Master Interuniversitario en Seguridad de las TIC (MISTIC)

Trabajo de Final de Máster

Metodología de Análisis y Gestión de Riesgos de la Seguridad de la Información

Metodología de Análisis y Gestión de Riesgos de SI		
CONTROL DE VERSIONES		
Versión inicial		**Fecha**
V.1.0		**19/03/2019**
Documento elaborado por		
Responsable de actualización		
Versiones Posteriores	**Cambio realizado**	**Fecha**
Estado	**Aprobado por :**	
Etiquetado del documento	**Uso Interno**	

LISTA DE DISTRIBUCIÓN

Este documento ha sido distribuido a los siguientes responsables:

Nombre	Responsabilidad

COPYRIGHT

Tabla de contenido

1. OBJETO Y ALCANCE

Este documento es de aplicación a todos los procesos y activos que forman parte del alcance del SGSI, incluyendo a las personas, los sistemas de información, la información, los edificios y dependencias, y cualquier otro que sea necesario para garantizar la disponibilidad de los servicios esenciales.

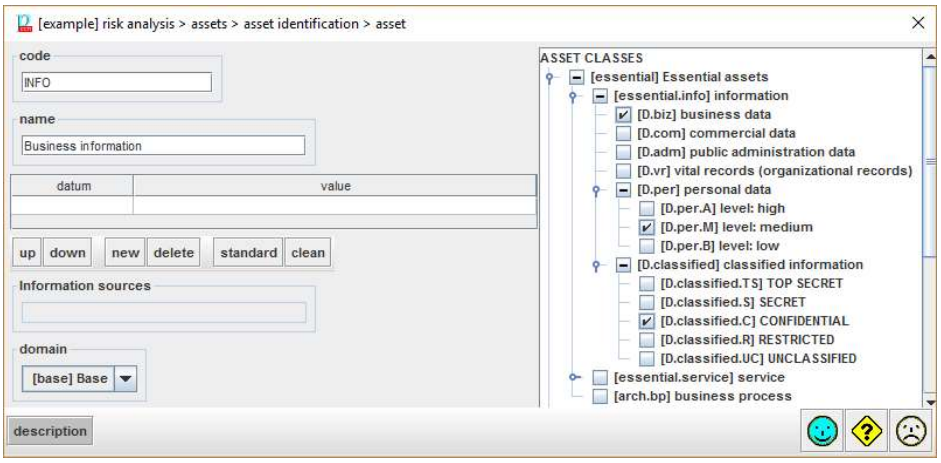
Este proceso estará soportado por la herramienta PILAR/EAR, siguiendo la metodología MAGERIT[1]

2. ACTIVOS

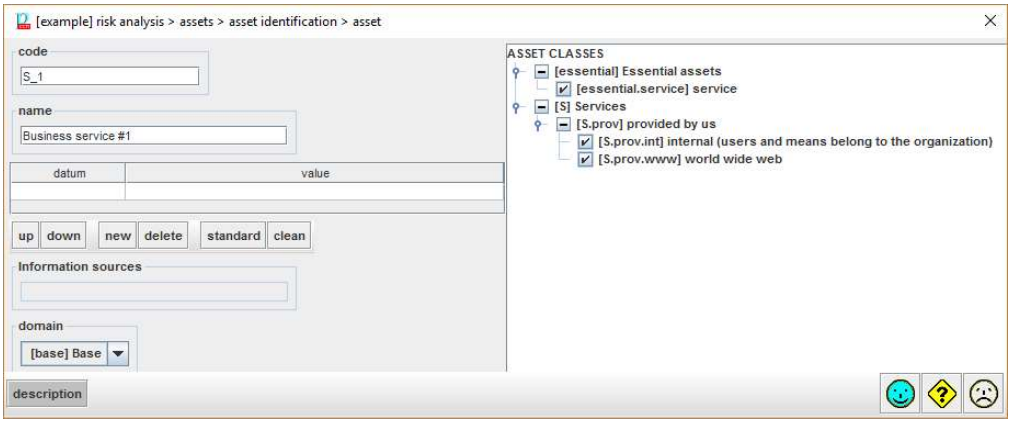
Se incluyen todos los activos que soportan las actividades e información dentro del alcance, que serán valorados diferenciando aquellos que son vitales de los que no lo son.

Los activos esenciales son fundamentalmente de tipo información y servicio, o una combinación de ambos.

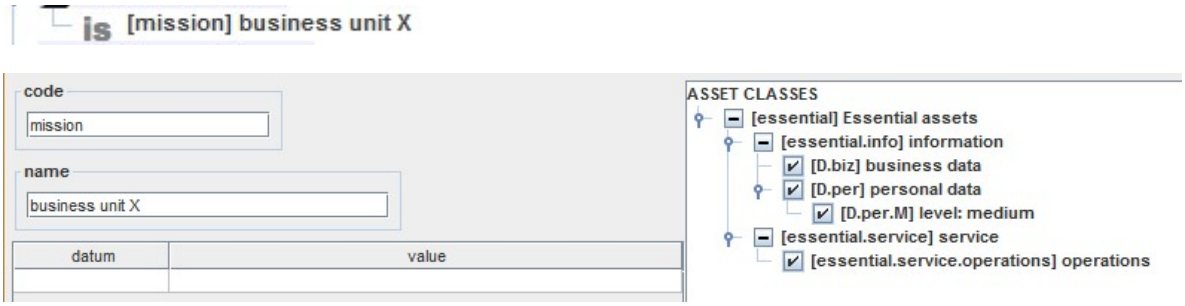
Dichos activos esenciales establecen los requisitos de seguridad, traducidos en los niveles de clasificación de información. Los activos de información los relacionamos típicamente con las dimensiones de seguridad confidencialidad e integridad, y los activos servicio con la dimensión disponibilidad. En el caso de que fueran aplicables, a ambos les aplica las dimensiones de autenticidad y trazabilidad.



