

PILAR – Continuidad

Manual de Usuario (versión 2024.1)

Marzo, 2024

Contenido

CAPÍTULO I - INTRODUCCIÓN	4
I.1. RESUMEN	4
I.1.1. RTO – TIEMPO OBJETIVO DE RECUPERACIÓN	4
I.1.2. RPO – PUNTO OBJETIVO DE RECUPERACIÓN	5
CAPÍTULO II – USO BÁSICO	7
II.1. OPCIONES DE CONFIGURACIÓN	7
II.2. ACTIVOS ESENCIALES	8
II.2.1. <i>Activos esenciales</i>	8
II.2.2. <i>Identificación y caracterización</i>	8
II.2.3. <i>Valoración</i>	9
II.3. ACTIVOS DE SOPORTE	12
II.4. SERVICIOS	13
II.5. AUTOMATIZACIÓN	14
II.6. MEDIOS DE RESPALDO	14
II.7. MEDIDAS DE SEGURIDAD	16
II.7.1. <i>Recomendación</i>	16
II.7.2. <i>Aplicabilidad</i>	16
II.7.3. <i>Atributos de las salvaguardas</i>	17
II.7.4. <i>Valoración</i>	18
II.7.5. <i>Semáforo</i>	20
II.7.6. <i>Dudas y comentarios</i>	20
II.8. INFORMES	20
CAPÍTULO III – USUARIO MEDIO	21
III.1. DOMINIOS DE SEGURIDAD	21
III.2. FASES DEL PROYECTO	21
CAPÍTULO IV – USO AVANZADO	23
IV.1. DEPENDENCIAS	23
IV.1.1. <i>Nodos OR</i>	24
IV.2. VALORACIÓN ACTIVO A ACTIVO	24
IV.3. AMENAZAS	24
CAPÍTULO V – PERSONALIZACIÓN	25
V.1. FICHERO DE CONFIGURACIÓN	25
V.2. PERÍMETROS	25
V.3. PATRONES PARA INFORMES	26
CAPÍTULO VI – OTROS TEMAS	27
VI.1. DRP – PLAN DE RECUPERACIÓN DE DESASTRES	27
VI.2. ZONAS	28
VI.3. IDIOMAS	28
VI.4. CONTROL DE ACCESO	29
VI.4.1. <i>Contraseñas</i>	30
VI.4.2. <i>Restricciones de acceso: dominios de seguridad</i>	30
VI.4.3. <i>Restricciones de acceso: fases del proyecto</i>	30
VI.4.4. <i>Restricciones de acceso: zonas</i>	31
VI.5. BASES DE DATOS	31
VI.6. MODO BATCH	31
ANEXO A – NIVELES DE MADUREZ	32
ANEXO B - GLOSARIO	33
ANEXO C - REFERENCIAS	36

Capítulo I - Introducción

I.1. Resumen

PILAR identifica y estima el riesgo potencial y el residual en un sistema de información. El riesgo es una medida de los posibles daños sobre la información gestionada por el sistema y los servicios prestados.

El análisis de riesgos proporciona información para tomar decisiones hacer de qué recursos dedicar a proteger el sistema, tanto recursos técnicos como de otra índole.

El análisis de riesgos es una aproximación metódica:

1. se identifica el valor a proteger
2. se identifican los elementos del sistema que soportan ese valor, que es donde el valor puede ser atacado
3. se disponen medidas de seguridad para contrarrestar esos ataques
4. se elaboran indicadores para ayudar a tomar decisiones

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

En este manual nos centraremos en la continuidad de las operaciones; es decir, en cómo los servicios podrían detenerse y en cómo gestionar la interrupción.

I.1.1. RTO – Tiempo objetivo de recuperación

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

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

Este parámetro, a veces tiene letra pequeña:

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

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

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

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

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

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

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

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

PILAR

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

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

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

Para saber si lo hemos alcanzado, en una cierta fase, analizaremos el impacto residual.

