GUÍA DE SEGURIDAD
(CCN-STIC-473A)

µPILAR

MARZO 2011

Edita:

NIPO: 075-11-055-4

Tirada: 1000 ejemplares
Fecha de Edición: marzo de 2011
José Antonio Mañas ha elaborado el 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.

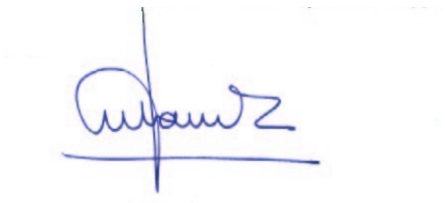
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia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

Marzo de 2011



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN 4
1.1. LECTURAS RECOMENDADAS 4
2. OBJETO 4
3. ALCANCE 5
4. INSTALACIÓN 5
4.1. ENTORNO JAVA 5
4.2. PILAR (WINDOWS) 5
4.3. PILAR (UNIX, LINUX, …) 5
4.4. PILAR (MAC OS X) 5
4.5. USO 5
5. PRIMERA PANTALLA 6
6. DATOS DEL PROYECTO 7
7. ACTIVOS ESENCIALES 7
7.1. MODIFICACIÓN DE UN ACTIVO (EDICIÓN) 9
7.2. VALORACIÓN 9
8. OTROS ACTIVOS 10
9. VULNERABILIDADES 12
10. PERFIL DE SEGURIDAD 13
10.1. NIVELES DE MADUREZ 14
10.2. IMPORTACIÓN DE VALORES DE OTRO PROYECTO 14
10.3. SEMÁFORO DE CUMPLIMIENTO 14
10.4. GRÁFICO 15
10.5. OTROS BOTONES 16
11. RIESGOS 16
11.1. GRÁFICO 18
12. INFORMES 19
13. MEJORAS 20
13.1. SEMÁFORO DE MADUREZ 21
14. PERSONALIZACIÓN 22
ANEXO A. GLOSARIO DE TÉRMINOS Y ABREVIATURAS 24
ANEXO B. REFERENCIAS 27

1. INTRODUCCIÓN

1. 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.
2. 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.
3. 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.
4. PILAR implementa la metodología Magerit: [[http://www.csi.map.es/csi/pg5m20.htm]]
5. microPILAR 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.
6. A la hora de seleccionar salvaguardas, microPILAR 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.
7. La información recopilada por microPILAR 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

8. Glosario de Términos
   [[http://www.ar-tools.com/glossary/index.html]]
9. Magerit:
   Capítulo 2, "Realización del Análisis y de la Gestión", dentro del “Libro I, Método”.
   [[http://www.csi.map.es/csi/pg5m20.htm]]
10. UNE 71504:2008 – Metodología de análisis y gestión de riesgos de los sistemas de información, AENOR.
    [[http://www.aenor.es/]]
11. ISO/IEC 27005:2008 - Tecnología de información - Técnicas de seguridad - Gestión de riesgos de seguridad de la información.
    [[http://www.iso.org/]]
12. ISO 31000:2009 – Gestión del riesgo – Principios y directrices.
    [[http://www.iso.org/]]
13. NIST SP 800-30:2002 - Risk Management Guide for Information Technology Systems.
    [[http://csrc.nist.gov/publications/PubsSPs.html]]

2. OBJETO

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

3. ALCANCE

15. Las Autoridades responsables de la aplicación de la Política de Seguridad de las TIC determinarán su aplicación a los Sistemas de su Organización bajo su responsabilidad.

4. INSTALACIÓN

4.1. ENTORNO JAVA

16. 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

4.2. PILAR (WINDOWS)

17. 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.

4.3. PILAR (UNIX, LINUX, …)

18. Normalmente java ya viene instalado en el sistema.

19. 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.

4.4. PILAR (MAC OS X)

20. 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_51.app

4.5. USO

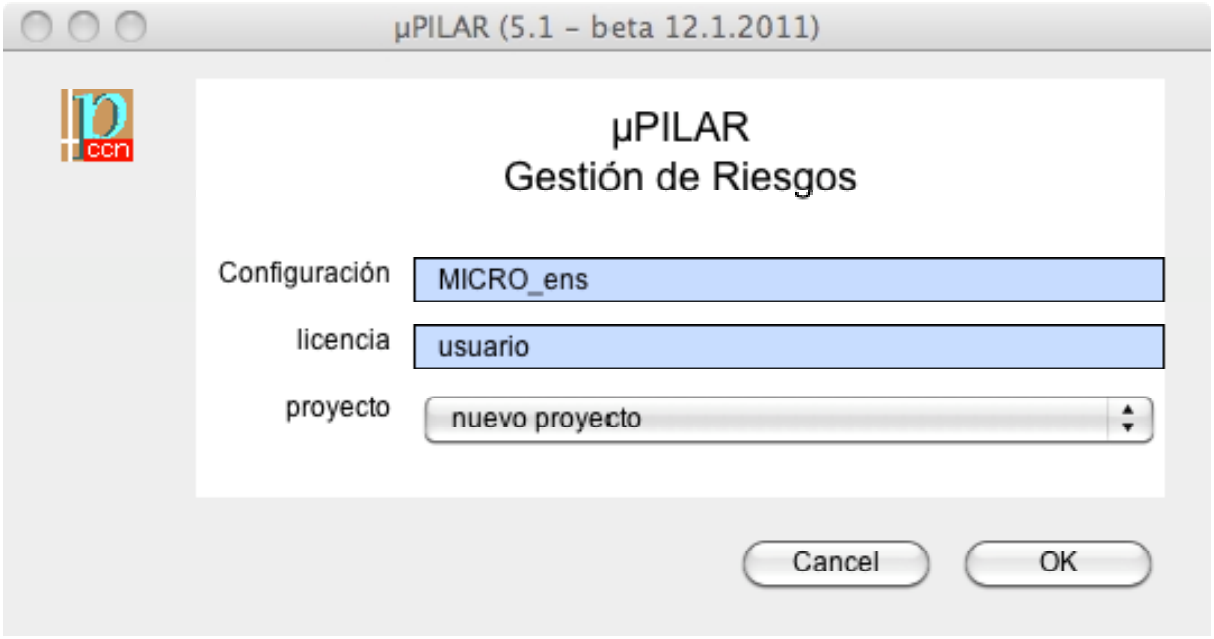
21. Ejecute pilarmicro:

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

- llevándole a la “primera pantalla”.