[1] Enlace MAGERIT:
http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

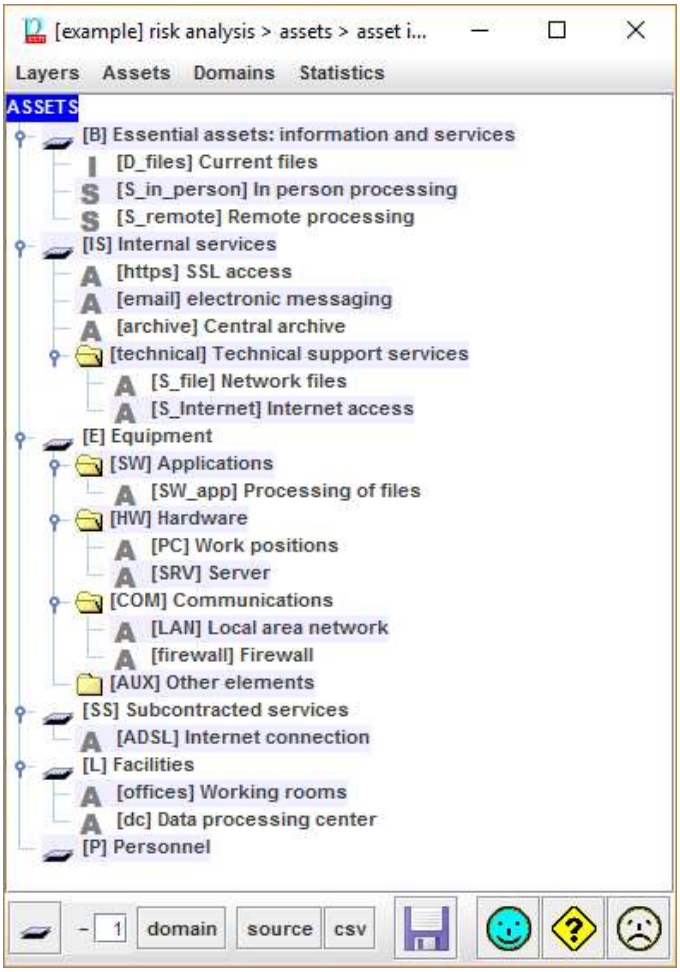


Ejemplo de activo que combina servicios e información en uno sólo.



A continuación, se deben establecer los activos de soporte, que deben ser incluidos en las capas estándar, y pueden ser agrupados según conveniencia para mayor claridad y organización del inventario.

Para ello se contemplan los siguientes tipos de activos:

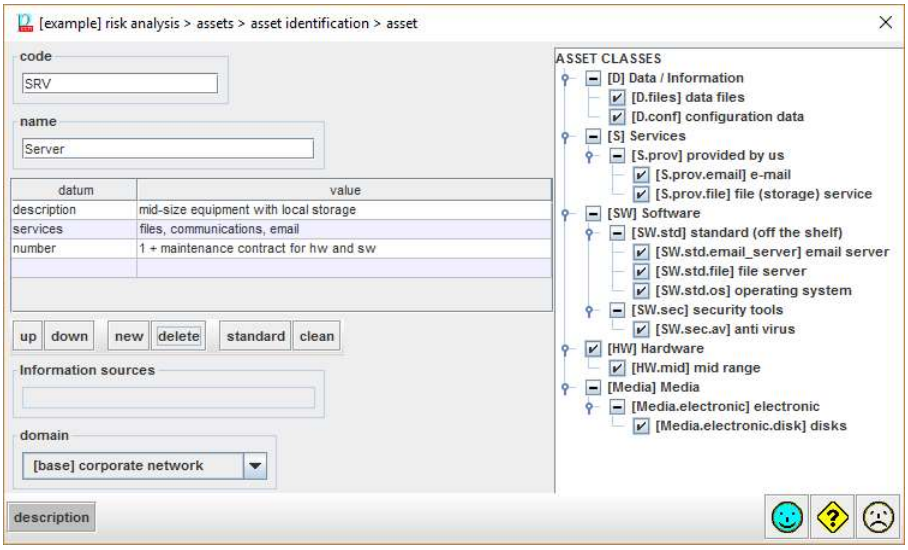


Que a su vez, aparecen detallados en la siguiente tabla:

Activos (Tipos)
▪ **Información y Servicios de Negocio (B)** ▪ **Servicios** – **Internos (SI)** – **Externos (SE)** ▪ **Sistemas de Información** – **Hardware (HW)** – **Software (SW)** ▪ **Comunicaciones (COM)** ▪ **Proveedores (SS)** – **Servicios esenciales** – **IT (Datacenter, otros)** – **Otros** ▪ **Personal (P)** – **Interno** – **Externo** ▪ **Instalaciones y ubicaciones (L)** – **Dependencias** – **Salas técnicas** – **Edificios** – **Otras**

Cada activo se clasifica con las clases que son utilizadas por PILAR para asignar amenazas y proponer contramedidas.

La granularidad se tendrá en cuenta en función del esfuerzo estimado para el estudio de los riesgos. Hay que encontrar un equilibrio entre un nivel suficientemente detallado para saber qué riesgos existen, y una descripción lo suficientemente compacta como para no perderse en los detalles. Típicamente, entre algunas decenas hasta unos pocos cientos.



PILAR se encarga de traducir los requisitos de seguridad (niveles) de los activos esenciales a los de soporte.

PILAR aplica un perfil de ataque estándar; es decir:

- Identifica las amenazas típicas
- Propone valoraciones estándar para la probabilidad y consecuencias (estimado como una fracción del valor de los activos esenciales).

