GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Guía de Seguridad de las TIC
CCN-STIC 472

PILAR Basic – Manual de Usuario v7.1

MAYO 2018

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2018.05.18 10:20:42 +02'00'

NIPO: 785-18-030-9

Fecha de Edición: mayo de 2018
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 la comunicación (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 (CNI), 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 (CCN) 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.

El 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 (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, 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 la comunicación (STIC) 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.

Mayo de 2018

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. CAPÍTULO I - INTRODUCCIÓN

1.1. PRESENTACIÓN

1. Analizar los riesgos es identificar los riesgos potenciales y residuales en un sistema de información y comunicaciones (CIS). Se denomina riesgo a la incertidumbre sobre lo que puede pasar. En este manual nos centraremos en los incidentes que pueden causar un perjuicio en la información y los servicios de la organización.
2. El análisis de riesgos proporciona información para decidir sobre la asignación de recursos, ya sean técnicos o de otro tipo, para proteger organización.
3. El análisis de riesgos requiere un enfoque metódico:
    1. identificar el valor que hay que proteger,
    2. Identificar los elementos del sistema que soportan ese valor; es decir, aquellos donde los ataques pueden causar daño,
    3. establecer medidas de seguridad para protegernos contra los ataques y
    4. estimar indicadores de la posición de riesgo para ayudar a los que tienen que tomar decisiones.
4. PILAR implementa la metodología Magerit: [http://administracionelectronica.gob.es/].

1.2. INSTALACIÓN

1.2.1. ENTORNO JAVA

5. Se necesita un
    - JRE – Entorno de ejecución Java
6. visite [http://java.com] y siga las instrucciones

    paso 1: descargar

    paso 2: instalar

    paso 3: probar

1.2.2. PILAR (WINDOWS)

7. Puede instalar PILAR como administrador o como usuario normal. Los archivos se pueden instalar en cualquier lugar. Si tiene privilegios de administrador, los archivos pueden entrar en "Archivos de programa" para todo el mundo, y el registro puede tener un número de entradas para asociar PILAR a ficheros con extensión .mgr.
8. Cuando Java esté instalado …
    - ejecute `pilarbasic_<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

  `pilarbasic.exe`

  donde haya decidido instalar el software.

1.2.3. PILAR (UNIX)

9. Cuando Java esté instalado…
   - ejecute `pilarbasic_linux_<version>_<perfil>_<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

     `pilarbasic.jar`

     donde haya decidido instalar el software.

1.2.4. PILAR (MAC OS X)

10. Habitualmente, java ya se encuentra instalado en el sistema, pudiendo pasar directamente a la instalación de PILAR:
    - ejecute `pilarbasic_mac_<version>_<perfil>_<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

      `pilarbasic_<versión>.app`

1.3. USO

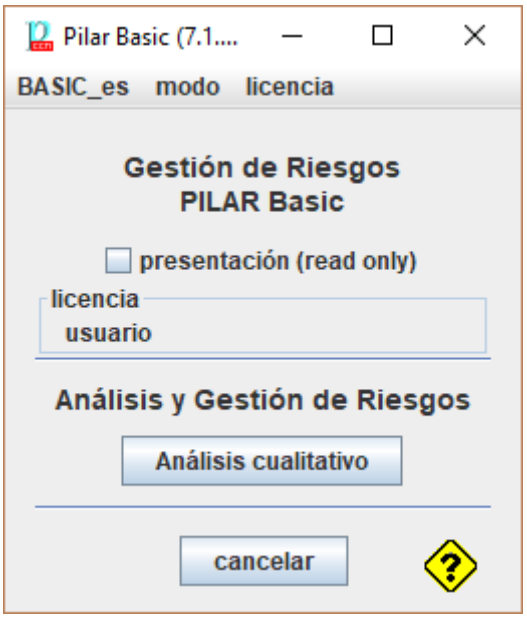
11. Ejecute pilarbasic. Le pedirá un fichero configuración, que puede encontrar en dónde realizó la instalación:

    ej. BASIC_es.car

12. El fichero CAR especifica un directorio para la biblioteca. Puede guardar varias librerías (varios idiomas o varias versiones) en el mismo directorio; pero sólo puede usar una en cada momento.
13. Si necesita más información, busque en “personalización”, en

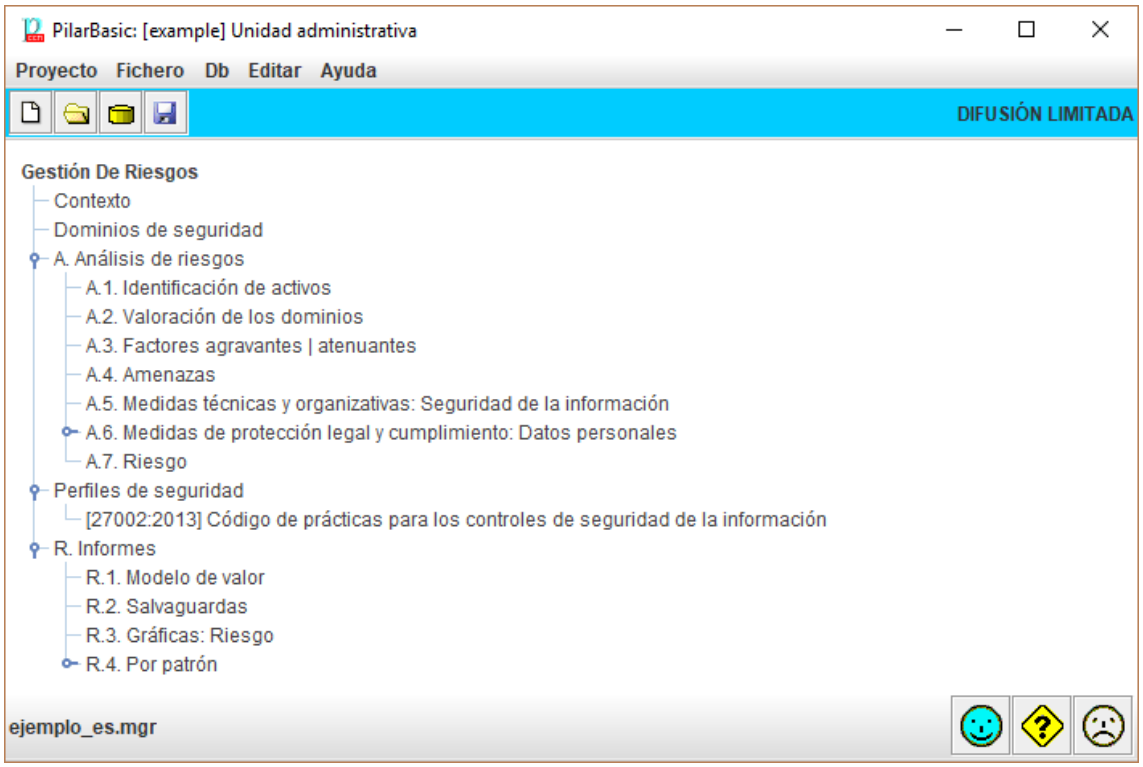
    http://www.pilar-tools.com/en/tools/pilar/doc.html

1.3.1. PRIMERA PANTALLA



- [BASIC_es] haga clic para cambiar el perfil (fichero CAR)
- [licencia] haga clic para cargar su licencia de uso (fichero LIC)