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

I.1.2. RPO – Punto objetivo de recuperación

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

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

Este parámetro, a veces tiene letra pequeña:

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

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

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

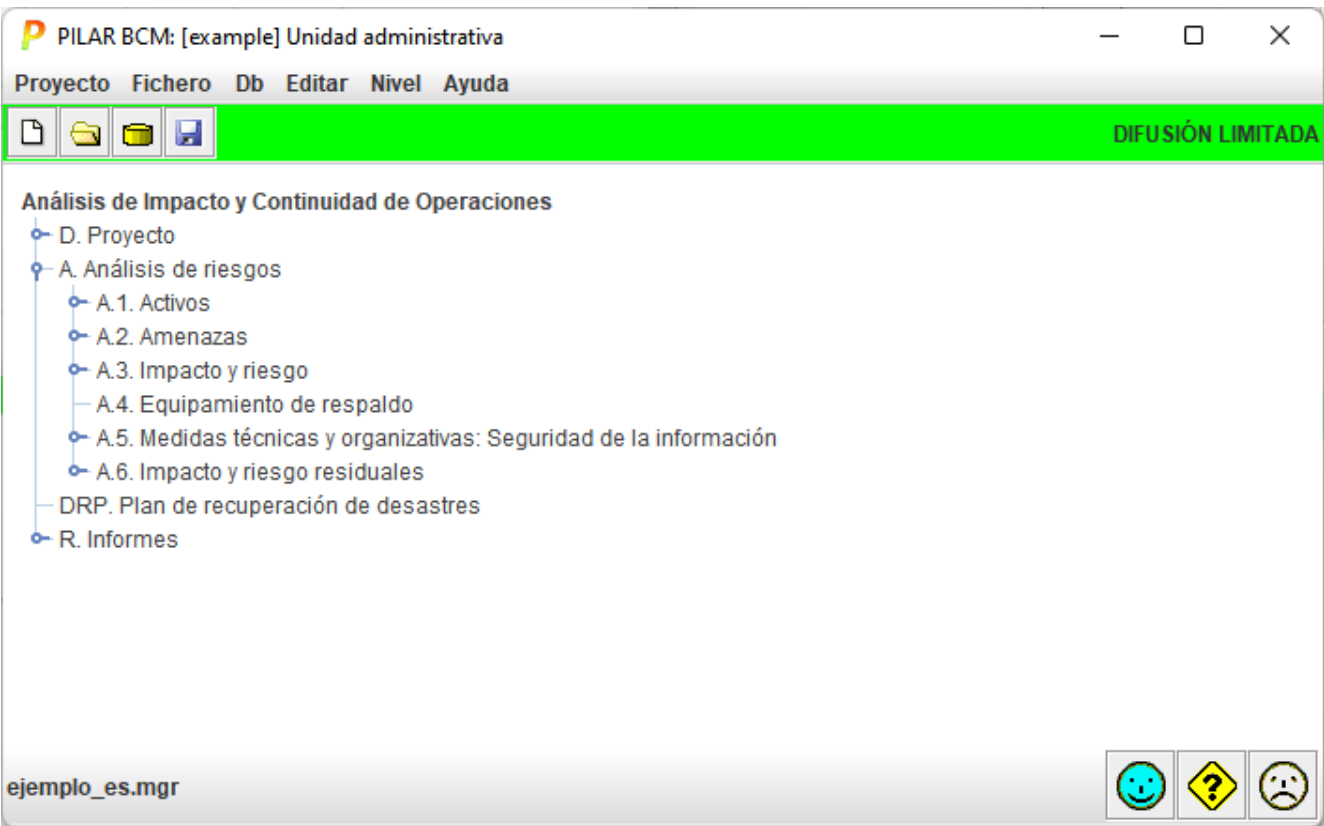
¹ Algunas metodologías recomiendan duplicar este tiempo. El argumento es que los soportes de información pueden estar dañados, obligando a recurrir a copias previas. Para argumentar al respecto, hay que conocer los detalles de cómo se realizan y conservan las copias de seguridad, dependiendo fuertemente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