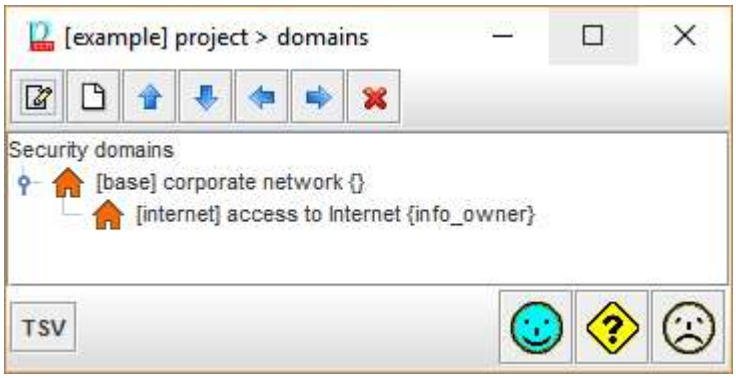
En total, PILAR elabora un mapa de riesgos: los riesgos que son inherentes a su sistema (riesgo potencial) que se puede consultar.

- vista técnico: Análisis de riesgos> Impacto y riesgo> valores acumulados ...>
- vista de negocio: Análisis de riesgos> Impacto y riesgo> valores repercutidos> ...

2.1. Dominios de seguridad

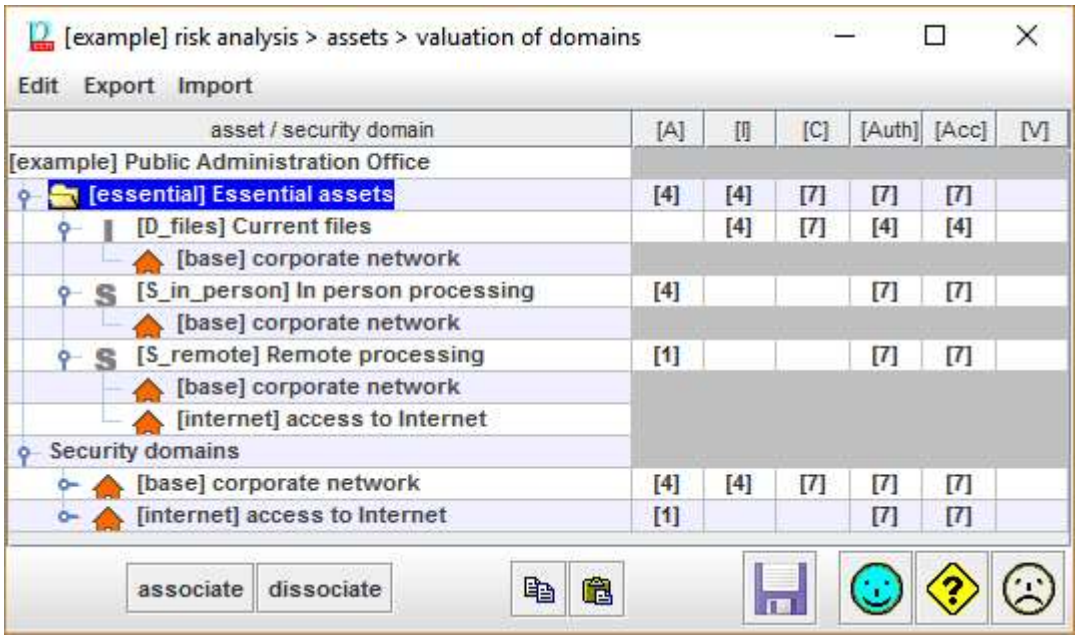
Los activos se distribuirán en dominios de seguridad (base e internet). Otros dominios pueden ser considerados. Cada dominio de seguridad puede tener un perfil de amenaza-ataque distinto y medidas de seguridad específicas.

Proyecto > Dominios de seguridad



Los dominios de seguridad pueden anidarse: un dominio que aparece como un hijo de otro dominio. El anidamiento se utiliza en la evaluación de las salvaguardias y perfiles de seguridad. Los dominios anidados heredan el nivel de madurez del dominio superior, de tal manera que se evalúa el dominio base, y luego se ajusta según sea necesario los dominios anidados.

Con el fin de valorar los activos, se valoran los activos esenciales, y su valor se traduce a todos los activos en el mismo dominio, y también para otros dominios a los que se asocia el activo esencial.



2.2. Dependencias entre activos

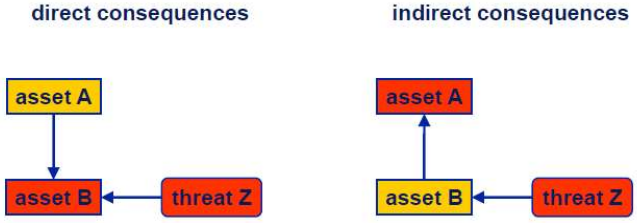
La aplicación de los requisitos de seguridad por dominio de seguridad es una aproximación rápida; pero a veces es demasiado general. Por ejemplo, cuando cada servicio de información se basa sólo en un subconjunto de los equipos en el dominio.

La traducción de grano fino de requisitos se puede conseguir por medio de dependencias entre activos.

Para activarlo, es necesario:

Editar> Opciones> Estimación> activos + dependencias

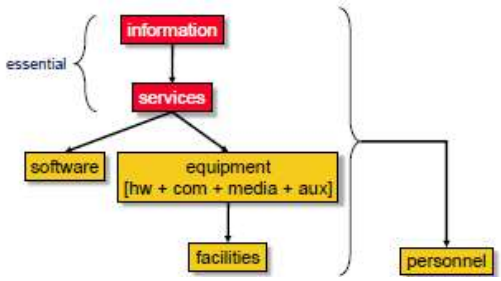
Ahora se puede afirmar que un activo A depende de otro activo B.



- Los requisitos de seguridad (valor) en los niveles de activos A se transfieren sobre activos B.
- Los ataques contra los activos B tienen un efecto directo sobre el valor acumulado en B.
- Los ataques contra los activos B tienen un efecto indirecto (repercutido) sobre el valor de A.