2. CAPÍTULO II - USO BÁSICO



2.1. ACTIVOS ESENCIALES

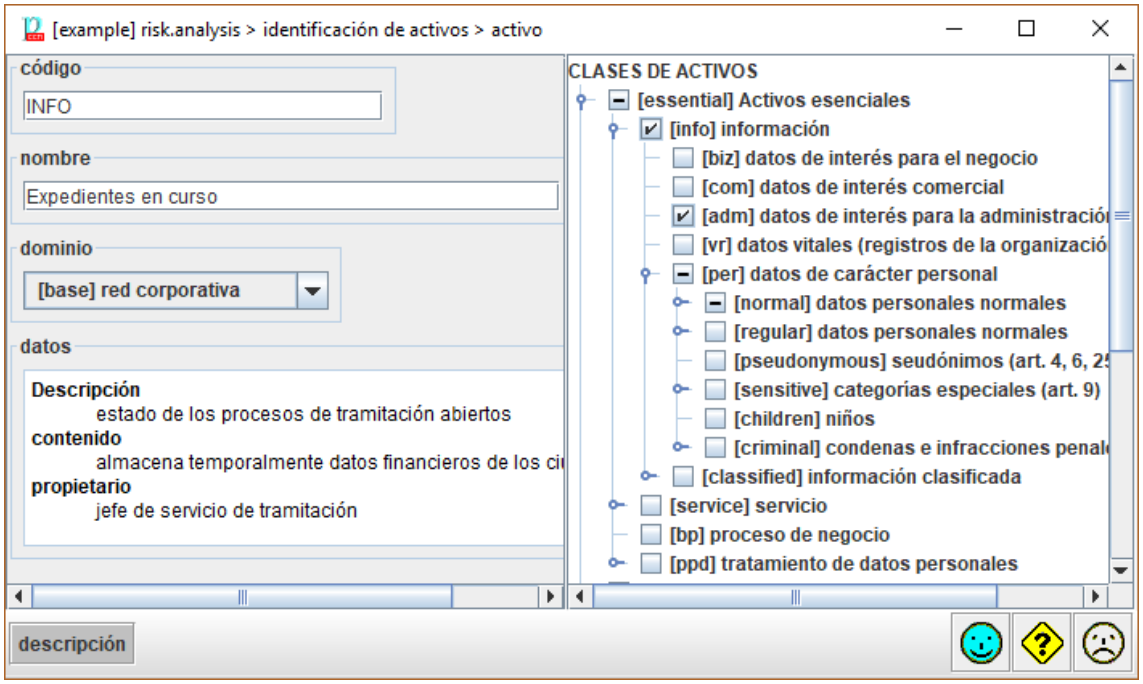
2.1.1. ACTIVOS ESENCIALES

14. Son activos esenciales la información y los servicios manejados por el sistema. Representan los requisitos de seguridad establecidos por sus dueños. Los activos esenciales existen antes de detallar la implementación del sistema de información:
    - Su jefe le dice: “Esta es la información que debemos tratar, y estos los servicios que debemos proporcionar”.
    - “Comprendo. Me hago cargo”, respondemos.
15. Los activos esenciales pueden ser de tipo ‘información’ o de tipo ‘servicio’. O una mezcla de ambos. Lo que es importante es queden identificados por un nombre que se entienda por la organización.
16. Los activos esenciales imponen requisitos de seguridad al sistema. En PILAR hablamos de niveles de seguridad. Los activos de información suelen estar caracterizados por sus requisitos de confidencialidad e integridad. Los activos de servicio suelen estar caracterizados por su disponibilidad. Y unos y otros pueden imponer requisitos de autenticidad y trazabilidad.

2.1.2. IDENTIFICACIÓN Y CARACTERIZACIÓN

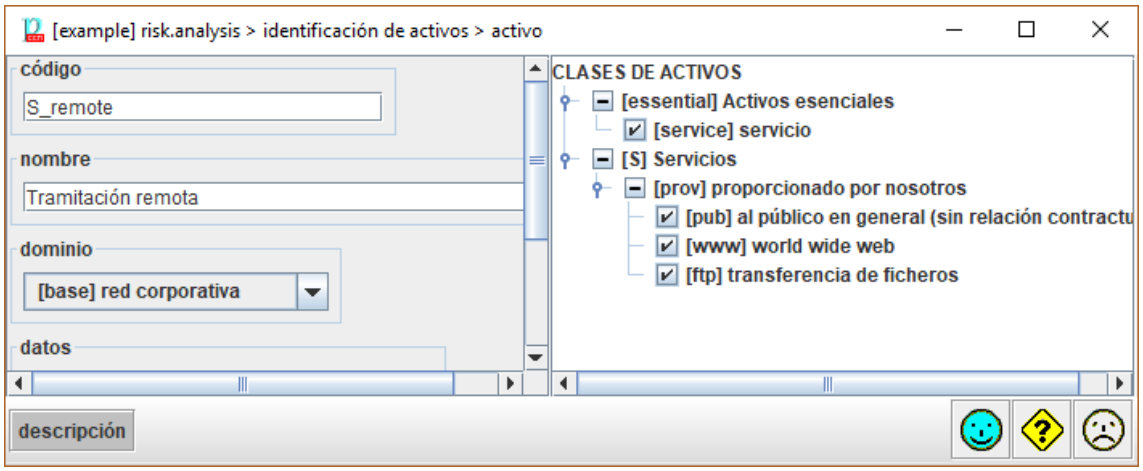
17. Análisis de riesgos > Activos > Identificación
    - Capas > Nueva capa
        - [B] Activos esenciales

- Activos > Nuevo activo
  - [INFO] Información del negocio
  - Seleccione las clases que considere oportunas

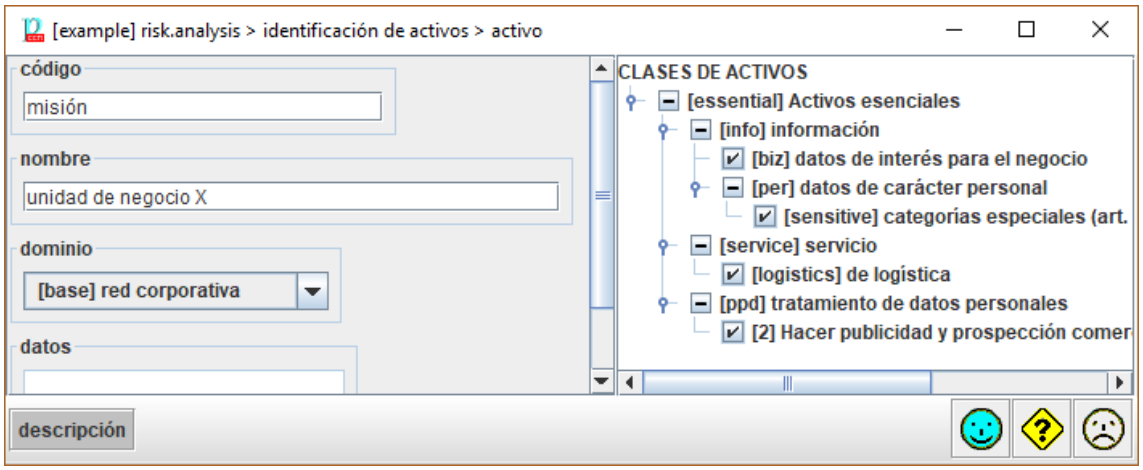


18. Añada los activos de información que necesite para capturar todos los elementos que son relevantes para los directores. Puede usar activos agregados que representen varios activos de información con igual valoración.