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

PILAR

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

Capítulo II – Uso básico



II.1. Opciones de configuración

Estas son las opciones más habituales:

Editar > opciones	seleccione	
valoración	activos + dominios	nos limitamos a valorar los activos esenciales; los demás activos se valoran en su dominio seguridad
amenazas	automáticas	PILAR aplica un perfil de ataque estándar
fases de proyecto	enlazadas	la valoración en una fase se propaga a las siguientes, hasta que se modifica
probabilidad	nivel	opcional: afecta a la presentación
efectos	porcentaje	opcional: afecta a la presentación
madurez	madurez	opcional: afecta a la presentación
fases	clic PILAR	PILAR recomienda valores razonables

II.2. Activos esenciales

II.2.1. Activos esenciales

Son activos esenciales la información tratada por el sistema de información y los servicios que éste presta. Desde el punto de vista de negocio. Esta información y estos servicios son anteriores a cómo se materialice luego el sistema por medio de lo que llamaremos activos de soporte.

Los activos esenciales pueden ser del tipo "información" o del tipo "servicio", o incluso una mezcla de ambos. Lo importante es que se identifiquen con un nombre que su organización entienda.

Los activos esenciales imponen requisitos de seguridad, llamados niveles en PILAR. Los activos de información suelen preocuparse por la integridad y la confidencialidad. Los activos de servicio suelen estar relacionados con la disponibilidad. Y unos y otros pueden preocuparse por la autenticidad y la trazabilidad.

II.2.2. Identificación y caracterización

Análisis de riesgos > Activos > Identificación

- Capas > Nueva capa
 - [B] Activos esenciales
- Activos > Nuevo activo
 - [INFO] Información del negocio
 - Seleccione clases como considere apropiado (normalmente, solamente bajo "información esencial"

Siga agregando los activos de información que crea necesarios hasta capturar todos los elementos que son relevantes para la Dirección. Puede utilizar activos agregados que representan varios elementos de información con los mismos requisitos de seguridad.

A continuación, agregue los servicios empresariales que tratan con la información.

[example] análisis de riesgos > activos > identificación de activos > activo

código
S_in_person

nombre
Tramitación presencial

Fuentes de información
info_owner,service_owner

dominio
[base] red corporativa

CLASES DE ACTIVOS

- [essential] Activos esenciales
 - [service] servicio
- [S] Servicios
 - [prov] proporcionado por nosotros
 - [int] interno (usuarios y medios de la propia organiz
 - [ftp] transferencia de ficheros

descripción

También puede usar activos que combinan información y servicio:

[ejemplo] análisis de riesgos > activos > identificación de activos

Capas Activos Dominios Estadísticas

ACTIVOS

- [B] Activos esenciales
 - is [mission] Misión de la unidad #

código
mission

nombre
Misión de la unidad #

dato	valor

CLASES DE ACTIVOS

- [essential] Activos esenciales
 - [info] información
 - [biz] datos de interés para el negocio
 - [per] datos de carácter personal
 - [sensitive] categorías especiales data (art. 9)
 - [7] salud
 - [ppd] tratamiento de datos personales
 - [6] Historial clínico o sanitario

Ha terminado cuando tiene elementos de información y servicio suficientes para hablar de requisitos con la Dirección.