Para establecer las dependencias, se establecen como normas generales:

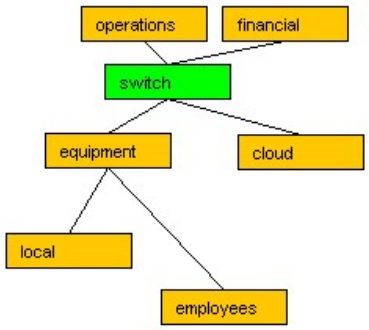
- La información esencial depende de los servicios esenciales.
- Los servicios esenciales dependen del equipo (HW, SW, Comunicaciones y medios de comunicación).
- El equipamiento depende de las instalaciones.
- Todos los activos dependen del personal que puedan perjudicar su CID.



Nodos OR

Algunos activos pueden ser calificados como nodos OR. Esto implica un comportamiento especial durante la transferencia de valor:

- La disponibilidad no se transfiere a los niños de O-nodo, a excepción de los nietos compartidos por todas las ramas del nodo OR.
- Es decir, los nodos OR representan aprovisionamiento alternativo. Cada rama tiene que cumplir los requisitos de seguridad de la información (confidencialidad, integridad, ...), excepto disponibilidad.



Por lo tanto, los activos en una sola rama no heredan los requisitos de disponibilidad, porque hay otra rama. A menos que los puntos comunes de falla; es decir, en los activos que soportan ambas ramas.

2.3. Valoración Activos

Una vez inventariados todos los activos, se realizará una valoración numérica entre el 1-10, valorando cada uno de los siguientes aspectos respecto al activo:

[ ] [lro] Obligaciones legales:
[ ] [si] Seguridad:
[ ] [cei] Intereses Comerciales / Económicos:
[ ] [da] Interrupción del servicio:
[ ] [po] Orden Público:
[ ] [olm] Operaciones:
[ ] [adm] Administración y Gestión:
[ ] [lg] Pérdida de Confianza (Reputación):
[ ] [crm] Persecución de Delitos:
[ ] [rto] Tiempo de Recuperación del Servicio:

Obligaciones Legales:

[ ] [lro] Obligaciones legales:
- [ ] [9.lro] probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
- [ ] [7.lro] probablemente cause un incumplimiento grave de una ley o regulación
- [ ] [5.lro] probablemente sea causa de incumplimiento de una ley o regulación
- [ ] [3.lro] probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
- [ ] [1.lro] pudiera causar el incumplimiento leve o técnico de una ley o regulación

Seguridad:

[ ] [si] Seguridad:
- [ ] [10.si] probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
- [ ] [9.si] probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
- [ ] [7.si] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
- [ ] [3.si] probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
- [ ] [1.si] pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

Intereses Comerciales / Económicos:

- [ ] [cei] Intereses Comerciales / Económicos:
  - [ ] [9.cei] Nivel 9
    - [ ] [a] de enorme interés para la competencia
    - [ ] [b] de muy elevado valor comercial
    - [ ] [c] causa de pérdidas económicas excepcionalmente elevadas
    - [ ] [d] causa de muy significativas ganancias o ventajas para individuos u organizaciones
    - [ ] [e] constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
    - [ ] [f] causa de unos costes excepcionalmente elevados de reemplazamiento
  - [ ] [7.cei] Nivel 7
  - [ ] [5.cei] Nivel 5
  - [ ] [3.cei] Nivel 3
  - [ ] [2.cei] Nivel 2
  - [ ] [1.cei] Nivel 1
    - [ ] [0.3] supondría pérdidas económicas mínimas

Interrupción del servicio:

- [ ] [da] Interrupción del servicio:
  - [ ] [9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
  - [ ] [9.da2] Probablemente tenga un serio impacto en otras organizaciones
  - [ ] [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
  - [ ] [7.da2] Probablemente tenga un gran impacto en otras organizaciones
  - [ ] [5.da] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
  - [ ] [5.da2] Probablemente cause un cierto impacto en otras organizaciones
  - [ ] [3.da] Probablemente cause la interrupción de actividades propias de la Organización
  - [ ] [1.da] Pudiera causar la interrupción de actividades propias de la Organización

Orden público:

- [ ] [po] Orden Público:
  - [ ] [9.po] Alteración seria del orden público
  - [ ] [6.po] Probablemente cause manifestaciones, o presiones significativas
  - [ ] [5.po] Puede causar un significativo malestar público
  - [ ] [4.po] Puede causar malestar público
  - [ ] [3.po] Causa de protestas puntuales
  - [ ] [1.po] Pudiera causar protestas puntuales

Operaciones:

- [ ] [olm] Operaciones:
  - [ ] [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
  - [ ] [9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
  - [ ] [7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
  - [ ] [5.olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
  - [ ] [3.olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
  - [ ] [1.olm] Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)

Administración y Gestión:

- [ ] [adm] Administración y Gestión:
  - [ ] [9.adm] probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
  - [ ] [7.adm] probablemente impediría la operación efectiva de la Organización
  - [ ] [5.adm] probablemente impediría la operación efectiva de más de una parte de la Organización
  - [ ] [3.adm] probablemente impediría la operación efectiva de una parte de la Organización
  - [ ] [1.adm] pudiera impedir la operación efectiva de una parte de la Organización

Pérdida de confianza (reputación):

- [ ] [lg] Pérdida de Confianza (Reputación):
  - [ ] [9.lg] Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones ...
  - [ ] [7.lg] Probablemente causaría una publicidad negativa generalizada
  - [ ] [5.lg] Probablemente sea causa una cierta publicidad negativa
  - [ ] [3.lg] Probablemente afecte negativamente a las relaciones internas de la Organización
  - [ ] [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la Organización
  - [ ] [1.lg] Pudiera causar una pérdida menor de la confianza dentro de la Organización
  - [ ] [0.4] no supondría daño a la reputación o buena imagen de las personas u organizaciones