19. Luego, añada los servicios que manejan la información:



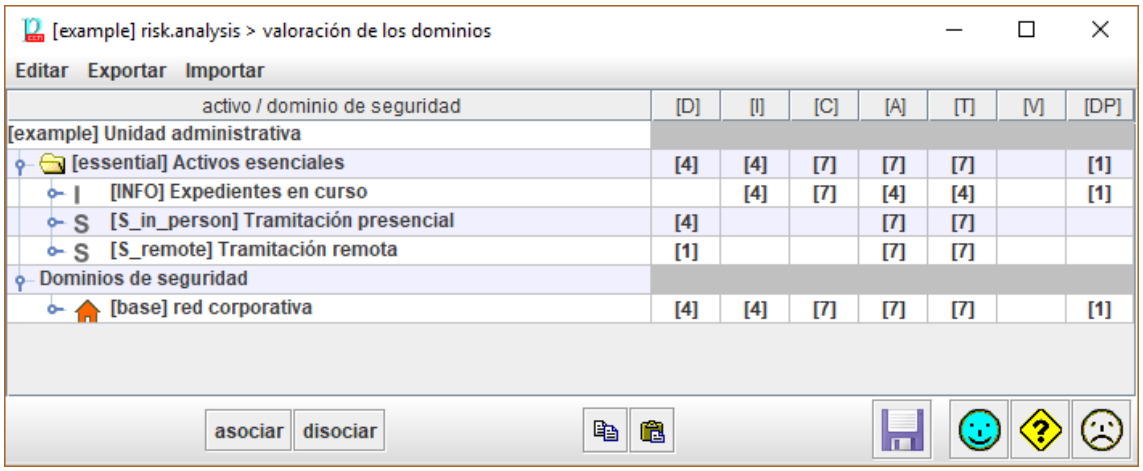
20. Puede ser útil combinar información y servicios en un único activo:



21. Ha terminado cuando tenga suficientes elementos de información y de servicio para hablar con sus directores de los requisitos de seguridad del sistema.

2.1.3. VALORACIÓN

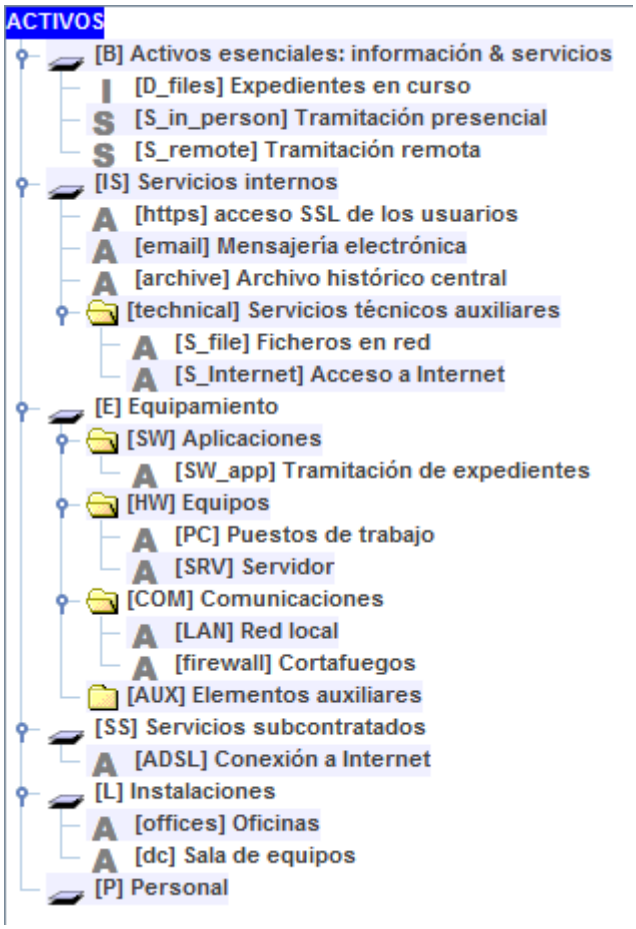
22. Análisis de riesgos > Activos > Valoración de los dominios
23. Para los activos de información, valore el nivel requerido de seguridad:
    - entre 0 (despreciable) y 10 (el máximo)
    - con respecto de la confidencialidad, la integridad, … la autenticidad y la trazabilidad
    - si no especifica ningún nivel, PILAR entenderá que el activo no tiene requisitos significativos en esa dimensión (por ejemplo, no hay requisitos de confidencialidad en la información que es pública)
24. Para los activos de servicio:
    - requisitos de disponibilidad



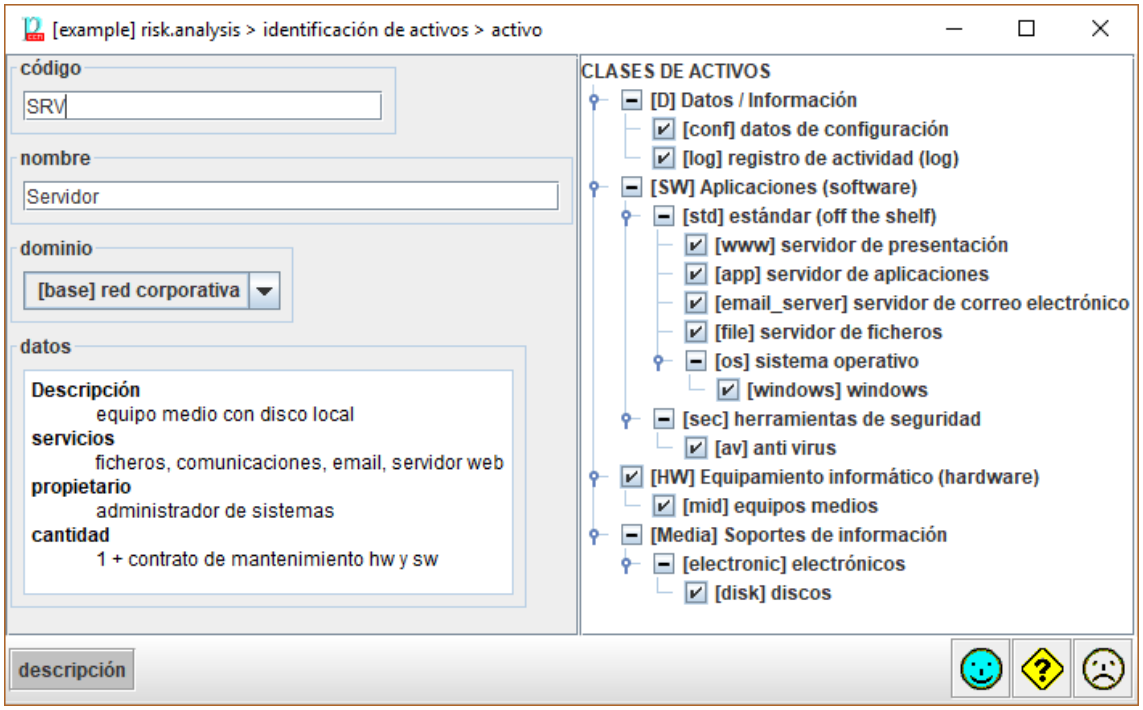
25. De momento, todos los activos están en el mismo dominio de seguridad, el dominio 'base', cuyos requisitos de seguridad son los máximos en cada dimensión de seguridad de los diferentes activos.

2.2. ACTIVOS DE SOPORTE

26. Análisis de riesgos > Activos > Identificación
27. Añada otros activos, materiales o intangibles, que constituyen el sistema de información. Puede organizarlos en capas y grupos por claridad, pero a PILAR solo le interesan los activos en sí.



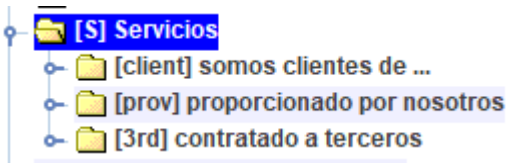
28. Cada activo debe calificarse con las clases que utiliza PILAR para proponer amenazas (oportunidades para los atacantes) y proponer contramedidas (de protección.



29. La granularidad de los activos puede variar desde activos muy detallados, hasta activos que representan un subsistema completo en sí mismos. Tendrá que encontrar un punto de equilibrio entre una descripción lo bastante detallada para conocer los riesgos a los que nos exponemos, y lo bastante compacta para no perdernos en los detalles. Típicamente, un número de activos entre decenas y unos pocos cientos.

2.3. SERVICIOS

30. PILAR contempla una serie de servicios respecto de los cuales el sistema de información objeto de análisis, puede ser consumidor, prestador directo, o tenerlo contratado a una tercera parte.



