusión.

8.5. VALORACIÓN DEL PERFIL

[SC] System and Communications Protection					29%	58%	96%
[SC-1] System and Communications Protection Policy and Procedures					24%	79%	95%
[SC-2] Application Partitioning					50%	45%	98%
[H142] There are separate accounts for security administration					L0	L0	L5
[H287] Administration and operation responsibilities are separated					L5	L3	L4
[H244] Establishment of specific menus to control access to the applications' functions			n.a.				

Para los controles y salvaguardas que son de aplicación, puede indicar una valoración en cada fase del proyecto. La valoración se aplica a las hojas terminales del árbol; si aplica una valoración a un nodo con ramas, el valor se propaga hasta las hojas.

El valor que se muestra en los nodos intermedios depende de la selección en [2].

porcentaje PILAR estima un porcentaje de cumplimiento derivado de los niveles de madurez de las ramas.

madurez PILAR presenta el rango de madurez de las ramas.

ENS PILAR compara la madurez en la fase correspondiente con la madurez de la columna PILAR. Si la madurez es igual o superior, PILAR dice que el cumplimiento es del 100%. Si es inferior, el porcentaje disminuye.

8.6. FASES DE REFERENCIA Y OBJETIVO

El semáforo [22] da una indicación rápida de si el nivel de madurez es suficiente.

Para calcular el color del semáforo, PILAR usa dos fases:

VERDE: fase objetivo

haga clic con el botón derecho en la cabecera de la fase deseada

ROJO: fase de referencia

haga clic con el botón izquierdo en la cabecera de la fase deseada

semáforo código de colores	
AZUL	si la madurez de la fase ROJA es mayor que la de la fase VERDE
VERDE	la madurez ROJA está a la par que la VERDE
AMARILLO	la madurez ROJA es inferior a la VERDE: puede mejorarse
ROJO	la madurez ROJA es muy inferior a la verde: debe mejorarse
GRIS	la medida no es de aplicación

8.7. NIVELES DE MADUREZ

Las salvaguardas se evalúan según la siguiente escala

n.a. – no es aplicable

use este valor cuando la salvaguarda no tiene sentido en el sistema; esté preparado con una buena explicación para justificar la decisión frente al auditor

L0 – inexistente

use este valor cuando la salvaguarda es aplicable y debe estar; pero no está

L1 – iniciado

use este valor cuando la salvaguarda está, pero en un estado incipiente o muy inmaduro

L2 – parcialmente realizado

use este nivel cuando la salvaguarda está e incluso su operación es repetible; pero no existe un procedimiento formal a seguir para gestionarla regularmente; la gestión se realiza de forma intuitiva