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

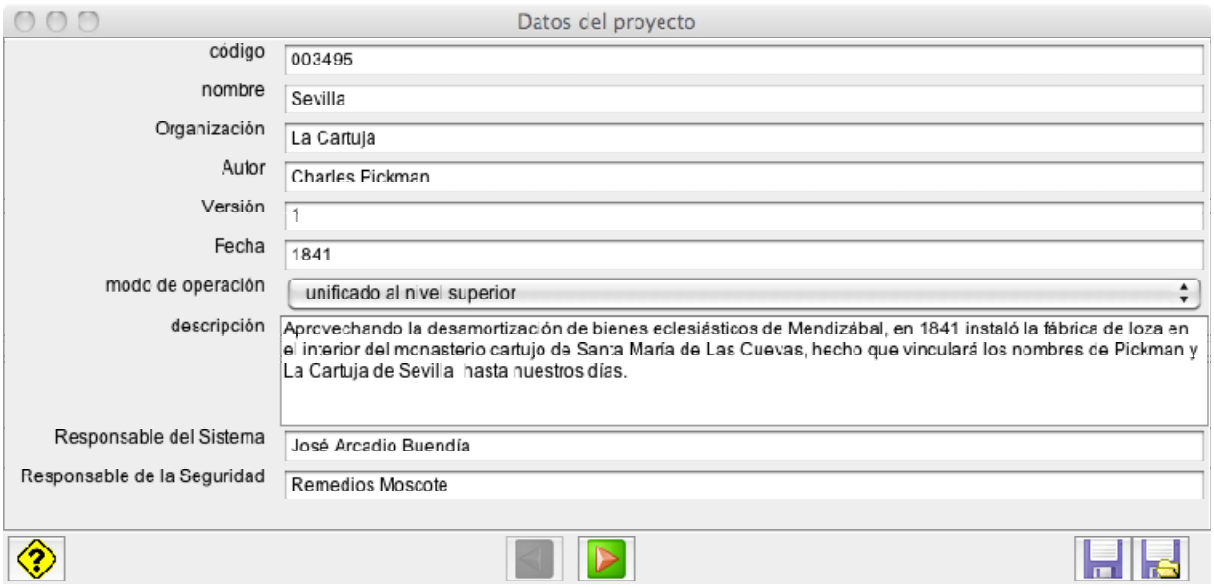
5. PRIMERA PANTALLA



23. Para cambiar la configuración
    - clic-clic en la cajita de configuración
    - seleccione el fichero de configuración (.CAR)
24. Para seleccionar / cambiar la licencia
    - clic-clic en la cajita de licencia
    - seleccione el fichero de licencia (.LIC)
25. La pantalla presentará el nombre del titular de la licencia. Si no tuviera una licencia válida, la cajita presenta el texto ¡sin licencia”; sin una licencia válida sólo se permite ver el análisis, pero no modificar datos.
26. El combo de proyecto permite:
    - iniciar un nuevo proyecto
    - abrir un proyecto ya existente
    - ir directamente a alguno de los últimos proyectos con los que hemos trabajado
    - seleccione lo apropiado desplegando el combo
27. Cuando tenga listo el contexto, clic en OK para proseguir. Si es la primera vez que ejecuta el programa, aparecerán los términos de uso de la herramienta. O bien acepta las condiciones de uso, o debe terminar el uso de la herramienta.

6. DATOS DEL PROYECTO

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



29. Para guardar una copia del proyecto en el disco
    - clic en el botón GUARDAR

30. Para guardar una copia en un fichero con otro nombre
    - clic en el botón GUARDAR COMO

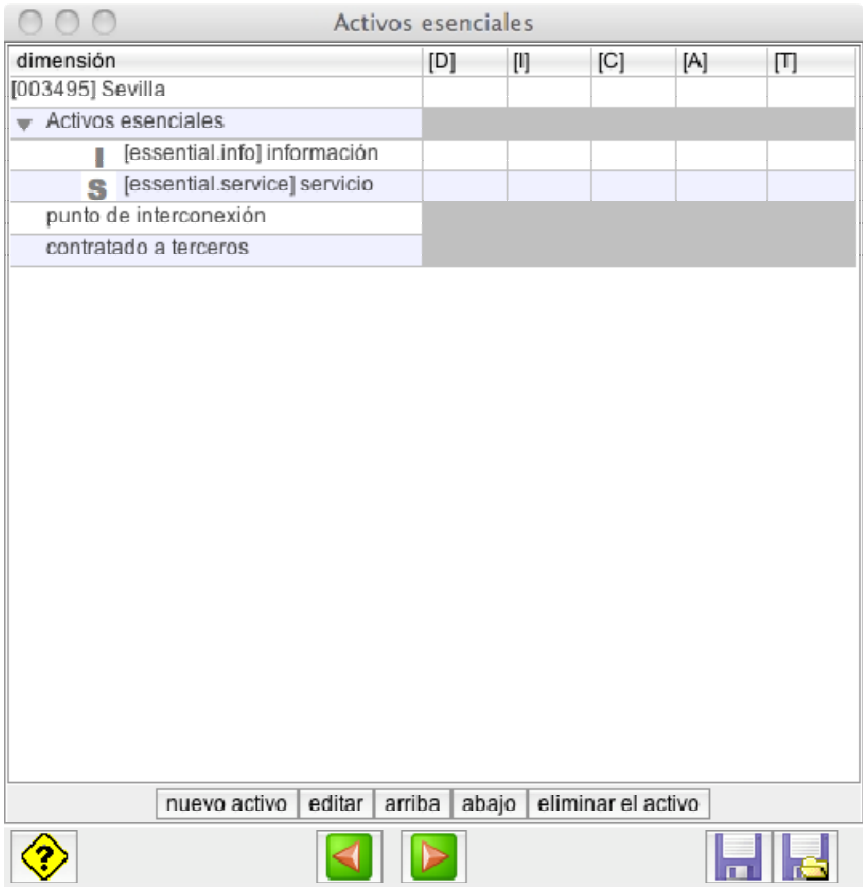
31. Para pasar a la siguiente pantalla
    - clic en el botón con la fecha a la derecha

7. ACTIVOS ESENCIALES

32. 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

33. 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.