31. Cada calificativo activa las salvaguardas correspondientes.

32. Los servicios que usamos como clientes o que proporcionamos con nuestro sistema suelen ir asociados a servicios esenciales o a servicios de soporte.

33. Los servicios calificados como contratados a terceras partes se asocian a activos de soporte.

2.4. AUTOMATIZACIÓN

34. PILAR se encarga automáticamente de trasladar los requisitos de seguridad (niveles) de los activos esenciales a los activos de soporte. Puede revisarlos y ajustarlos manualmente si fuera necesario:

35. Análisis de riesgos > Activos > valoración de los activos

36. PILAR aplica un perfil típico de ataque; es decir,
    - identifica amenazas típicas
    - propone valores típicos de probabilidad y consecuencias (estimadas como una fracción del valor transferido desde los activos esenciales).

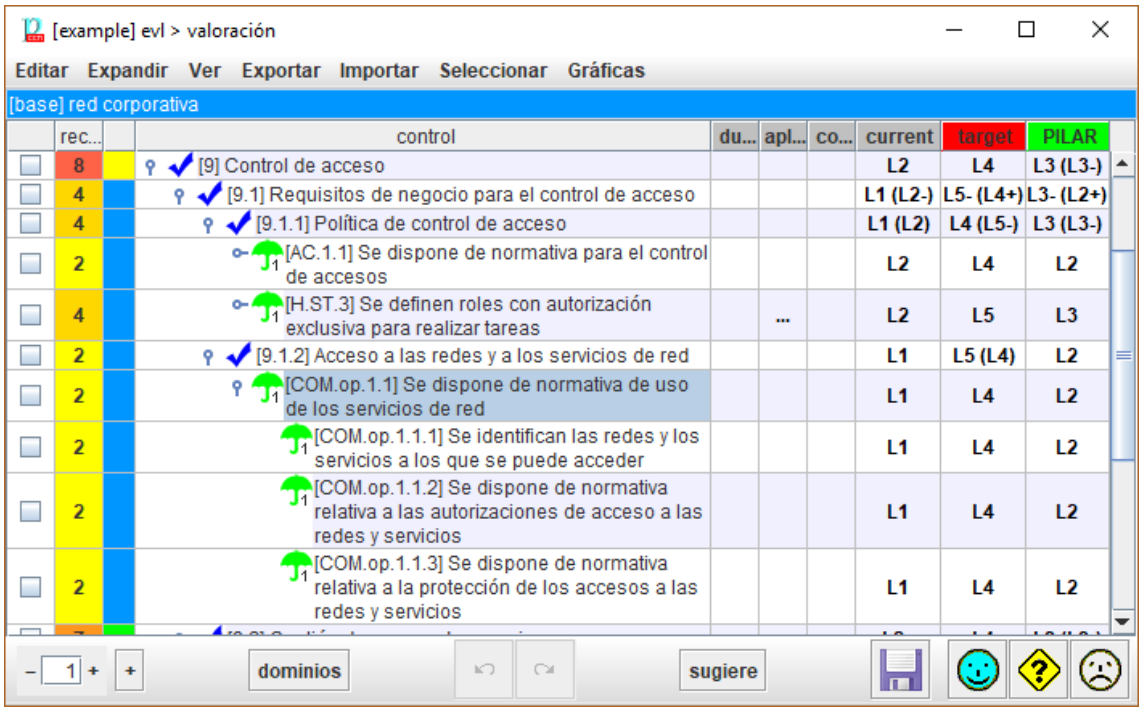
37. En conjunto, PILAR elabora un mapa de riesgos: los riesgos inherentes al sistema (riesgo potencial) que puede consultar
    - desde un punto de vista técnico:
      Análisis de riesgos > Impacto y riesgo > Valores acumulados > …
    - desde el punto de vista del negocio:
      Análisis de riesgos > Impacto y riesgo > Valores repercutidos > …

2.5. PERFILES DE SEGURIDAD

38. Un perfil de seguridad es un conjunto de contramedidas, técnicas y procedimentales. PILAR puede cargar uno o más para ayudar a los usuarios
    - a tratar los riesgos técnicos por medio de contra medidas
    - a cumplir requisitos de acreditación

39. Perfiles de seguridad > 27002:2013 > Valoración

40. Esta pantalla presenta el cumplimiento de un cierto perfil de seguridad, compuesto por controles ( ) que pueden ser refinados o alineados con salvaguardas ( ).



2.5.1. RECOMENDACIÓN

41. Para cada medida de seguridad, la columna [recomendación] presenta una estimación de la importancia relativa de esa fila.
42. Es un valor en el rango [nulo .. 10], estimado por PILAR teniendo en cuenta los activos, las dimensiones de seguridad y el nivel de riesgo que trata la medida.
43. La celda está en gris si PILAR no ve utilidad para la medida: no sabría a qué riesgo aplicarla.

    (o) – overkill – PILAR piensa que la medida es desproporcionada para los riesgos a que se enfrenta el sistema

    (u) – under kill – PILAR piensa que la medida es insuficiente para los riesgos a que se enfrenta el sistema

2.5.2. APLICABILIDAD

44. En la columna [aplica] puede indicar si la fila es aplicable o no. Tenga en cuenta que algunos perfiles marcan algunos controles como obligatorios a efectos de conformidad. PILAR marca estos controles como M. Incluso para los controles que la norma marca como obligatorios, usted puede decidir que en su caso no es aplicable (bien porque el sistema no cumple algún requisito, bien porque dispone de controles compensatorios).
45. Por ejemplo, si carece de servidores (porque usa servicios virtuales en la nube), entonces no hay que proteger ningún equipo. PILAR pone la recomendación en gris.
46. O puede ocurrir que el control sería útil, pero el sistema dispone de mejores medidas de protección.
47. Algunas medidas pueden ser desproporcionadas (overkill), y puede argumentarse que no se justifican. Esto no hace que la medida no sea aplicable. Si decide no implantarla (madurez L0), el riesgo permanece y PILAR lo presenta. Normalmente, una medida que no se justifica va asociada a un riesgo bajo que se acepta tal cual. Cuando un control obligatorio se marca como 'n.a.', PILAR mantiene el color para recordar que es una situación singular.
48. Puede usar la columna [recomendación] como una guía, pero al final será su mejor criterio el que determine qué hacer. Tenga en cuenta que si el sistema va a ser objeto de una acreditación, el inspector requerirá una buena explicación para eliminar una fila. La explicación puede introducirse como un comentario en su columna correspondiente.
49. Cuando selecciona un control y lo marca como 'n.a.', todos los controles 'hijos' quedan marcados como 'n.a.'; pero la no aplicabilidad no se transmite a las salvaguardas bajo el control. Puede ser que haya unas salvaguardas que sí y otras que no bajo el mismo control. Queda de su mano marcarlas manualmente.

2.5.3. VALORACIÓN

control	current	target	PILAR
[9.1] Requisitos de negocio para el control de acceso	L0-L5	L3-L5	L2-L3
[9.1.1] Política de control de acceso	L0-L5	L3-L5	L2-L3
[AC.1.1] Se dispone de normativa para el control de accesos	L0-L5	L3	L2
[H.ST.3] Se definen roles con autorización exclusiva para realizar tareas	L1	L5	L2-L3
[9.1.2] Acceso a las redes y a los servicios de red	L0-L3	L5	L2
[COM.op.1.1] Se dispone de normativa de uso de los servicios de red	L0-L3	L5	L2
[COM.op.1.1.1] Se identifican las redes y los servicios a los que se puede acceder	L3	L5	L2
[COM.op.1.1.2] Se dispone de normativa relativa a las autorizaciones de acceso a las redes y servicios	L0	L5	L2
[COM.op.1.1.3] Se dispone de normativa relativa a la protección de los accesos a las redes y servicios	L0	L5	L2

50. Las columnas presentan fases del proyecto. Sirven para evaluar la madurez de las medidas en varios momentos y poder observar la evolución de la seguridad del sistema. Típicamente, hay 2 fases: la situación actual y adónde nos proponemos llegar. Una última columna, PILAR sirve para que PILAR proponga un objetivo "razonable" o "prudente".