L3 – en funcionamiento

use este nivel cuando se sigue un procedimiento de actuación de forma rutinaria

L4 – monitorizado

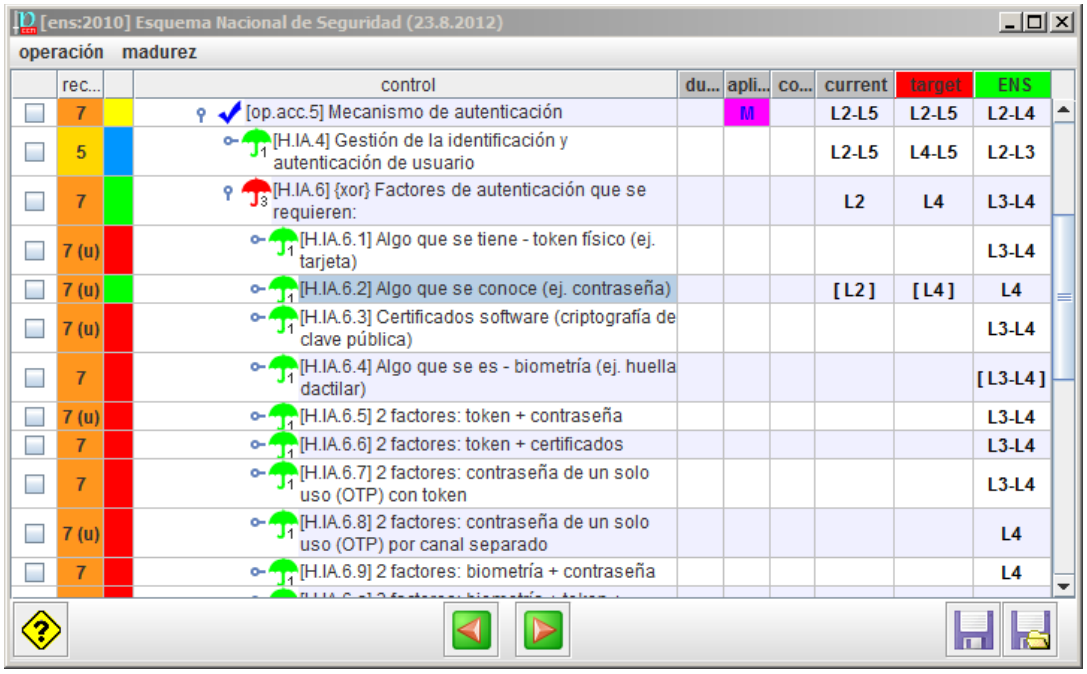
use este nivel cuando se dispone de medidas regulares de la eficacia y eficiencia de la salvaguarda en el desempeño de su cometido

L5 – mejora continua

use este nivel cuando el proceso de gestión es parte de un ciclo de mejora continua – típicamente esto significa que se emplea un sistema de gestión de la seguridad de la información (SGSI)

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

La salvaguarda seleccionada aparece entre llaves cuadradas:



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

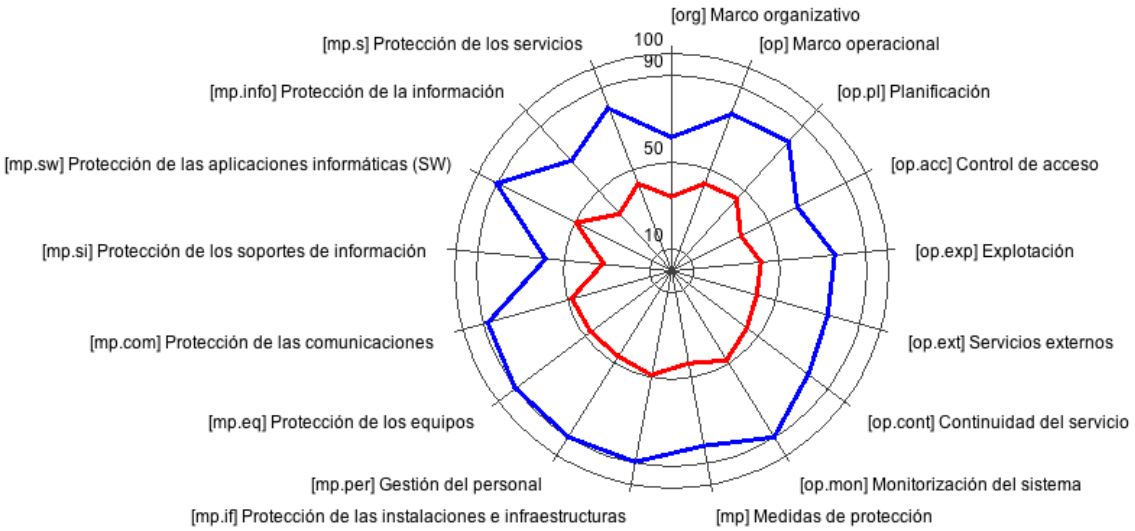
8.8. GRÁFICO

Usted puede seleccionar las líneas que desea llevar al gráfico. Sólo se llevan al gráfico las líneas que se ven y además están seleccionadas.

- Para seleccionar o ignorar una línea, haga clic en la primera columna.
- Para seleccionar un rango, haga clic en la primera línea del rango y MAYÚSCULAS+clic en la última.
- Para borrar la selección, haga clic en la cabecera.
- Cuando no se ha seleccionado nada, PILAR selecciona el segundo nivel del árbol.