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



35. 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

36. Para guardar una copia del proyecto en el disco
    - clic en el botón GUARDAR

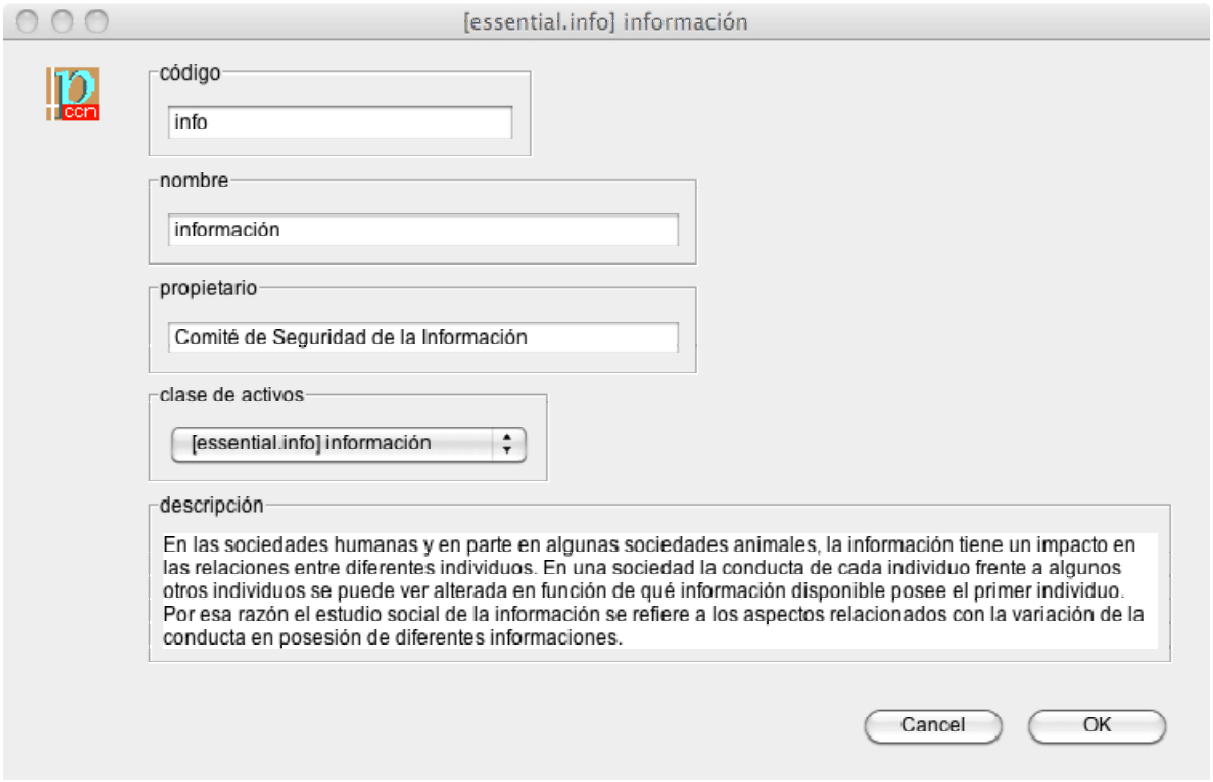
37. Para guardar una copia en un fichero con otro nombre
    - clic en el botón GUARDAR COMO

38. Para regresar a la pantalla anterior
    - clic en el botón con la fecha a la izquierda

39. Para pasar a la siguiente pantalla
    - clic en el botón con la fecha a la derecha

7.1. MODIFICACIÓN DE UN ACTIVO (EDICIÓN)

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



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

42. Puede introducir cualquier nombre, propietario y descripción.

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

44. El activo debe ser de alguna de las clases que se despliegan con el combo. En la pantalla principal, el activo se ubicará automáticamente en la zona del árbo que le corresponda en función de su clase.

7.2. VALORACIÓN

45. 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

46. 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 nivel más externo del árbol.

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

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

49. Los puntos de interconexión y los servicios deben ser protegidos al nivel establecido para el sistema (el mayor en cada dimensión). No obstante, puede especificar para estos activos que un cierto nivel no es de aplicación (n.a.). Esta situación aparece cuando el valor en este sistema no trasciende los demás.

dimensión	[D]	[I]	[C]	[A]	[T]
[003495] Sevilla	[M]	[M]	[A]	[A]	[M]
▼ Activos esenciales					
I [essential.info] información		[M]	[A]	[A]	[M]
S [essential.service] servicio	[M]			[M]	[M]
▼ punto de interconexión					
[ip1] punto de interconexión #1	[M]	[M]	[A]	[A]	[M]
[ip2] punto de interconexión #2	[n.a.]	[M]	[A]	[A]	[M]
▼ contratado a terceros					
[S.cont] proporcionado por un tercer	[M]	[n.a.]	[n.a.]	[n.a.]	[n.a.]