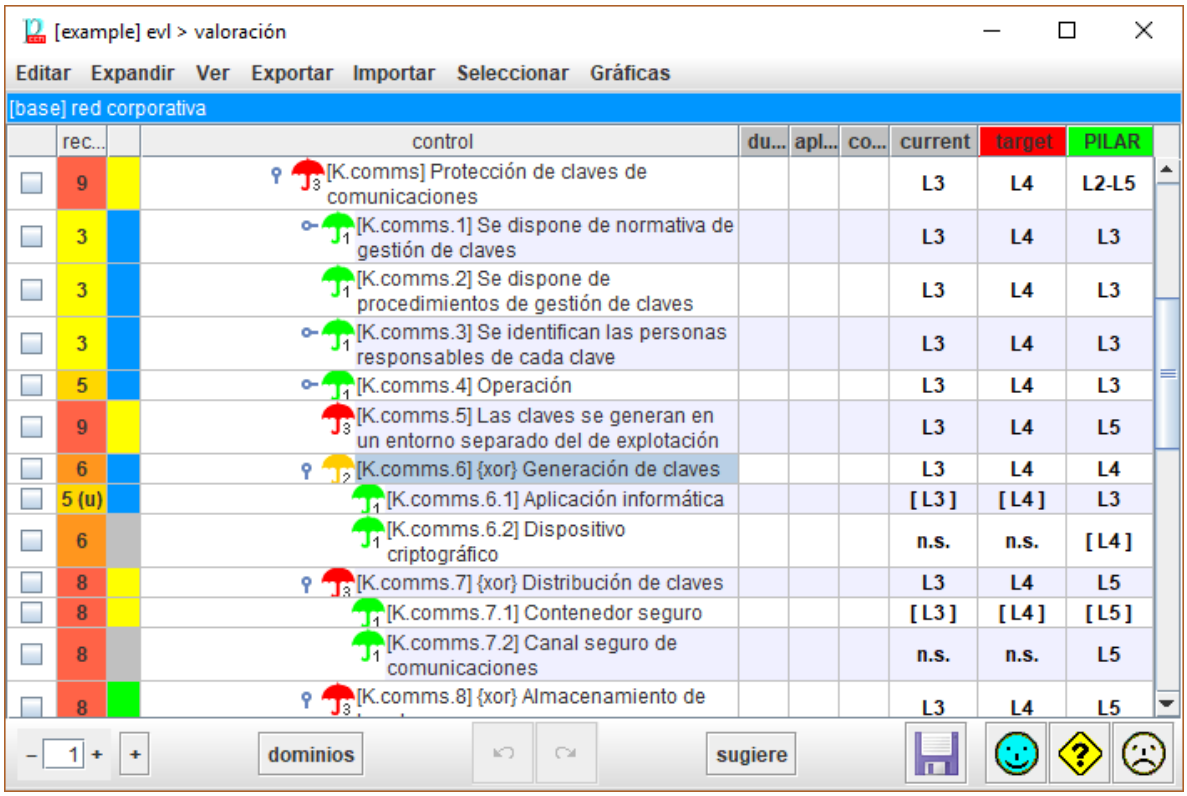
51. La valoración se realiza usando niveles de madurez (ver Anexo A). Para medidas sendillas, tenemos un valor simple de madurez entre L0 y L5. Para medidas compuestas, PILAR muestra el rango (min-max) de la madurez de los componentes. Existe la opción de presentar la madurez del conjunto como una aproximación teniendo en cuenta la madurez 'media' de los componentes.

52. Se espera del usuario que valore la madurez de cada salvaguarda en cada fase. Algunos trucos pueden ayudar a agilizar la tarea:

    - IMPORTAR: si dispone de la valoración realizada en otro análisis de riesgos, puede importarla.
    - SUGERENCIA: empiece con una valoración global, a bulto, de todas las medidas y luego vaya refinando expandiendo el árbol
    - La madurez de una medida en una fase se traslada a las fases siguientes, salvo que se introduzca un valor explícito
    - Si introduce un valor en una fila, éste se propaga a los componentes hijos
    - Los valores de madurez de los hijos se propagan al padre como rango

53. Cuando una medida se marca como XOR, se puede elegir cuál de los componentes optativos se va a utilizar en este sistema. PILAR marca n.s. (no seleccionado) lo que no se usa, valorándose la madurez de la opción en uso.

    clic derecho > seleccionar



Presentación

Puede indicarle a PILAR que presente niveles de madurez (simples, rangos, o una aproximación a la madurez media), o que presente la madurez interpretada como un porcentaje de efectividad, o que compare la madurez presente con la recomendación de PILAR.

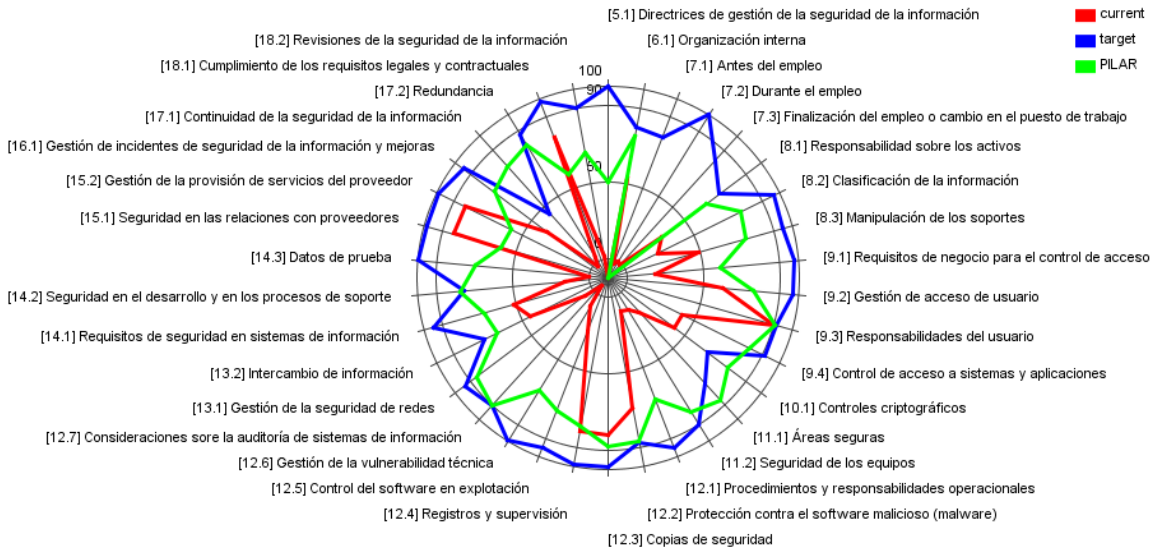
PILAR distingue entre la madurez de las salvaguardas (técnica) y la madurez de los controles (formal), presentado ambos valores simultáneamente si son diferentes.

[5.1] Directrices de gestión de la seguridad de la información				L0 (L1)	L5	L2
[5.1.1] Políticas para la seguridad de la información				L0 (L1)	L5	L2
[G.3.3] Normas de seguridad				L1	L5	L2
[5.1.2] Revisión de las políticas para la seguridad de la información				L0 (L1)	L5	L2
[G.3.3.6] Se revisan regularmente				L1	L5	L2

El valor entre paréntesis es el que se deriva de las salvaguardas inferiores. Usted puede “subir” el valor de las salvaguardas a los controles asociados (botón derecho).