Para generar el gráfico

- menú superior OPERACIÖN
- clic GRÁFICO

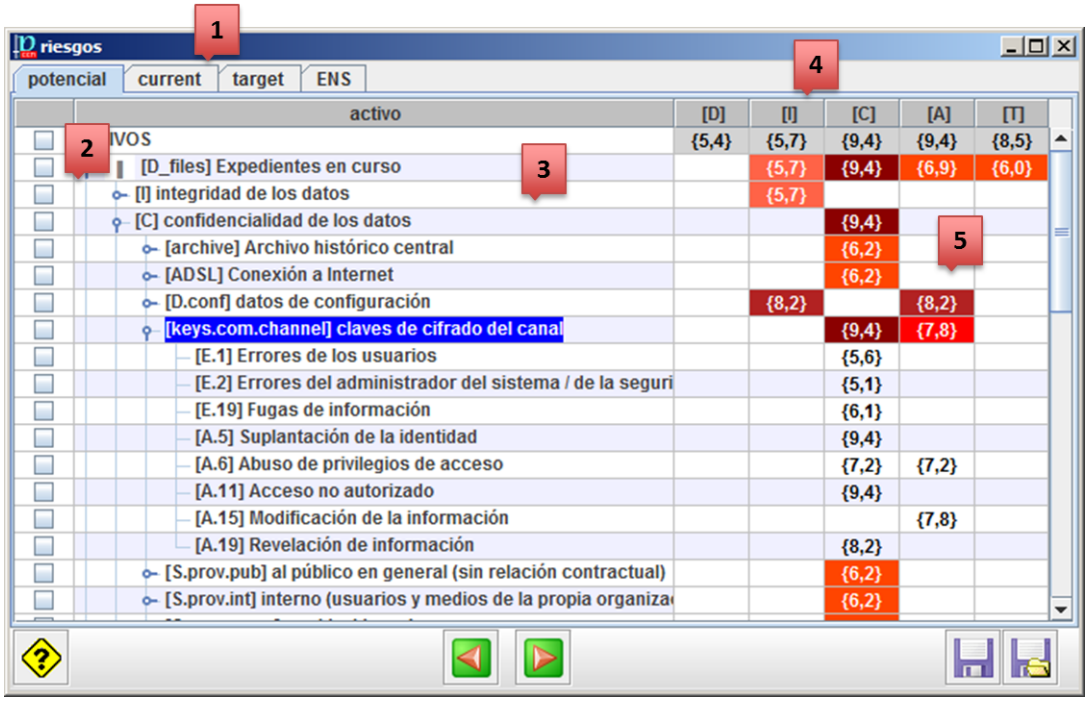


En el menú superior del gráfico puede seleccionar diferentes tipos de gráficas.

-  copia el gráfico al portapapeles; a continuación puede pegarse en otro documento (por ejemplo, e power point o en word)
-  guarda el gráfico en un fichero; puede seleccionar el formato en que se almacena de entre los proporcionados por su sistema (típicamente, todos los sistemas son capaces de generar .PNG y .JPG)
-  envía el gráfico a la impresora

9. RIESGOS

Esta pantalla presenta los resultados del análisis de riesgos. Es una pantalla meramente de presentación, sin que de opción al usuario de introducir datos.



El riesgo se mide en una escala entre 0.0 y 10.0 siguiendo estos criterios:

El uso de un decimal sirve para establecer un orden relativo entre los riesgos del mismo nivel. Por ejemplo, {3.4} es más que {3.0} dentro ambos del nivel 'alto'.

1	fases	Una pestaña por ase. Haga clic para seleccionar. La pseudo-fase "potencial" muestra el riesgo inherente, sin

		salvaguardas.
2	selección	no se usa
3		Árbol de activos. 1er nivel: activos con valor: riesgo repercutido. 2do nivel: reparto del riesgo por dimensión de seguridad. 3er nivel: activos inferiores (en el árbol de dependencias): riesgo acumulado. 4to nivel: amenazas sobre los activos inferiores: riesgo acumulado.
4		Una columna por cada dimensión de seguridad.
5		Riesgo. El riesgo se evalúa por cada amenaza y se va consolidando por activos. La primera fila muestra el riesgo del sistema.