8. OTROS ACTIVOS

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

[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

51. Para seleccionar o eliminar una clase

- haga clic en ella

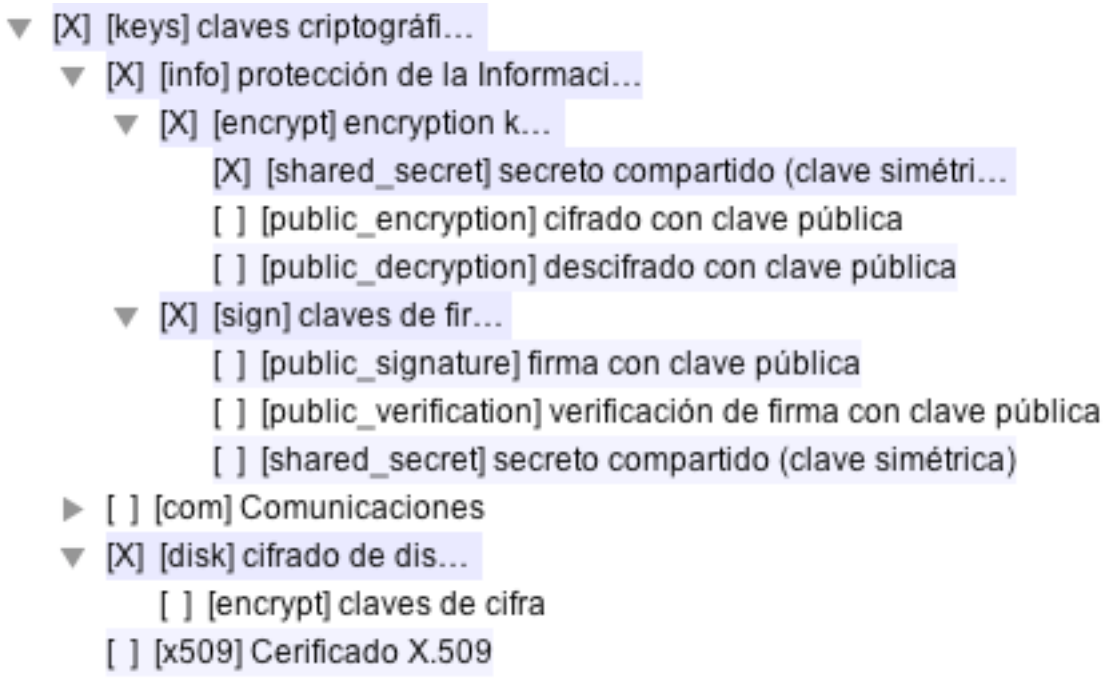
52. Para limpiar una clase (es decir, para eliminar las clases que tienen subclases marcadas)

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

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

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

54. Ejemplo



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

55. Para guardar una copia del proyecto en el disco
    - clic en el botón GUARDAR

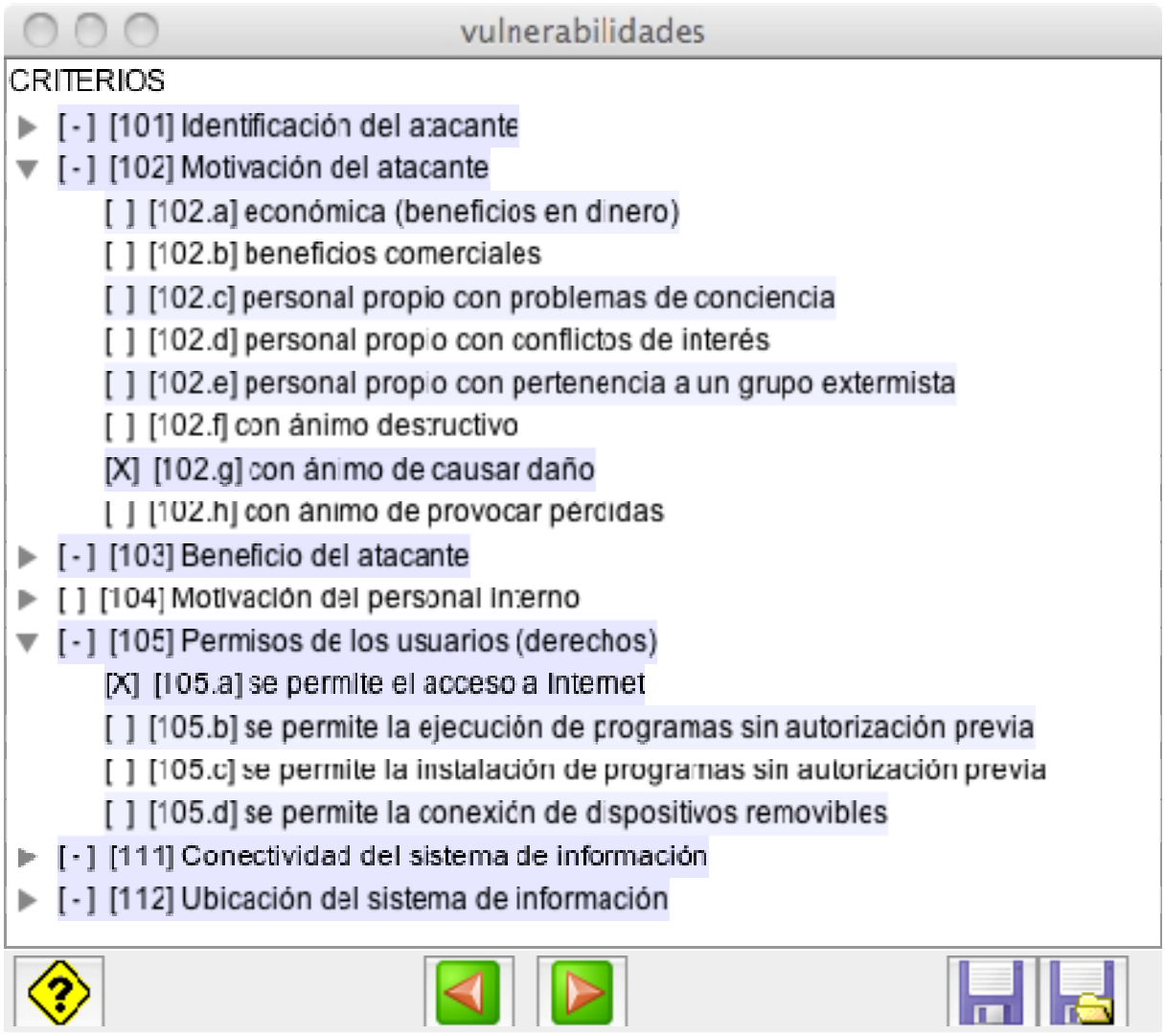
56. Para guardar una copia en un fichero con otro nombre
    - clic en el botón GUARDAR COMO