Presentación gráfica

Seleccione en la columna [1] las filas que desea llegar al gráfico:



2.5.4. SEMÁFORO

54. El semáforo [columna 3] resume en un color si la madurez de la medida es suficiente o no.

55. 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

56. 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

2.5.5. DUDAS Y COMENTARIOS

57. En la columna [dudas] puede marcar una medida como que quedan temas pendientes.

58. La columna [comentario] puede albergar un comentario referente a la medida.

2.6. INFORMES

59. PILAR se distribuye con una serie de informes predefinidos. Algunos informes están codificados dentro de la herramienta (textuales y gráficos), mientras que otros vienen regidos por patrones. Los patrones son plantillas RTF que pueden editarse con muchos procesadores de textos.

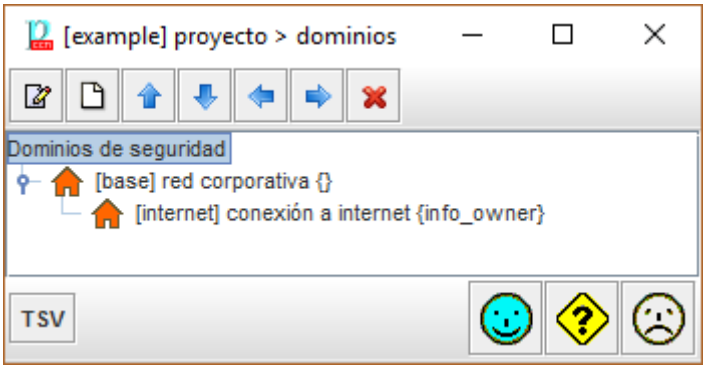
3. CAPÍTULO III - USO MEDIO

3.1. DOMINIOS DE SEGURIDAD

60. Los activos pueden ser distribuidos en dominios de seguridad. un dominio de seguridad define un perfil de ataque y un perfil de protección propios, permitiendo agrupar los activos desde el punto de vista de su exposición y su protección.

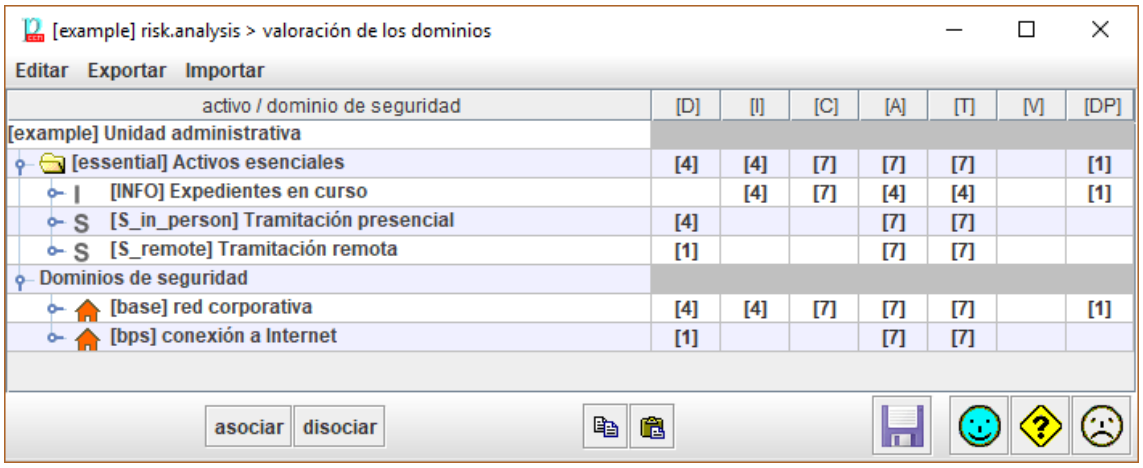
61. Proyecto > Dominios de seguridad

62. Para identificar dominios de seguridad



63. Los dominios de seguridad pueden anidarse unos dentro de otros formando una jerarquía de dominios. Un dominio es 'hijo' de otro. La jerarquía se utiliza para valorar salvaguardas y perfiles de seguridad. El dominio anidado hereda los niveles de madurez del dominio que lo contiene. De esta forma, basta valorar completamente el dominio base y luego ir refinando los cambios en los demás dominios.

64. A fin de valorar los activos, el usuario debe valorar los activos esenciales. PILAR traslada estos valores a todos los activos del dominio en el que está el activo esencial y a todos los dominios asociados a él.



3.2. III.2. SALVAGUARDAS

65. PILAR ofrece un amplio catálogo de medidas de seguridad bajo el nombre de salvaguardas. Las salvaguardas se organizan en forma de árbol, donde las salvaguardas cercanas a la raíz se van refinando en medidas más detalladas según

bajamos por el árbol.

66. Las salvaguardas se seleccionan por dominios de seguridad. Cada dominio puede tener diferentes salvaguardas: de pende de los riesgos sobre sus activos.

67. PILAR calcula un nivel de recomendación (entre 0 y 10) para cada salvaguarda en cada dominio, teniendo en cuenta:

    - las clases de los activos en el dominio
    - El nivel de seguridad requerido, directa o indirectamente, para cada dimensión para cada activo en el dominio
    - la capacidad de cada salvaguarda para proteger cada dimensión
    - la potencia intrínseca de la salvaguarda

68. La columna [aspecto] presenta G para aspectos de gestión, T para aspectos técnicos, F para temas de seguridad física y P para lo referente al personal.

69. La columna [tdp] presenta el tipo de protección que proporciona la salvaguarda

- 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

70. No todas las salvaguardas son igual de importantes:

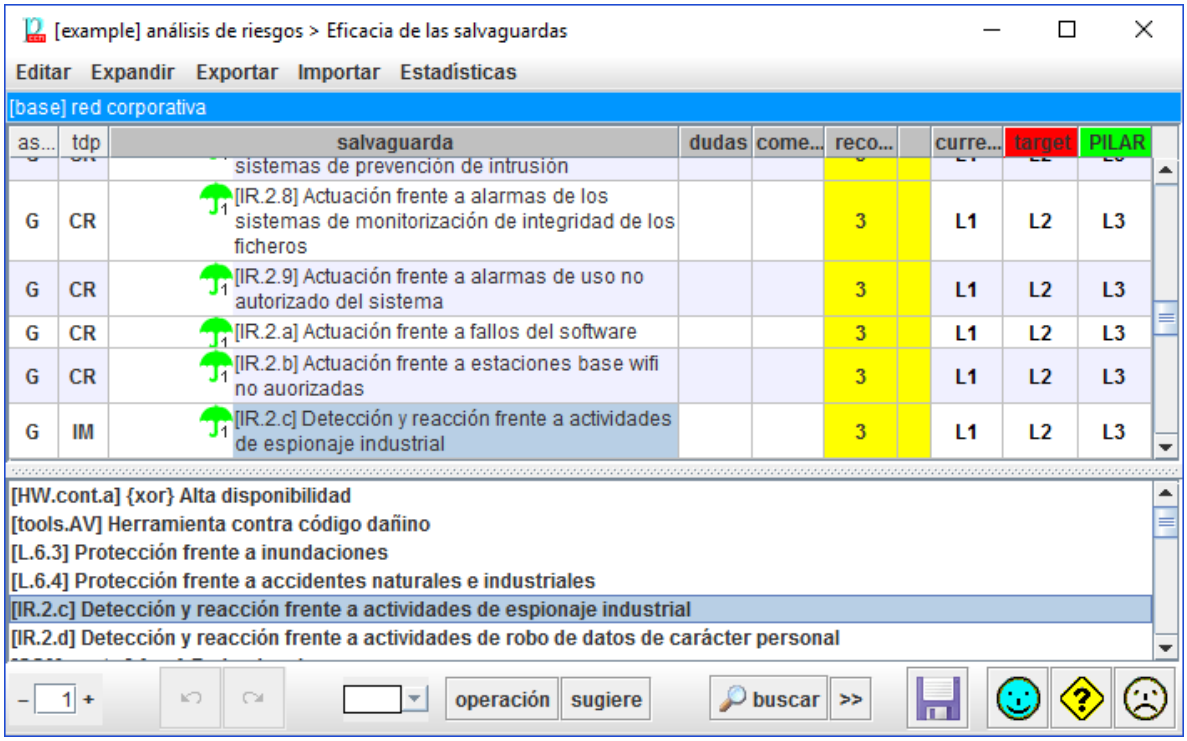
	máximo peso	crítica
	peso alto	muy importante
	peso normal	importante
	peso bajo	interesante
	aseguramiento: componentes certificados	

71. Algunas salvaguardas tienen diferentes formas de implementarse, formas que son alternativas y se etiquetan como XOR. En cada dominio de seguridad solo se aplica una de esas opciones, quedando las demás marcadas como n.s. (no seleccionadas). Se selecciona la que debe usando el botón derecho del ratón

72. La opción seleccionada aparece [entre corchetes]. La selección no se hereda entre dominios: son independientes.

73. A continuación, puede introducir la evaluación de la madurez de cada salvaguarda en cada fase en cada dominio de seguridad. Tenga en cuenta que los valores se heredan en dominios anidados, salvo que se modifiquen manualmente. Y los valores en una fase se mantienen en las fases siguientes, salvo que se modifiquen manualmente.