En la parte superior aparecen varias pestañas

POTENCIAL

presenta el riesgo potencial; es decir, el riesgo si no hubiera salvaguardas

CURRENT

riesgo residual a fecha de hoy, cuando se aplican las salvaguardas con la madurez declarada en la fase ‘current’

TARGET

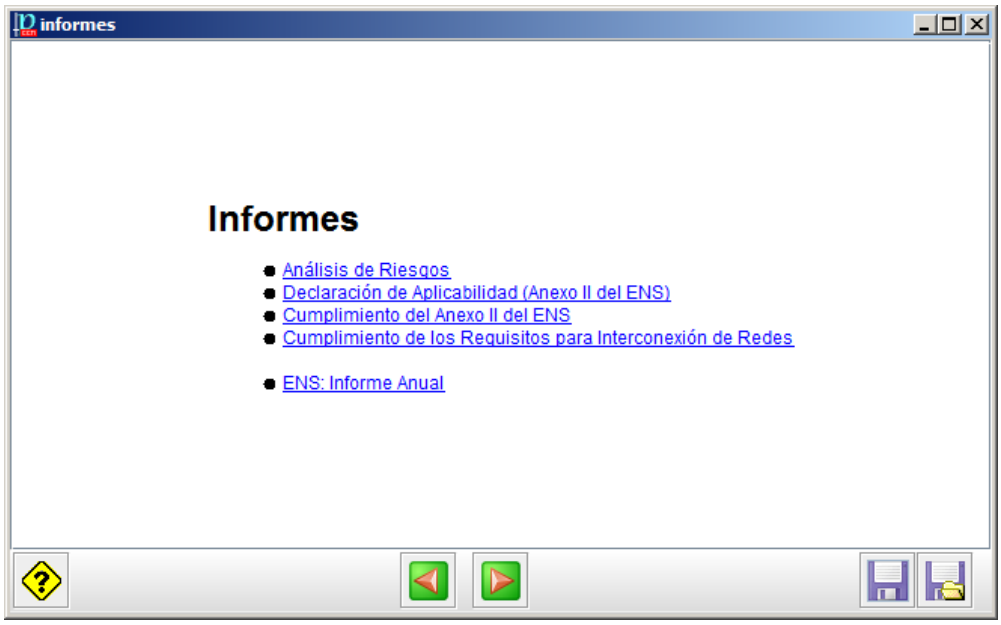
riesgo residual objetivo, cuando se aplican las salvaguardas con la madurez declarada en la fase ‘target’

PILAR

riesgo residual si se siguen las recomendaciones de PILAR

10. INFORMES

PILAR ofrece una serie de informes tipo. Los informes se generan usando el formato RTF que puede ser editado por la mayoría de los procesadores de texto.