Persecución de delitos:

- [ ] [crm] Persecución de Delitos:
  - [ ] [8.crm] Impida la investigación de delitos graves o facilite su comisión
  - [ ] [4.crm] Dificulte la investigación o facilite la comisión de delitos

Tiempo de recuperación del servicio:

- [ ] [rto] Tiempo de Recuperación del Servicio:
  - [ ] [7.rto] RTO < 4 horas
  - [ ] [4.rto] 4 horas < RTO < 1 día
  - [ ] [1.rto] 1 día < RTO < 5 días
  - [ ] [0.rto] 5 días < RTO

3. Amenazas

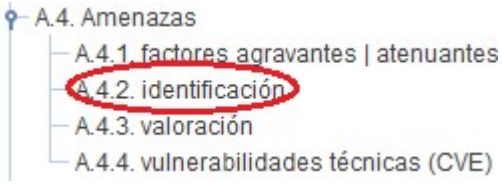
3.1. Identificación

Una vez identificados y valorados los activos que soportan los servicios esenciales de la infraestructura crítica, se deben identificar las amenazas que se evaluaran para cada activo:

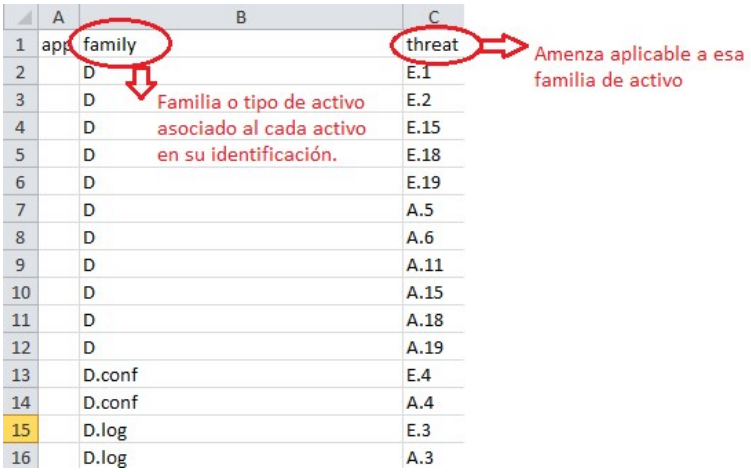
Por defecto, PILAR aplica un perfil de ataque-amenazas que indica qué amenazas pueden afectar potencialmente a los activos, estimando su probabilidad y las consecuencias en caso de materializarse sobre los mismos.

La asociación de amenazas a activos se podrá realizar:

- Manualmente: Para cada familia de activo (tipo) se asocian las amenazas desde:



- De forma automatizada: Para ello, se utilizará un fichero (formato Excel), que contendrá la identificación (y valoración) de cada amenaza para cada familia de activo (tipo). Dicho archivo se encuentra por defecto en la siguiente ruta: C:\<<ruta_instalacion_programa_PILAR_EAR>>\bib_es, y su formato es el siguiente:



	A	B	C
1	app	family	threat
2		D	E.1
3		D	E.2
4		D	E.15
5		D	E.18
6		D	E.19
7		D	A.5
8		D	A.6
9		D	A.11
10		D	A.15
11		D	A.18
12		D	A.19
13		D.conf	E.4
14		D.conf	A.4
15		D.log	E.3
16		D.log	A.3

Se pueden mantener varios de estos ficheros y seleccionar uno para cada dominio.

La configuración se puede cambiar en:

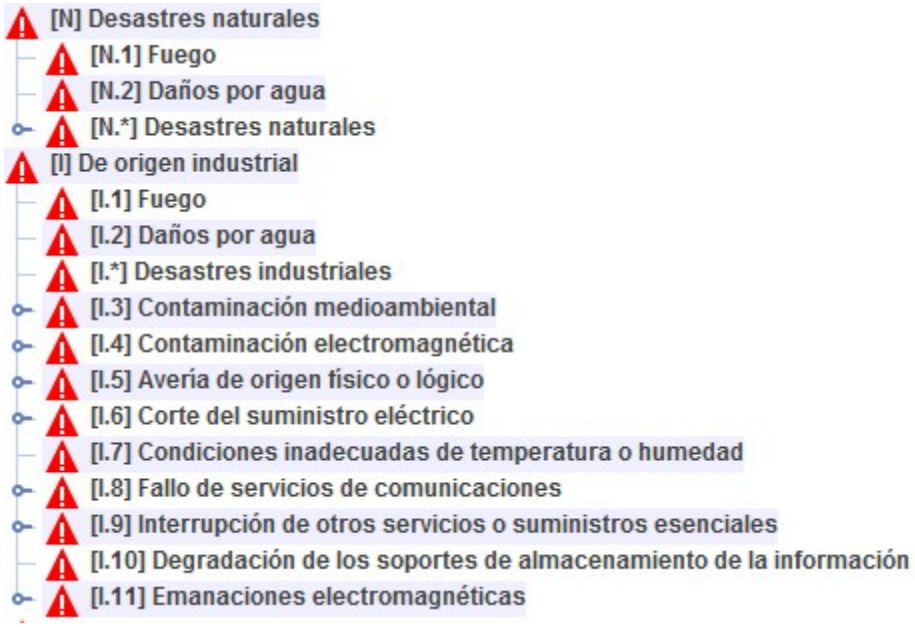
- **Edición > Opciones > Amenazas > Manual | Automático**