II.2.3. Valoración

Análisis de riesgos > Activos > Valoración de los dominios

Para los activos de información, valore sus niveles de seguridad

- entre 0 (despreciable: no nos preocupa) hasta 10 (máxima preocupación)
- con respecto a la disponibilidad
- si no se valora explícitamente, PILAR lo interpreta como si el valor fuera [0]

Claro que la disponibilidad no se puede caracterizar por un simple nivel: las consecuencias de incidente se agravan según va pasando el tiempo y el servicio sigue interrumpido:

[example] análisis de riesgos > activos > valoración de los dominios								
Editar Exportar Importar								
activo / dominio de seguridad	[10m]	[30m]	[1h]	[3h]	[8h]	[1d]	[2d]	[7d]
[example] Unidad administrativa								
📁 [essential] Activos esenciales		[3]		[3]		[5]	[5]	[7]
📁 [INFO] Expedientes en curso						[4]		
📄 [S_in_person] Tramitación presencial		[3]				[4]	[5]	[7]
📄 [S_remote] Tramitación remota				[3]		[5]		
Dominios de seguridad								
🏠 [base] red corporativa		[3]		[3]		[5]	[5]	[7]
🏠 [internet] conexión a internet				[3]		[5]		
asociar disociar 📄 📁 💾 😊 ⚠️ 😞								

La escala de valoración es parametrizable. PILAR, por defecto, usa una de estas escalas:

[example] proyecto > escalones de interrupción

☒ [1d, 2d, 3d, 4d, 5d, 6d, 7d, 8d, 9d, 10d]
 ☐ [10m, 30m, 1h, 3h, 8h, 1d, 2d, 7d, 10d, 14d]
 ☐ [15s, 1m, 30m, 1h, 6h, 12h, 24h, 2d, 7d, 30d]

OK cancelar

Típicamente:

- se usa la escala lineal cuando los escenarios de recuperación consisten en sedes alternativas, donde la reanudación del servicio requiere días
- use la escala exponencial en escenarios interactivos, donde los usuarios se van enfadando según se prolonga la interrupción (coste reputacional)

Para cada escalón temporal, estime las consecuencias

- merma de beneficios, pérdida de oportunidades
- daño a la imagen (reputación) + gestos necesarios para recuperar la imagen
- multas (ej. incumplimiento de SLAs)
- costes extra (ej. horas extra para recuperar las jornadas perdidas)

Analicemos un ejemplo como el presentado anteriormente:

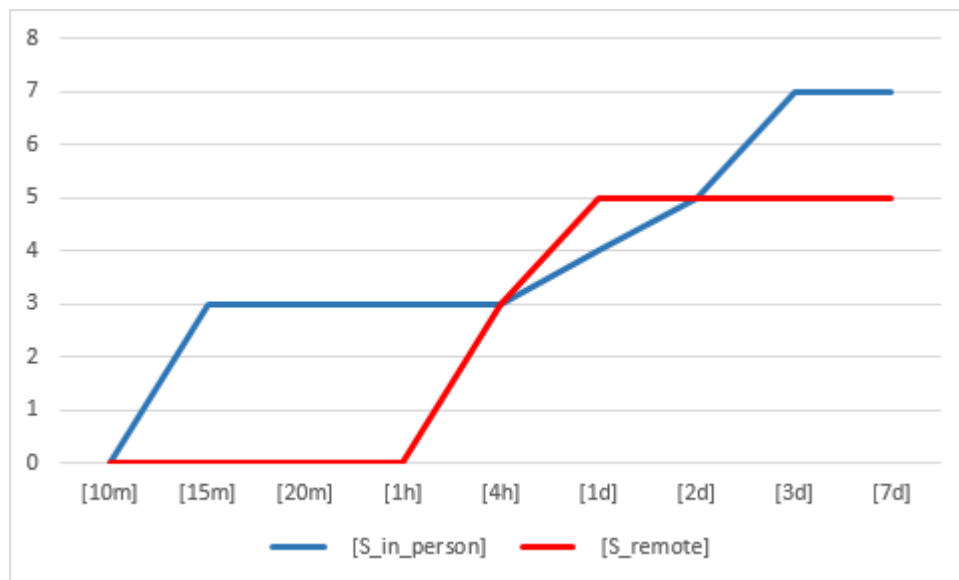
activo / dominio de seguridad	[10m]	[30m]	[1h]	[3h]	[8h]	[1d]	[2d]	[7d]
[example] Unidad administrativa								
📁 [essential] Activos esenciales		[3]		[3]		[5]	[5]	[7]
📁 [INFO] Expedientes en curso						[4]		
📄 [S_in_person] Tramitación presencial		[3]				[4]	[5]	[7]
📄 [S_remote] Tramitación remota				[3]		[5]		