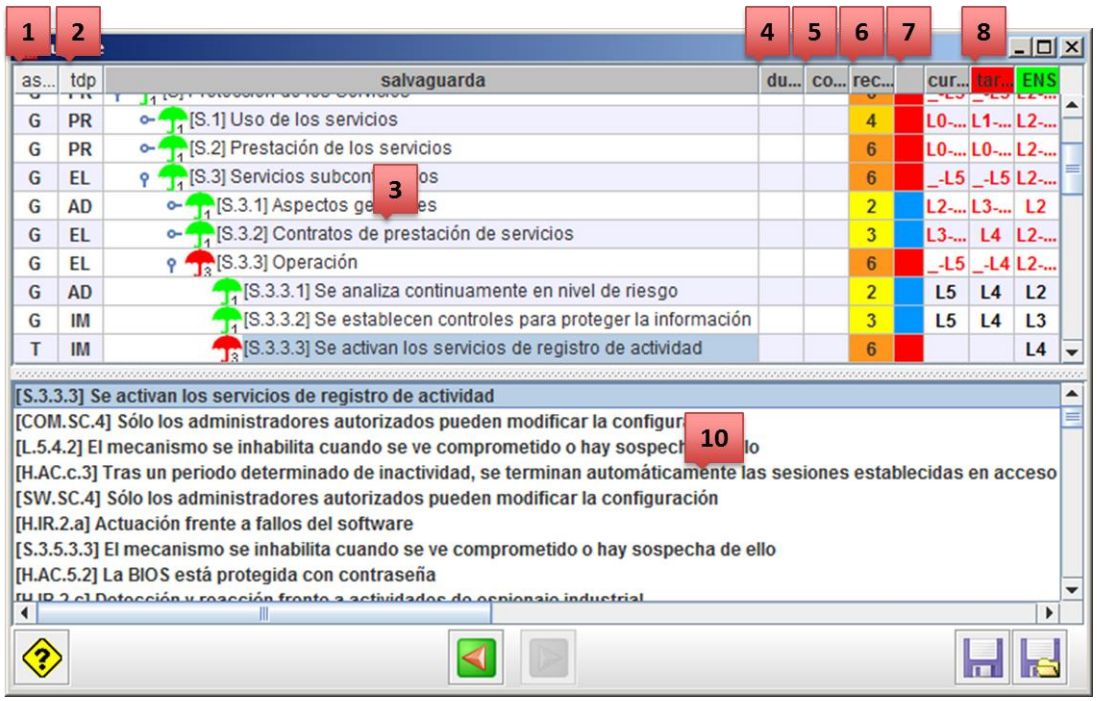
Haga clic en el informe que desea generar.

Si desea elaborar sus propios informes,

- vaya al directorio donde instaló la aplicación
- lea el fichero .CAR para determinar la librería que se usa
- vaya al directorio de la librería
- edite su propio patrón siguiendo las instrucciones disponibles en [http://www.pilar-tools.com/tools/pilar/doc.htm] descargue 'Report Templates'
- cuando el patrón (.RTF) esté listo, dígaselo a µPILAR editando el fichero 'reports.xml' que le asigna un nombre a su fichero y lo hace aparecer en la pantalla de generación de informes

11. MEJORAS

Si no le satisface el riesgo residual presente, puede pedirle a PILAR ideas acerca de cómo mejorar. PILAR presenta una pantalla compleja para orientarle hacia las salvaguardas que pudiera mejorar. Puede seguir las orientaciones de PILAR, o no; la aplicación se limita a analizar el riesgo residual pero es usted y su organismo los que tendrán que vérselas con el riesgo residual que quede.



1	aspecto	Ver "*Salvaguardas / Aspecto*".
2	top	Ver "*Salvaguardas / Tipo de protección*".
3		Árbol de salvaguardas. Ver *Salvaguardas / Peso* Haga clic-clic para colapsar / expandir el árbol. Haga clic con el botón derecho para "*Salvaguardas / Árbol*".
4	dudas	Para marcar puntos de duda; es decir, si cuando está rellenado la tabla de valores aparecen dudas que deben ser respondidas por alguien más, marque esta columna, simplemente para recordar que faltan datos. Haga clic para cambiar el estado de duda. La marca "flota" a los controles superiores para destacar el problema cuando está anidado.
5	comentario	Se usa para asociar comentarios a los controles o salvaguardas. Haga clic para editar un comentario.

		Cuando hay un comentario asociado, se marca como (*). El cuerpo del comentario puede ser cualquier texto. Además, puede usted introducir URLs para lanzar automáticamente un navegador web; esto es útil, por ejemplo, si se dispone de un sistema de gestión documental en la intranet.
6	recomendación	Un valor en el rango [null .. 10] estimado por PILAR teniendo en cuenta los activos declarados, la valoración en cada dimensión de seguridad y el nivel de riesgo afrontado por esta medida o control. La celda queda gris (null) si PILAR no encuentra ninguna razón para recomendar la medida. (o) - PILAR piensa que es excesivo ("overkill"). (u) - PILAR piensa que es insuficiente ("underkill"). Haga clic con el botón derecho para acceder a una pantalla con un resumen de las razones para la recomendación: es decir, los activos y dimensiones que hacen que la salvaguarda sea de aplicación.
7	semáforo	Ver "*Fases de referencia y objetivo*".
8		Fases del proyecto . Ver "*Salvaguardas / Valoración de la madurez*".
10	sugerencias	Salvaguardas cuya madurez se recomienda mejorar en la fase ROJA. PILAR ordena las salvaguardas por orden de prioridad. Para localizar la salvaguarda en el árbol superior, haga clic en la salvaguarda en el panel inferior y PILAR desplegará el árbol superior para ubicarla en su contexto.