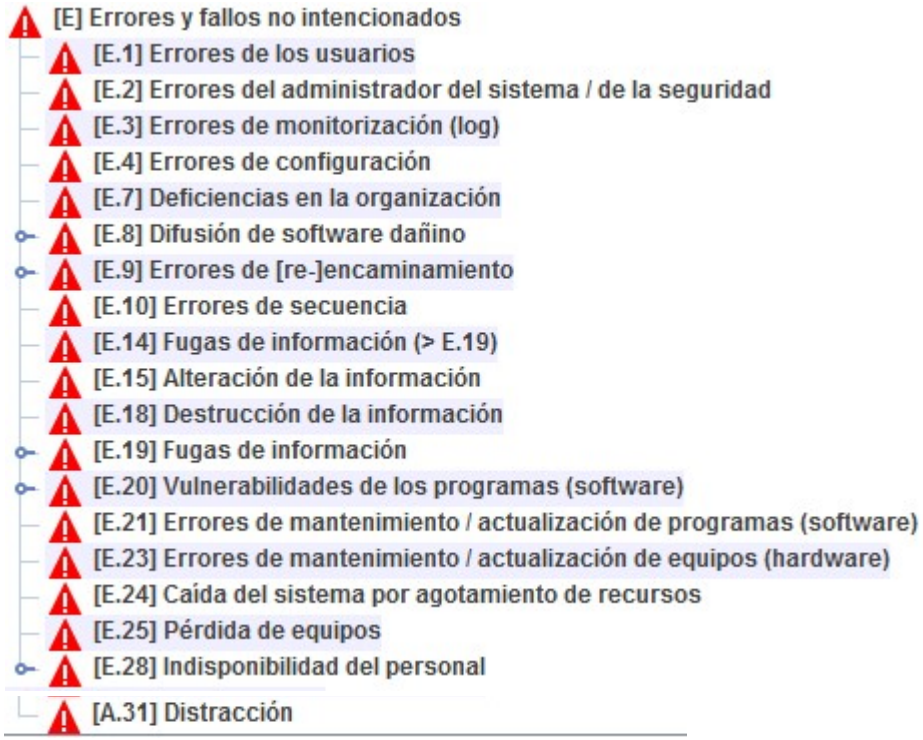
TSV no se utilizará | TSV se utilizará

- **Edición > Opciones > Amenazas > Mixto**

Se puede configurar para que algunos activos sean manuales y TSV aplique al resto

El siguiente listado muestra el catálogo completo de amenazas.





A continuación, se deben asociar las amenazas a cada activo. Para ello se atenderá a la tipología de activo.

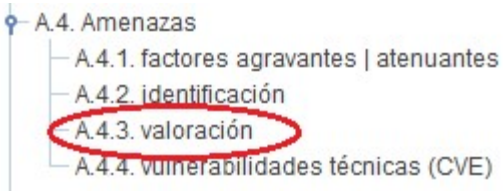
3.2. Valoración

Degradación

Representa cuán perjudicado resultaría el supuesto o activo contemplado al materializarse cada amenaza y se estima por un % que representa la degradación o daño que sufriría el activo, sin tener en cuenta la aplicación de salvaguardas o controles ya aplicados.

La evaluación de amenazas (degradación) se podrá realizar:

- Manualmente: Para cada familia de activo (tipo) se asocian las amenazas desde:



- De forma automatizada: Para ello, se utilizará un fichero (formato Excel), que contendrá la identificación (y valoración) de cada amenaza para cada familia de activo (tipo). Dicho archivo se encuentra por defecto en la siguiente ruta: C:\<<ruta_instalacion_programa_PILAR_EAR>>\bib_es, y su formato es el siguiente:

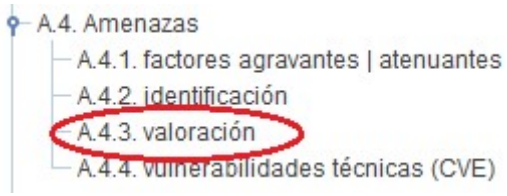
B	C	D	E	F	G	H
family	threat	likely	step	D=en:A	D=en:I	D=en:C
SW	I.5	1	7d	50%		
SW	E.1	1	1h	1%	10%	10%
SW	E.2	1	6h	20%	20%	20%
SW	E.8	1	1d	10%	10%	10%
SW	E.15	1			1%	
SW	E.18	1	1d	50%		
SW	E.19	1				10%
SW	E.20	1	6h	1%	20%	20%
SW	E.21	10	2h	1%	1%	
SW	A.5	1			50%	50%
SW	A.6	1	2h	1%	10%	10%
SW	A.7	1	10m	1%	10%	10%
SW	A.8	1	7d	100%	100%	100%
SW	A.11	1			10%	50%
SW	A.15	1			50%	
SW	A.18	1	2d	50%		
SW	A.19	1				50%
SW	A.22	1	1d	50%	100%	100%
HW	N.1	0,1	15d	100%		
HW	N.2	0,1	7d	50%		

Probabilidad

La probabilidad se modela como una tasa anual de ocurrencia, siendo valores típicos

Probabilidad	Valor	Descripción	Descripción
MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10 (0,1)	poco frecuente	cada varios años
MB	1/100 (0,01)	muy poco frecuente	siglos

- La evaluación de amenazas (probabilidad) se podrá realizar:
  - Manualmente: Para cada familia de activo (tipo) se asocian las amenazas desde:



  - De forma automatizada: Para ello, se utilizará un fichero (formato Excel), que contendrá la identificación (y valoración) de cada amenaza para cada familia de activo (tipo). Dicho archivo se encuentra por defecto en la siguiente ruta: C:\<<ruta_instalacion_programa_PILAR_EAR>>\bib_es, y su formato es el siguiente:

4. Perfil de Seguridad – Compliance ISO/IEC 27002

PILAR mapea los controles (Compliance) con las salvaguardas (riesgo), por lo que la evaluación de madurez de los controles es propagados a las salvaguardas y viceversa.