57. Para regresar a la pantalla anterior
    - clic en el botón con la fecha a la izquierda

58. Para pasar a la siguiente pantalla
    - clic en el botón con la fecha a la derecha

9. VULNERABILIDADES

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



60. Para seleccionar una vulnerabilidad
    - haga clic en ella

61. Para eliminar una vulnerabilidad
    - haga clic en ella

62. Para guardar una copia del proyecto en el disco
    - clic en el botón GUARDAR

63. Para guardar una copia en un fichero con otro nombre
    - clic en el botón GUARDAR COMO

64. Para regresar a la pantalla anterior
    - clic en el botón con la fecha a la izquierda

65. Para pasar a la siguiente pantalla

    - clic en el botón con la fecha a la derecha

10. PERFIL DE SEGURIDAD

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

67. Columna 1 – se usa para seleccionar líneas para el informe gráfico

68. Columna 2 – presenta un nivel de recomendación calcula por PILAR teniendo en cuenta los activos del sistema y su valoración.

69. Columna 3 – presenta un semáforo que un resumen conciso del grado de cumplimiento del perfil. Ver más abajo.

70. Columna 4 – describe 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

71. Columna 5 – usada 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

72. Columna 6 – se usa para indicar que un control o salvaguarda no es de aplicación (n.a.). Lo más normal es que todos los controles y salvaguardas sean aplicables, así que si va a marcar algo como n.a., esté preparado para explicárselo al auditor.

    - haga clic para cambiar el estado

    PILAR presenta unos PUNTOS para indicar que esta rama del árbol tiene bajo ella cosas que aplican y cosas que no.

    La celda se colorea y contiene una M (de ‘mandatory’), cuando el perfil de seguridad dice que es de obligado cumplimiento. Aunque PILAR permite decir que un control no aplica aún siendo de obligado cumplimiento, esté preparado para explicárselo muy clarito a los auditores. PILAR retiene el color de la celda aunque se indique que no es de aplicación, a modo de recordatorio.

73. Columna 7 – 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.

74. Columnas 8, 9 – presentan el grado de cumplimiento de los controles en forma de porcentaje. Los porcentajes se calculan en base a la madurez de las salvaguardas que los materializan.

Típicamente, PILAR usa 2 fases para capturar la evolución de la seguridad: la situación actual (CURRENT) y un objetivo (TARGET).

Cuando se asigna un nivel de madurez a una salvaguarda en una fase, éste mismo nivel se traslada automáticamente a las fases posteriores, salvo que se indique un nuevo nivel.

10.1. NIVELES DE MADUREZ

75. 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)

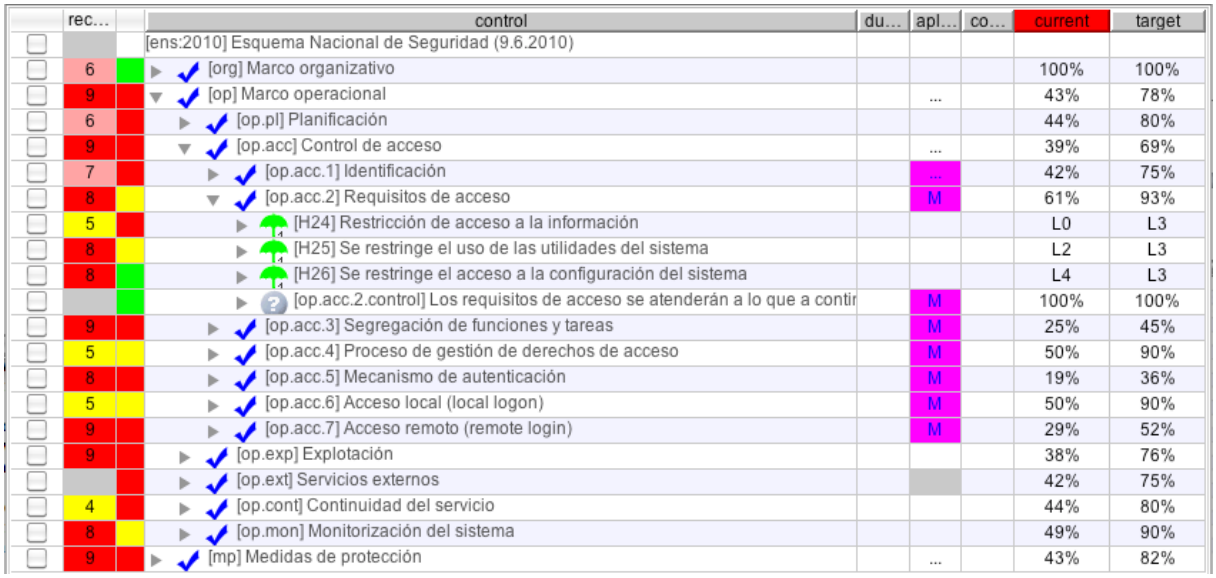
10.2. IMPORTACIÓN DE VALORES DE OTRO PROYECTO

76. 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.