74. El usuario puede pedir a PILAR que sugiera salvaguardas para un cierto dominio en una cierta fase, teniendo en cuenta las necesidades de seguridad y la fortaleza propia de la salvaguarda.


[example] análisis de riesgos > Eficacia de las salvaguardas
Editar Expandir Exportar Importar Estadísticas
[base] red corporativa
as... tdp salvaguarda dudas come... reco... curre... target PILAR
sistemas de prevención de intrusión
G CR [IR.2.8] Actuación frente a alarmas de los sistemas de monitorización de integridad de los ficheros 3 L1 L2 L3
G CR [IR.2.9] Actuación frente a alarmas de uso no autorizado del sistema 3 L1 L2 L3
G CR [IR.2.a] Actuación frente a fallos del software 3 L1 L2 L3
G CR [IR.2.b] Actuación frente a estaciones base wifi no autorizadas 3 L1 L2 L3
G IM [IR.2.c] Detección y reacción frente a actividades de espionaje industrial 3 L1 L2 L3
[HW.cont.a] {xor} Alta disponibilidad
[tools.AV] Herramienta contra código dañino
[L.6.3] Protección frente a inundaciones
[L.6.4] Protección frente a accidentes naturales e industriales
[IR.2.c] Detección y reacción frente a actividades de espionaje industrial
[IR.2.d] Detección y reacción frente a actividades de robo de datos de carácter personal
1
operación
sugiere
buscar
>>

4. CAPÍTULO IV - USO AVANZADO

4.1. AMENAZAS

75. Por defecto, PILAR aplicar un perfil estándar de amenazas sobre sus activos. Este perfil identifica amenazas sobre cada activo, así como los valores de probabilidad y consecuencias. El perfil está en un fichero externo, bien en formato Excel o en formato xml. Busque TSV en el fichero de configuración CAR.

76. El usuario puede editar el fichero TSV. Incluso puede tener varios ficheros TSV que apliquen en diferentes dominios de seguridad. El uso de ficheros externos es ideal para

    - documentar los cambios
    - analizar el mismo sistema de información en diferentes escenarios de ataque

5. CAPÍTULO V – PERSONALIZACIÓN

77. PILAR puede personalizarse en muchos aspectos modificando ficheros en el directorio que funciona como biblioteca.

78. Aquí vamos a presentar un resumen. Puede encontrar los detalles en la web

    "Personalización" en http://www.pilar-tools.com/doc/v62/

5.1. FICHERO DE CONFIGURACIÓN

79. PILAR se distribuye con una serie de ficheros de configuración estándar. Los ficheros CAR. Por ejemplo

    BASIC_es.car

80. Este fichero es de texto: puede visualizarlo y editarlo y tener su propia versión del mismo.

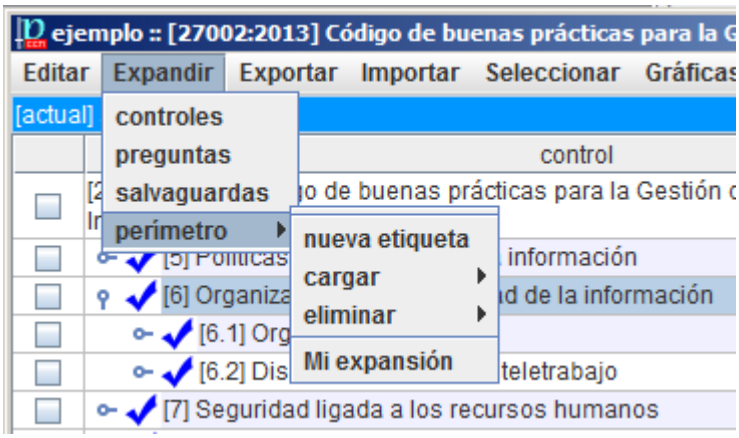
81. Algunos ajustes que se pueden hacer:

- añadir un icono de su organización
- añadir una pantalla de inicio (splash)
- cambiar el carácter de separación de los ficheros CSV
- ajustar las capas estándar y los datos administrativos estándar
- ajustar los niveles de confidencialidad
- añadir nuevos activos y nuevas amenazas
- añadir / modificar los criterios de valoración de activos
- usar otro(s) perfil(es) de ataque (TSV)
- …

5.2. PERÍMETROS

82. PILAR recurre a estructuras arbóreas sistemáticamente para agrupar datos. Dependiendo de las circunstancias, a veces necesitamos desplegar más para ver detalles, o desplegar menos para ver el conjunto. Los perímetros son una forma de decirle a PILAR que un cierto grado de expansión nos interesa, y darle un nombre propio.

83. Algunos perímetros son parte de la librería estándar. El usuario puede añadir los suyos propios.



84. Los pasos a seguir son los siguientes:
    1. Cree una nueva etiqueta con un nombre de su elección

       `Expandir > perímetro > nueva etiqueta`
    2. En el árbol, expanda o contraiga nodos hasta obtener el grado de detalle que le sea útil
    3. Cargue el perímetro en su etiqueta

       `Expandir > perímetro > cargar > su etiqueta`
    4. Para cambiar el perímetro, repita los pasos 2-3
85. Par usar una etiqueta

    `Expandir > perímetro > su etiqueta`
86. Para eliminar una etiqueta

    `Expandir > perímetro > eliminar > su etiqueta`

5.3. PATRONES PARA INFORMES

87. El usuario puede preparar sus propios informes por medio de patrones, que son plantillas escritas en el formato RTF.

    Ver “Patrones” en http://www.pilar-tools.com/doc/v62/
88. Puede establecer los patrones por defecto para sus análisis:

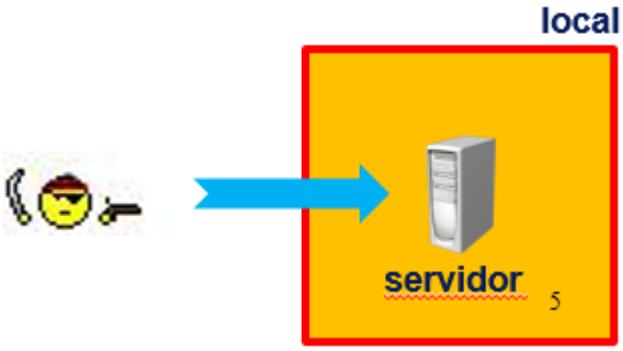
    Ver “Personalización” en http://www.pilar-tools.com/doc/v62/
89. Para organizar su conjunto propio de patrones:
    - edite el patrón (RTF) que necesita usando la documentación de patrones
    - busque en el fichero CAR donde se indica qué patrones se van a usar (normalmente, en el fichero “reports.xml”
    - adapte reports.xml

6. CAPÍTULO VI - TEMAS AVANZADOS

6.1. ZONAS

90. Zonas son conjuntos de activos protegidos por un perímetro. Las zonas se usan en PILAR para reflejar arquitecturas de defensa en profundidad, donde los activos más valiosos están separados de los posibles atacantes.