- Para [INFO] tenemos 3 saltos: 15 minutos, 1 hora y 2 días

- si establecemos el RPO por debajo de 15m, las consecuencias de una interrupción del servicio son irrelevantes
- si establecemos el RPO por debajo de 1h, las consecuencia son de grado [3]
- si ese objetivo nos supone un desembolso imposible, podemos tomar un riesgo superior; el siguiente escalón está en 2d; o incluso podemos ir a soluciones menos costosas a base de asumir un mayor riesgo
- La decisión no es técnica, pero debe basarse en datos técnicos
- Para los servicios. Para [S_in_person], las opciones son
 - un RTO por debajo de 1h, con un impacto irrelevante
 - un RTO por debajo de 1d, con un impacto máximo de grado [3]
 - o alguna solución más barata ...

Y siempre está la opción de proporcionar un plan conjunto para todos los servicios:

- RTO < 15m; sin consecuencias dignas de mención
- RTO < 4h; consecuencias hasta grado [3]
- RTO < 2d; consecuencias hasta grado [5]
- RTO < 3d; consecuencias hasta grado [7]



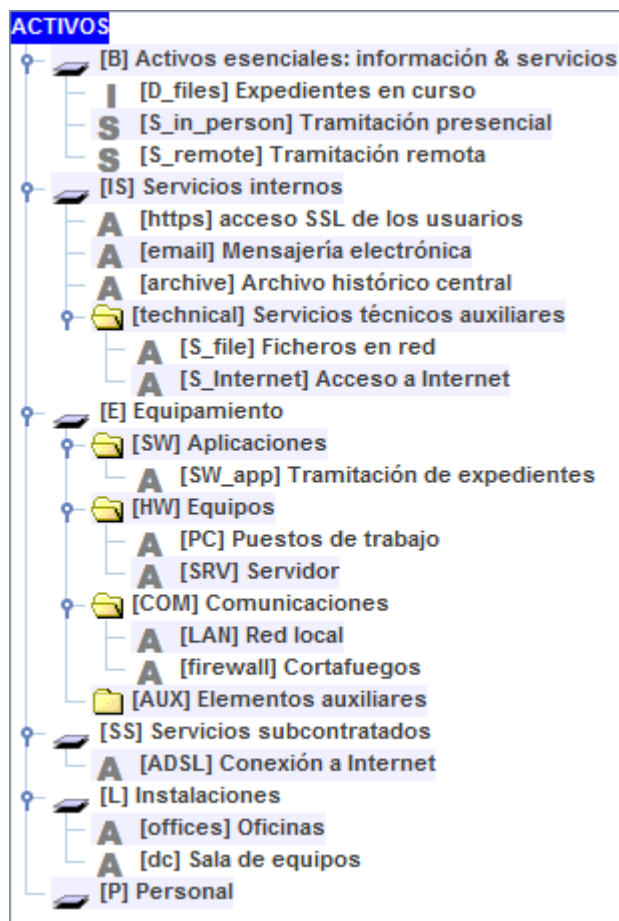
La decisión no es técnica, pero debe conjugar las opciones técnicas y los recursos disponibles.

De momento, todos los activos están en el mismo dominio de seguridad.

II.3. Activos de soporte

Análisis de riesgos > Activos > Identificación

Siga añadiendo activos, tangibles o intangibles, que van formando el sistema de información. Puede organizarlos en capas o en grupos por claridad. A PILAR solo le interesa saber qué activos hay.

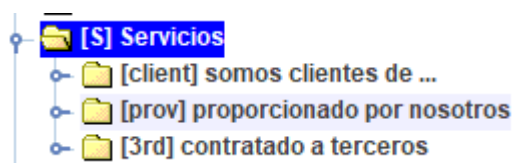


Cada activo está calificado por una serie de clases. PILAR utiliza esta calificación para proponer posibles amenazas y para proponer medidas de seguridad.