- menú superior OPERACIÓN
- clic IMPORTAR
- seleccione un proyecto para importar datos de él

10.3. SEMÁFORO DE CUMPLIMIENTO

77. La tercera columna presenta un semáforo que resume la madurez de la línea.



rec…	control	du…	apl…	co…	current	target
	[ens:2010] Esquema Nacional de Seguridad (9.6.2010)					
6	[org] Marco organizativo				100%	100%
9	[op] Marco operacional		…		43%	78%
6	[op.pl] Planificación				44%	80%
9	[op.acc] Control de acceso		…		39%	69%
7	[op.acc.1] Identificación		…		42%	75%
8	[op.acc.2] Requisitos de acceso		M		61%	93%
5	[H24] Restricción de acceso a la información				L0	L3
8	[H25] Se restringe el uso de las utilidades del sistema				L2	L3
8	[H26] Se restringe el acceso a la configuración del sistema				L4	L3
	[op.acc.2.control] Los requisitos de acceso se atenderán a lo que a contir		M		100%	100%
9	[op.acc.3] Segregación de funciones y tareas		M		25%	45%
5	[op.acc.4] Proceso de gestión de derechos de acceso		M		50%	90%
8	[op.acc.5] Mecanismo de autenticación		M		19%	36%
5	[op.acc.6] Acceso local (local logon)		M		50%	90%
9	[op.acc.7] Acceso remoto (remote login)		M		29%	52%
9	[op.exp] Explotación				38%	76%
	[op.ext] Servicios externos				42%	75%
4	[op.cont] Continuidad del servicio				44%	80%
8	[op.mon] Monitorización del sistema				49%	90%
9	[mp] Medidas de protección		…		43%	82%

ROJO	cumplimiento muy pobre; o sea, madurez muy baja
VERDE	excelente cumplimiento
AMARILLO	cumplimiento parcial
GRIS	PILAR no ve ninguna razón para aplicar esta línea, o usted la ha marcado como N.A.
NEGRO	cuando la línea se marca como “NO SE”

78. Puede seleccionar respecto de qué fase se evalúa el semáforo

- clic en la cabecera de la columna de la fase deseada
- la cabecera se pinta en ROJO para que se vea que es la seleccionada

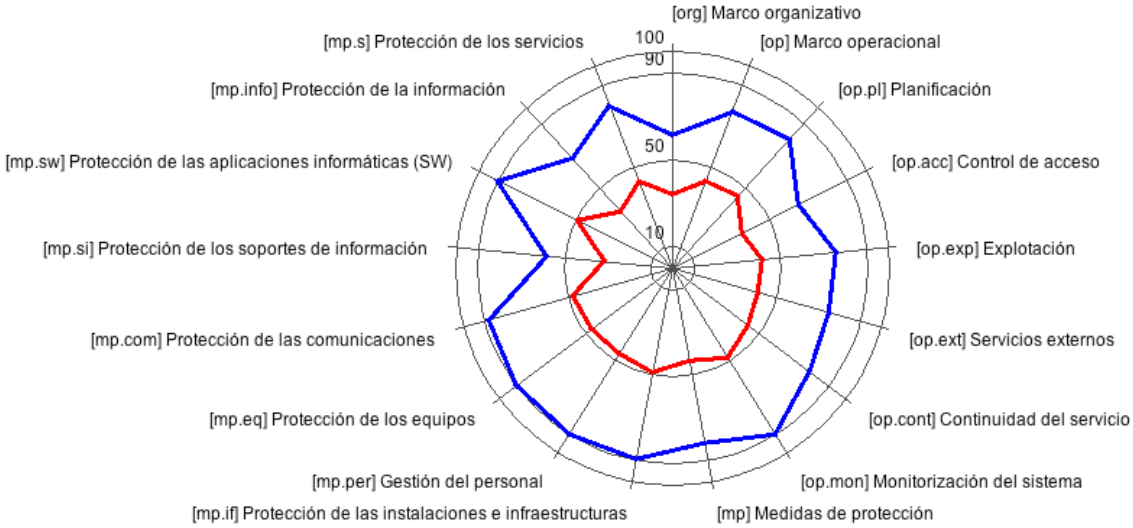
10.4. GRÁFICO

79. 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.

80. Para generar el gráfico

- menú superior OPERACIÖN
- clic GRÁFICO



81. 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

10.5. OTROS BOTONES

82. Para guardar una copia del proyecto en el disco
    - clic en el botón GUARDAR
83. Para guardar una copia en un fichero con otro nombre
    - clic en el botón GUARDAR COMO
84. Para regresar a la pantalla anterior
    - clic en el botón con la fecha a la izquierda
85. Para pasar a la siguiente pantalla
    - clic en el botón con la fecha a la derecha

11. RIESGOS

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

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

{5}	crítico
{4}	muy alto
{3}	alto

{2}	medio
{1}	bajo
{0}	despreciable

88. 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'.

89. En la parte superior aparecen 3 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'

90. Las columnas presentan el riesgo en cada dimensión de seguridad:

[D] disponibilidad

[I] integridad

[C] confidencialidad

[A] autenticidad

[T] trazabilidad

activo	[D]	[I]	[C]	[A]	[T]
[código] denominación del sistema	{2,1}	{2,1}	{3,8}	{2,1}	{2,1}
[essential.info] información		{2,1}	{3,8}		
[D.adm] datos de interés para la administración pública		{1,9}	{3,7}		
[E.1] Errores de los usuarios	{0,0}	{0,0}	{1,8}		
[E.2] Errores del administrador	{0,0}	{0,0}	{1,4}		
[E.15] Alteración de la información		{0,0}			
[E.19] Fugas de información			{0,9}		
[A.5] Suplantación de la identidad del usuario		{0,0}	{3,0}	{1,7}	
[A.6] Abuso de privilegios de acceso		{0,0}	{3,0}		
[A.11] Acceso no autorizado		{0,7}	{3,7}		
[A.15] Modificación de la información		{1,7}			
[A.19] Divulgación de información			{3,5}		
[D.conf] datos de configuración		{1,9}	{3,7}		
[D.log] registro de actividad (log)		{2,1}	{3,8}		
[D.per.M] de nivel medio		{1,9}	{3,7}		
[S.www] world wide web		{1,1}	{2,8}		
[S.file] almacenamiento de ficheros		{1,1}	{2,8}		
[S.print] servicio de impresión		{1,1}	{2,8}		
[S.backup] servicio de copias de respaldo (backup)		{1,1}	{2,8}		
[SW.prp] desarrollo propio (in house)		{1,6}	{3,4}		
[SW.std.www] servidor de presentación		{1,8}	{3,6}		
[SW.std.app] servidor de aplicaciones		{1,8}	{3,6}		
[SW.std.email_server] servidor de correo electrónico		{1,8}	{3,6}		