Para configure la propagación:

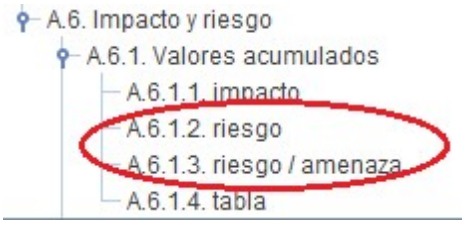
Edición > Opciones > Perfil de Seguridad: propagar > Si | No

current	target	PILAR
L0-L1 (L0-L5)	L1-L4 (L1-L5)	L3-L5 (L2-L5)
L0-L1 (L0-L2)	L2-L4 (L1-L5)	L3-L5 (L2-L5)
L1 (L0-L2)	L2 (L1-L5)	L3 (L2-L3)
L1 (L1-L2)	L2 (L1-L5)	L5 (L2-L5)
L2	L5	L3-L5
L1	L1-L5	L2-L3
L1	L1-L5	L2-L3
L1	L4	L3
L1	L1-L4	L3
n.a.	n.a.	n.a.
L1	L4	L3-L4
L0	L4	L3
L1 (L0-L5)	L1 (L3-L5)	L3 (L2-L3)

Se evaluará el nivel de madurez de los controles de ISO/IEC 27002 para la columna “current”, y una vez finalizado, se revisarán las salvaguardas para evaluar aquellas que hayan quedado sin evaluar y sean aplicables.

La definición de cada nivel de madurez se encuentra en el Anexo A de este procedimiento.

5. Determinación del riesgo

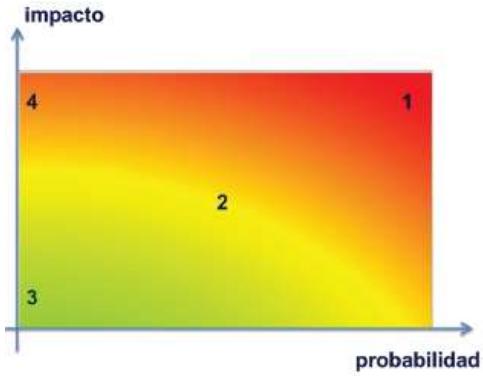


5.1. Riesgo potencial y residual

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas para tener en cuenta en el tratamiento del riesgo (que veremos más adelante):

- zona 1 – riesgos muy probables y de muy alto impacto
- zona 2 – franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo
- zona 3 – riesgos improbables y de bajo impacto
- zona 4 – riesgos improbables, pero de muy alto impacto



5.2. Riesgos No Aceptables

De la totalidad de riesgos potenciales que se hayan identificado, será necesario proceder a la gestión de estos. Dicha gestión consiste en la identificación de las medidas de seguridad que reduzcan los riesgos potenciales. Serán de especial interés los controles en caso de incidentes. Los riesgos resultantes de la aplicación de estas medidas de control determinarán los riesgos residuales a los que está expuesto cada operador.

En este sentido, se indicará la combinación de medidas de seguridad a aplicar para prevenir, detectar o actuar en caso de que se materialice alguna de dichas amenazas.

5.3. Riesgo Aceptable

Sobre los riesgos aceptables se vigilarán las condiciones para mantener el nivel obtenido, actuando a través de los procedimientos operativos correspondientes.

5.4. Propietario del Riesgo

Todo riesgo que afecte a cualquier activo tendrá un propietario que asumirá dicho riesgo, y propondrá las medidas para tratarlo.

Está permitido asignar más de un propietario para un riesgo, para el caso del Comité de Dirección.

Se han establecido los siguientes criterios:

- Riesgos por encima de 3/10. El propietario del riesgo para todos los activos será el Comité de Dirección (Seguridad).
- Riesgos por debajo o igual a 3/10. El propietario del riesgo será el responsable del activo.

NIVEL	RIESGO	CONDICIÓN	TRATAMIENTO	PROPIETARIO	REVISIÓN
>7-10	EXTREMO	NO ACEPTABLE	OBLIGATORIO	COMITÉ DIRECCIÓN	MENSUAL
>3,0-7	SIGNIFICATIVO	NO ACEPTABLE	OBLIGATORIO	COMITÉ DIRECCIÓN	MENSUAL
>2-3,0	APRECIABLE	ACEPTABLE	OPCIONAL	PROPIETARIO DEL RIESGO	TRIMESTRAL
>1-2	BAJO	ACEPTABLE	OPCIONAL	PROPIETARIO DEL RIESGO	ANUAL
0-1	DESPRECIABLE	ACEPTABLE	NO	PROPIETARIO DEL RIESGO	ANUAL

- En cualquier caso, en el PTR se indicará de manera específica quién es el propietario de cada riesgo que requiere tratamiento.
- La decisión del tratamiento o aceptación de los riesgos debe tener en cuenta los siguientes aspectos:
- Requisitos de negocio (cumplimiento de política y normas de seguridad, cumplimiento de estándares del sector, etc.)
- Requisitos del resultado del análisis de riesgos (fallos de seguridad, incidentes y fallos, mal uso, cambios no autorizados, etc.)
- Requisitos legales, reglamentarios y/o contractuales.
- Costes, imposibilidades técnicas si se aplican, etc.

5.5. Establecimiento de acciones

A partir de los resultados de la evaluación de riesgos y del umbral de riesgo definido, el Responsable de Seguridad, junto con el propietario de cada riesgo correspondiente, actuará frente a los riesgos detectados. Esta actuación puede consistir en:

- Reducir el riesgo (disminuir probabilidades y/o impactos,) implantando los controles apropiados.
- Asumir el riesgo. (no se realiza nada).
- Evitar el riesgo. (eliminar el uso del activo involucrado, servicio, proceso o fuente de amenaza).
- Transferir el riesgo a terceros (seguros, proveedores, outsourcing, etc.).