91. Por ejemplo, el atacante puede estar en el exterior mientras el servidor está en un local:



- tenemos 2 zonas
  - dentro del área
  - fuera del área
- y una frontera, el local

92. El atacante necesita entrar, superando el perímetro de protección física (la protección que aportan paredes, puertas, ventanas, etc.) y luego podría atacar el servidor.

93. PILAR proporciona

- zonas lógicas, separando la red interna del exterior por medio de dispositivos y servicios de frontera (ej. cortafuegos y DMZs)
- zonas físicas, separando áreas internas de áreas externas por medios de sistemas de protección física del perímetro (ej. puertas, ventanas, …)
- zonas tempest, separando las emisiones de cables y equipos de los posibles escuchas externos (ej. jaulas de Faraday)

94. Ver “Zonas” en http://www.pilar-tools.com/doc/v62/

ANEXO A – NIVELES DE MADUREZ

PILAR utiliza niveles de madurez para evaluar salvaguardas y controles según el modelo de madurez (CMM) usado para calificar la madurez de procesos.

L0 - Inexistente

En el nivel L0 de madurez no hay nada.

L1 - Inicial / ad hoc

En el nivel L1 de madurez, las salvaguardas existen, pero no se gestionan. El éxito depende de buena suerte. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta.

El éxito del nivel L1 depende de tener personal de la alta calidad.

L2 - Reproducible pero intuitivo

En el nivel L2 de madurez, la eficacia de las salvaguardas depende de la buena suerte y de la buena voluntad de las personas. Los éxitos son repetibles, pero no hay plan para los incidentes más allá de la reacción heroica.

Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.

L3 - Proceso definido

Se despliegan y se gestionan las salvaguardas. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular de las protecciones. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado).

El éxito es algo más que buena suerte: se merece.

L4 – Gestionado y medible

Usando medidas de campo, la dirección puede controlar empíricamente la eficacia y la efectividad de las salvaguardas. En particular, la dirección puede fijar metas cuantitativas de la calidad. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza es cuantitativa, mientras que en el nivel L3, la confianza era solamente cualitativa.

L5 - Optimizado

El nivel L5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora de los procesos. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.

ANEXO B - GLOSARIO

activo

Algo que tiene un valor, tangible o intangible, que vale la pena proteger, incluyendo personas, información, infraestructuras, aspectos financieros o de reputación. [ISACA, Cybersecurity Fundamentals Glossary, 2014]

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.

En un sistema suele haber información esencial y servicios esenciales que debemos proteger. La información y los servicios esenciales marcan, en última instancia, las necesidades del sistema de información en materia de seguridad.

activos de soporte

Activos que no son esenciales. Estos activos no son una necesidad de la organización, sino un instrumento para implementar la funcionalidad que se necesita. Los activos de soporte son tan valiosos como los activos esenciales que soportan.

amenazas

Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización. [ISO/IEC 27000:2014]

aplicabilidad

Declaración formal en relación a una salvaguardia o un control acerca de su idoneidad para proteger el sistema de información. Una salvaguardia no se aplica cuando no tendría ningún efecto sobre los riesgos del sistema. Un control no se aplica cuando no tendría ningún efecto sobre el cumplimiento de una norma.

declaración de aplicabilidad (SoA)

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

autenticidad

Aseguramiento de la identidad u origen.

confidencialidad

Garantía de que se cumplen las restricciones autorizadas en materia de acceso y divulgación, así como los medios para la protección de la privacidad y la propiedad de la información. [ISACA, Cybersecurity Fundamentals Glossary, 2014]

cumplimiento

Adhesión a los requisitos obligatorios definidos por leyes o reglamentos, así como los requisitos voluntarios que resultan de las obligaciones contractuales y las políticas internas. [ISACA, Cybersecurity Fundamentals Glossary, 2014]

disponibilidad

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

dominios de seguridad

Los activos se ubican dentro de algún dominio de seguridad. Cada activo pertenece a un dominio y sólo a un dominio.

Un dominio de seguridad es una colección de activos uniformemente protegidos, típicamente bajo una única autoridad.

Los dominios de seguridad se utilizan para diferenciar entre unas partes y otras en el sistema de información. Por ejemplo:

- instalaciones centrales, sucursales, comerciales trabajando con portátiles
- servidor central (host), frontal unix, y PCs administrativos
- seguridad física, seguridad lógica
- …

fases

El tratamiento del riesgo se puede afrontar por etapas o fases.

Estas fases son fotografías de la evolución del sistema de protección; mientras que se ponen en ejecución las nuevas salvaguardas, o se mejora su madurez.

impacto

El impacto es un indicador de qué puede suceder cuando ocurren las amenazas.

integridad

Garantía de que datos importantes no se han modificado ni se han eliminado sin autorización o sin que se pueda detectar.

medidas de protección – medidas de seguridad – salvaguardas

Mecanismos para tratar el riesgo, incluyendo políticas, guías, prácticas y estructuras organizativas que pueden ser administrativas, técnicas, de gestión e incluso de tipo legal. [ISACA, Cybersecurity Fundamentals Glossary, 2014]

perfiles de seguridad

Agrupación de salvaguardas en una serie de epígrafes que se convierten en requisitos a satisfacer. [PILAR]

propietario del riesgo – dueño del riesgo

Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo. [ISO Guide 73:2009]

riesgo

Efecto de la incertidumbre sobre la consecución de los objetivos. [ISO Guide 73:2009]

NOTA 1 Un efecto es una desviación, positiva y/o negativa, respecto a lo previsto.

NOTA 2 Los objetivos pueden tener diferentes aspectos (tales como financieros, de salud y seguridad, o ambientales) y se pueden aplicar a diferentes niveles (tales como, nivel estratégico, nivel de un proyecto, de un producto, de un proceso o de una organización completa).

NOTA 3 Con frecuencia, el riesgo se caracteriza por referencia a sucesos potenciales y a sus consecuencias, o a una combinación de ambos.

NOTA 4 Con frecuencia, el riesgo se expresa en términos de combinación de las consecuencias de un suceso (incluyendo los cambios en las circunstancias) y de su probabilidad.

NOTA 5 La incertidumbre es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un suceso, de sus consecuencias o de su probabilidad.

riesgo inherente – riesgo potencial

Nivel de riesgo sin tener en cuenta las acciones tomadas para tratarlo (ej. implementar controles). [ISACA, Cybersecurity Fundamentals Glossary, 2014]

riesgo residual

Riesgo remanente que existe después de que se hayan tomado las medidas de seguridad. [ISACA, Cybersecurity Fundamentals Glossary, 2014]

salvaguardas

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

Una salvaguarda o contramedida es cualquier cosa que ayuda a impedir, contener o reaccionar frente a las amenazas sobre nuestros activos.

trazabilidad

Capacidad para asociar una actividad o sueco a un responsable. [ISACA, Cybersecurity Fundamentals Glossary, 2014]

valoración

Los activos son valorados para establecer sus requisitos de seguridad; es decir, el valor que debe protegerse frente a las consecuencias directas o indirectas de una amenaza ejecutada sobre dicho activo.

zonas

Las zonas se utilizan para determinar la posición del ataque. Un ataque se origina en una zona y puede progresar a otras zonas a través de los elementos de frontera.

Un activo pertenece a una o más zonas, siendo objeto directo de los ataques desde la zona a la que pertenece y objeto indirecto de ataques originados en otra zona, a través de los activos de frontera.

PILAR dispone de zonas lógicas (separadas, por ejemplo, por cortafuegos), de zonas físicas (separadas por defensas físicas perimetrales) y zonas TEMPEST (separadas por barreras anti-emisiones).

ANEXO C - REFERENCIAS

- 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