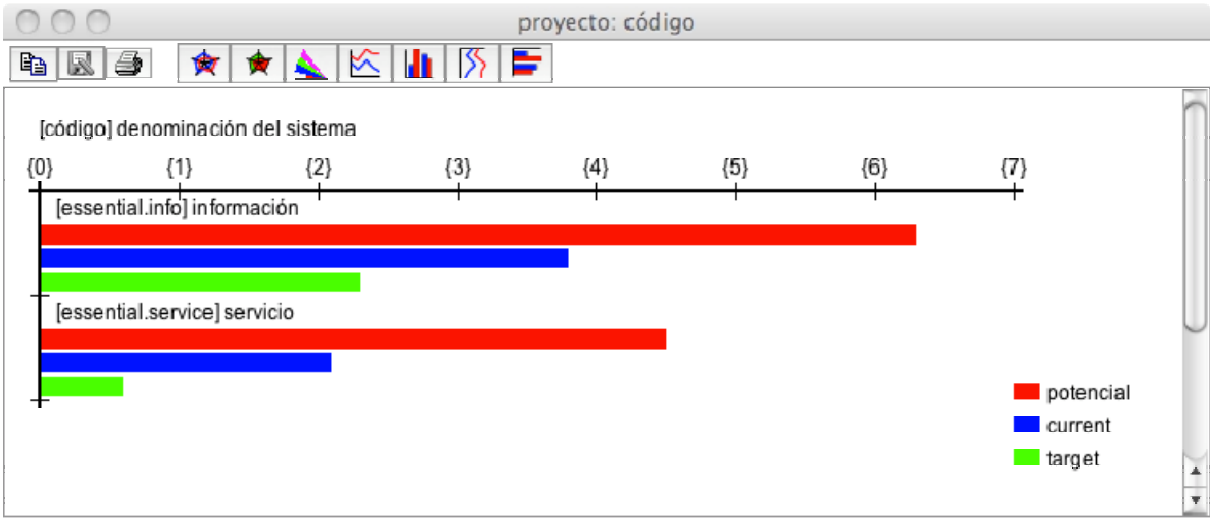
91. La primera fila presenta el riesgo global en el sistema.
92. Las demás filas presentan el riesgo sobre los diferentes activos del sistema.
93. El primer nivel de expansión muestra los activos esenciales y el riesgo repercutido sobre ellos.
94. Cuando va desplegando sucesivos niveles del árbol, va apareciendo el riesgo acumulado en los demás activos y el riesgo asociado a cada amenaza concreta.
95. Para guardar una copia del proyecto en el disco
    - clic en el botón GUARDAR
96. Para guardar una copia en un fichero con otro nombre
    - clic en el botón GUARDAR COMO
97. Para regresar a la pantalla anterior
    - clic en el botón con la fecha a la izquierda
98. Para pasar a la siguiente pantalla
    - clic en el botón con la fecha a la derecha

11.1. GRÁFICO

99. Usted puede seleccionar activos para una representación gráfica de la evolución del riesgo.
100. 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
101. Para generar el gráfico para un activo esencial
    - seleccione 1 activo esencial
    - botón derecho
    - clic GRÁFICO

102. Para generar el gráfico para todos los activos en el sistems

- botón derecho sobre la línea del sistema
- clic GRÁFICO



12. INFORMES

103. 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.

104. 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.ar-tools.com/tools/pilar/doc.htm
  descargue 'Report Templates'
- cuando el patrón (.RTF) esté listo, dígaselo a microPILAR editando el fichero 'reports.xml' que le asigna un nombre a su fichero y lo hace aparecer en la pantalla de generación de informes

105. Para guardar una copia del proyecto en el disco
    - clic en el botón GUARDAR

106. Para guardar una copia en un fichero con otro nombre
    - clic en el botón GUARDAR COMO

107. Para regresar a la pantalla anterior
    - clic en el botón con la fecha a la izquierda

108. Para pasar a la siguiente pantalla
    - clic en el botón con la fecha a la derecha

13. MEJORAS

109. 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.

110. Puede ser conveniente que consulte la terminología de PILAR en el glosario de términos

    http://www.ar-tools.com/glossary/index.html

111. La columna 1 presenta es aspecto de seguridad que contempla la salvaguarda.

112. La columna 2 presenta el tipo de protección que proporciona la salvaguarda.

113. La columna 3 presenta en forma jerárquica el conjunto de salvaguardas relacionadas con el perfil de seguridad que estemos usando.

    Dentro de cada grupo de salvaguardas, los paragüitas se colorean para indicar la importancia relativa de cada salvaguarda en el grupo:

PARAGUAS ROJO	3	crítica
PARAGUAS NARANJA	2	muy importante
PARAGUAS VERDE	1	importante
PARAGUAS GRIS	0	interesante

114. La columna 4 se usa para marcar dudas pendiente de resolver
    - haga clic para cambiar de estado

115. La columna 5 se usa para asociar comentarios
    - haga clic para cambiar de estado

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.

116. La columna 6 presenta un nivel de recomendación (0-10) calcula por PILAR teniendo en cuenta la valoración del sistema y los tipos de activos que lo componen.

117. La columna 7 presenta en forma de semáforo una estimación concisa del grado de madurez de la salvaguarda, teniendo en cuenta la recomendación de la columna 6.

118. Las columnas 8, 9 presentan la madurez de la salvaguarda en cada fase.

119. El panel inferior presenta las salvaguardas cuya madurez se recomienda mejorar en la fase TARGET. PILAR ordena las salvaguardas por orden de prioridad.

120. 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.

121. Para guardar una copia del proyecto en el disco

- clic en el botón GUARDAR

122. Para guardar una copia en un fichero con otro nombre

- clic en el botón GUARDAR COMO

123. Para regresar a la pantalla anterior

- clic en el botón con la fecha a la izquierda

13.1. SEMÁFORO DE MADUREZ

124. La columna 7 presenta en forma de semáforo si la madurez de la salvaguarda es suficiente.

125. A fin de calcular el color del semáforo, PILAR usa 2 referencias:

- **la madurez objetivo**

  Por defecto, es L4; este valor por defecto es útil para un coloreado absoluto.