En el primero de los casos, a la hora de seleccionar las acciones organizativas o de gestión, medidas operacionales o procedimentales y medidas de protección o técnicas, el Responsable de Seguridad, junto con el propietario del riesgo, procurarán que haya un equilibrio entre acciones de prevención, detección, reacción y respuesta, y podrá ser consultada cualquier fuente de controles, salvaguardas o mejores prácticas, entre otras:

- ISO/IEC 27002 Guía de buenas prácticas de seguridad de la información.
- Catálogo de salvaguardas de herramienta PILAR/EAR.
- Otras (Compliance con regulaciones, etc.).

5.6. Plan de tratamiento de riesgos (PTR)

Será elaborado el Plan de Tratamiento de Riesgos (**TFM_REG_Acciones**), estableciendo una planificación que recogerá al menos los siguientes elementos:

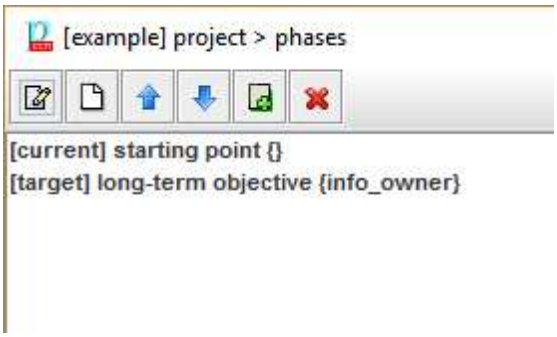
- Identificación de la medida de seguridad: Consistente en un código único y un nombre descriptivo de la medida de seguridad.
- Descripción: Resume los contenidos e implicaciones de la medida de seguridad de manera descriptiva.

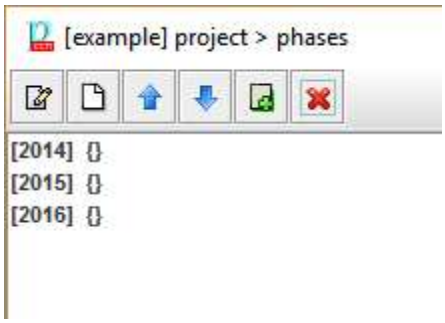
- Responsable: Identifica el departamento o persona al cargo de la ejecución de la medida de seguridad.
- Fechas de inicio y fin previstas.
- Carácter: El carácter distingue entre medida de seguridad permanente o gradual.
- Permanente: Medida de seguridad que se aplica en cualquier circunstancia.
- Gradual: Se activará en función de los distintos niveles de amenaza. Se deberá indicar las circunstancias de activación.
-
- Activos: Activos sobre los que se aplica la medida de seguridad.
- Listado de tareas: Recoge las diferentes tareas unitarias a desarrollar que podrían considerarse necesarias, si bien no suficientes, para la consecución de la medida de seguridad. Así como una descripción de dicha tarea.
- Seguimiento
- Observaciones o comentarios
- Estado:
    - Sin iniciar.
    - En proceso.
    - Parada.
    - Finalizada.

Las acciones de tratamiento serán introducidas en PILAR (Perfil de Seguridad – ISO/IEC 27002; y en Salvaguardas), en función de las fases establecidas en el proyecto.

Proyecto > Fases del proyecto

- Las fases son utilizadas cuando los controles y salvaguardas son evaluados.





6. Revisión del análisis de riesgos

Todos los servicios sujetos a este procedimiento deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año,
- Cuando cambien sustancialmente los servicios prestados o procesos,
- Cuando ocurra un incidente grave de seguridad,
- Cuando se reporten vulnerabilidades graves.

7. Registros y Archivo

Nombre del registro	Código	Responsable del registro	Tipo de archivo	Periodo mínimo
Análisis de Riesgos	PILAR/EAR	Responsable de Seguridad	Electrónico	3 años
TFM_REG_Acciones		Responsable de Seguridad	Electrónico	3 años

8. Anexo A – Niveles de madurez controles/salvaguardas

Los niveles de madurez para evaluar controles y salvaguardas, de acuerdo con Capability Maturity Modelo (CMM).

L0 – Non existent

- At maturity level L0 there is nothing.

L1 – Initial / ad hoc

- At maturity level L1, safeguards exist, but are not managed. Success in these organizations depends on good luck. In this case, organizations frequently exceed the budget and schedule.
- Level L1 success depends on having high quality people.

L2 - Repeatable but intuitive

- At maturity level L2, safeguards effectiveness depends on good luck and good will on the part of the people. Successes are repeatable, but there is no plan for failures beyond heroic reaction.
- There is still a significant risk of exceeding cost and time estimates.

L3 – Defined process

- Safeguards are deployed and managed. There are known policies and procedures to guarantee professional reaction to incidents, and due maintenance of the protection services. The chances to survive are high, up to the limits of the unknown.
- Success is more than good luck: it is deserved.

L4 – Managed and measurable

- Using precise measurements, management can effectively control the effectiveness and efficiency of the safeguards. In particular, management can identify ways to set quantitative quality goals. At maturity level L4, the performance of processes is controlled using statistical and other quantitative techniques, and is quantitatively predictable. At maturity level L3, processes were only qualitatively predictable.

L5 - Optimized

- Maturity level L5 focuses on continually improving process performance through both incremental and innovative technological improvements. Quantitative process-improvement objectives for the organization are established, continually revised to reflect changing business objectives, and used as criteria in managing process improvement. The effects of deployed process improvements are measured and evaluated against the quantitative process-improvement objectives. Both the defined processes and the organization's set of standard processes are targets of measurable improvement activities.
- Process improvements to address common causes of process variation and measurably improve the organization's processes are identified, evaluated, and deployed.
- Optimizing processes that are nimble, adaptable and innovative depends on the participation of an empowered workforce aligned with the business values and objectives of the organization. The organization's ability to rapidly respond to changes and opportunities is enhanced by finding ways to accelerate and share learning.