11.1. ASPECTO

Aspecto que trata la salvaguarda:

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

11.2. TIPO DE PROTECCIÓN

- PR – prevención
- DR – disuasión
- EL – eliminación
- IM – minimización del impacto
- CR – corrección
- AD – administrativa
- AW – concienciación
- DC – detección
- MN – monitorización

— RC – recuperación

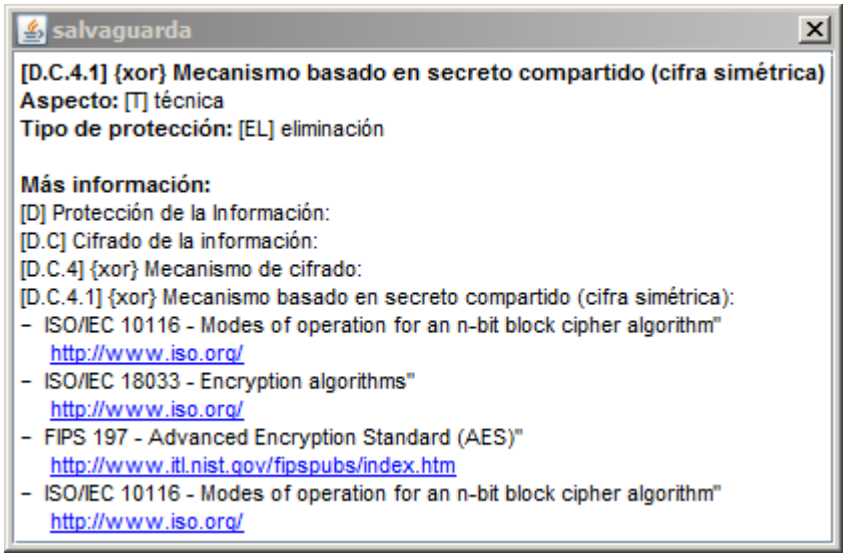
— std – norma
— proc – procedimiento
— cert – certificación o acreditación

11.3. PESO RELATIVO

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

11.4. INFORMACIÓN ADICIONAL

Una ventana separada presenta información adicional relativa a la salvaguarda



11.5. 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

11.6. VALORACIÓN DE LA MADUREZ DE LAS SALVAGUARDAS

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. Si después de esa búsqueda sigue sin valor, se usa el valor "L0".

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

código de color	
caracteres rojos	cuando el valor se calcula a partir de otros
negro sobre blanco	cuando el valor es explícito

Para cambiar un valor de madurez

- haga clic con el botón derecho y elija un valor
- seleccione una o más celdas (filas y columnas), luego copie y pegue

12. PERSONALIZACIÓN

Dispone de amplias opciones para personalizar la herramienta. Para ello debe editar los ficheros del directorio de la biblioteca.

Puede ubicar el directorio de biblioteca leyendo el fichero *Fichero de configuración* que elige en la primara pantalla.

- Puede añadir nuevos tipos de activos
- Puede añadir nuevos criterios de valoración
- Puede añadir nuevas amenazas
- Puede adaptar el perfil de amenazas
- Puede preparar sus propios informes

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

12.1. FICHERO DE CONFIGURACIÓN

La distribución de PILAR incluye ficheros de configuración que se copian en el directorio de instalación.

Busque ficheros con este patrón

MICRO_ … _ens.car

La distribución estándar debería ser suficiente para las necesidades de la mayor parte de los usuarios.

El fichero es texto. Puede editarlo fácilmente para adecuar el idioma, y los directorios.