  Alternativamente, PILAR puede pintar un color relativo a otra fase:

  usted puede seleccionar una fase como referencia, es decir, usar la madurez de la salvaguarda en la fase seleccionada

  - 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
    - el color es relativo a la madurez de la salvaguarda en la fase seleccionada

  Para regresar a la madurez por defecto, haga clic con el botón derecho en cualquier cabecera que no sea de una de las fases.

- **la madurez evaluada**

  Por defecto, PILAR compara la madurez de la última fase con la madurez objetivo.

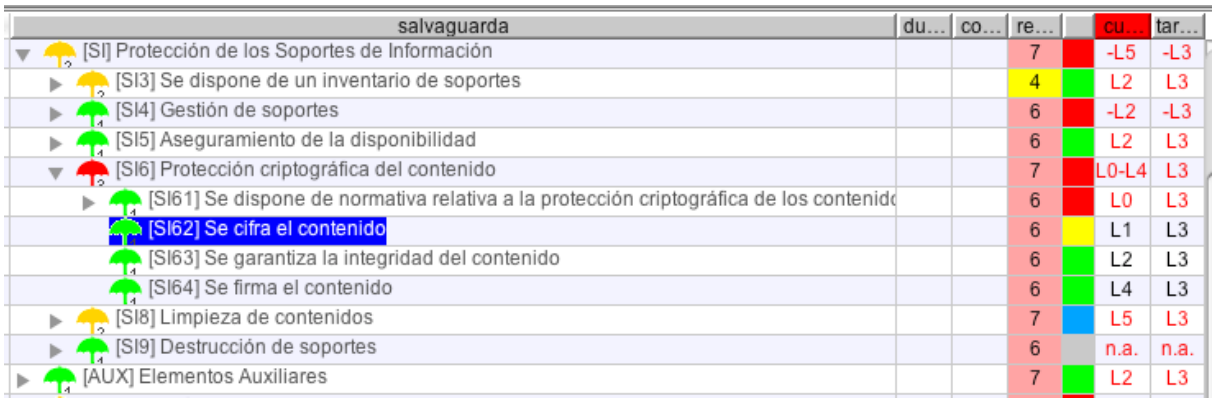
  Puede seleccionar cualquier fase como objeto de comparación:

  - haga clic en la cabecera de la fase que desea evaluar

  La cabecera de la fase seleccionada se pinta en ROJO.

126. Usando la información anterior, PILAR decide un color:

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



14. PERSONALIZACIÓN

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

128. Puede ubicar el directorio de biblioteca leyendo el fichero .CAR 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

129. Vea http://www.ar-tools.com/tools/pilar/doc.htm

ANEXO A. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Activos

Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su Dirección.

Activos esenciales

Activos del sistema de información que tienen unos requisitos de seguridad propios, a diferencia de otros elementos cuyos requisitos de seguridad derivan de la información y los servicios que soportan.

Amenazas

Cualquier cosa que puede suceder y que, cuando ocurre, tiene consecuencias negativas sobre el valor de nuestros activos.

Análisis de riesgos

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Autenticidad

Aseguramiento de la identidad u origen.

Confidencialidad

Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

Criterios de valoración

Criterios o razones usadas para asignar un valor a un activo.

Declaración de aplicabilidad

Declaración oficial que establece que las salvaguardias (o controles) son apropiados para un sistema de información.

Disponibilidad

Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Gestión de riesgos

Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos. ENS.

Incidente de seguridad

Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información. ENS.

Información

Caso concreto de un cierto tipo de información.

Information. An instance of an information type. FIPS 199.

Integridad

Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

Responsable de la información

Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Information Owner. Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. CNSS Inst. 4009.

Responsable de la seguridad

El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

The **Computer Security Program Manager** (and support staff) directs the organization's day-today management of its computer security program. This individual is also responsible for coordinating all security-related interactions among organizational elements involved in the computer security program as well as those external to the organization. NIST Special Publication 800-12.

Information systems security manager (ISSM). Individual responsible for a program, organization, system, or enclave's information assurance program. CNSS Inst. 4009.

Responsable del servicio

Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema

Persona que se encarga de la explotación del sistema de información.

Information System Owner (or Program Manager). Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. CNSS Inst. 4009, Adapted

Riesgo

El riesgo es un indicador de lo que probablemente suceda por causa de las amenazas.

Salvaguardas

Las salvaguardas son medios para luchar contra las amenazas. Pueden tratar aspectos organizativos, técnicos, físicos o relativos a la gestión de personal.

Servicio

Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Sistema de información

Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. ENS.

Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. 44 U.S.C., Sec. 3502; OMB Circular A-130, Appendix III.

Tratamiento de los riesgos

El análisis de riesgos es la fuente de información para el tratamiento del riesgo, donde el riesgo…

- se mitiga hasta unos niveles aceptables: limitando el impacto o reduciendo la probabilidad de que ocurra
- se transfiere a otra organización, proveedor, aseguradora, ...
- se acepta

Trazabilidad (accountability)

Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.

Valor de un activo

El valor de un activo es la estimación del coste que causaría la materialización de una amenaza sobre dicho activo.

ABREVIATURAS

CCN	Centro Criptológico Nacional
ENS	Esquema Nacional de Seguridad
STIC	Seguridad TIC
TIC	Tecnologías de la Información y las Comunicaciones

ANEXO B. REFERENCIAS

CCN-STIC-402

Organización y Gestión para la Seguridad de los Sistemas TIC. Diciembre 2006.

CCN-STIC-801

ENS - Responsables y Funciones. 2010.

Ley 11/2007

Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. BOE de 23 de junio de 2007.

Ley 15/1999

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE de 14 de diciembre de 1999.

RD 1720/2007

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. BOE de 19 de enero de 2008.

RD 3/2010

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. BOE de 29 de enero de 2010.