La granularidad de los activos puede ir desde activos muy concretos, singularizados, hasta activos tan grandes como todo un subsistema. Hay que llegar a un cierto equilibrio entre tener suficiente nivel de detalle para saber a qué riesgos estamos expuestos, y una descripción compacta que evite que nos perdamos en el detalle. Típicamente, es razonable un modelo entre unas decenas y unos pocos cientos de activos.

II.4. Servicios

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.



Cada calificación activa las salvaguardas correspondientes.

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

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

II.5. Automatización

PILAR se hace cargo de trasladar los requisitos de seguridad de los activos esenciales a los activos de soporte. Puede ver el resultado de este traslado y refinarlo manualmente.

Análisis de riesgos > Activos > Valoración de los activos

PILAR aplica un perfil de atacante típico; es decir

- identifica amenazas típicas
- propone una valoración estándar de la probabilidad de ocurrencia y de las consecuencias (estimada como una fracción del valor trasladado desde los activos esenciales)

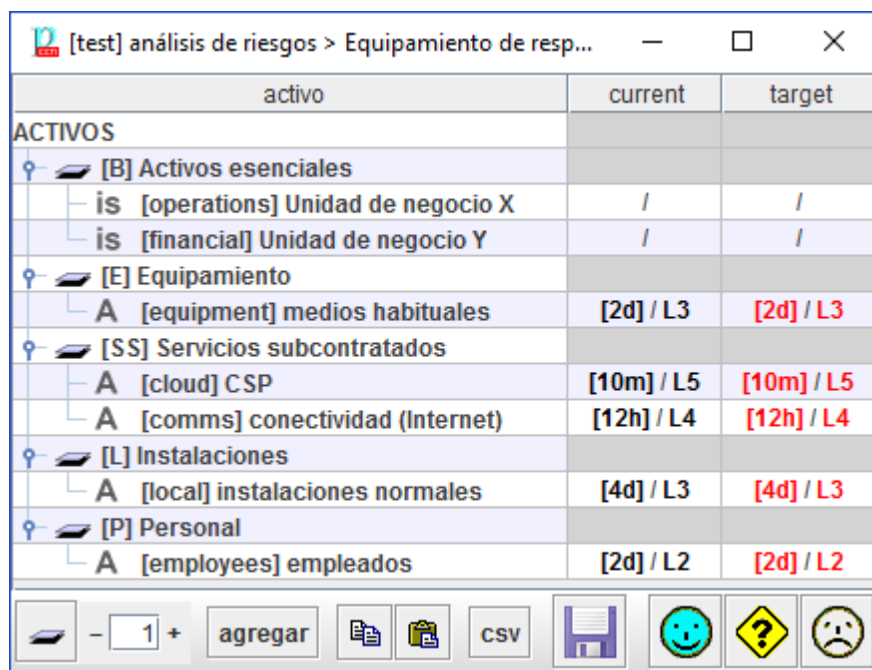
En conjunto, PILAR elabora un “mapa de riesgos” típico: los riesgos inherentes a su sistema (riesgo potencial). Puede consultarlo

- visión técnica: Análisis de riesgos > Impacto & riesgo > Valores acumulados > ...
- visión de negocio: Análisis de riesgos > Impacto & riesgo > Valores repercutidos > ...

II.6. Medios de respaldo

Un componente básico de protección de la continuidad es la existencia de recursos alternativos que entran en funcionamiento cuando los elementos rutinarios no están disponibles.

Veamos un ejemplo:



activo	current	target
ACTIVOS		
♀ [B] Activos esenciales		
is [operations] Unidad de negocio X	/	/
is [financial] Unidad de negocio Y	/	/
♀ [E] Equipamiento		
A [equipment] medios habituales	[2d] / L3	[2d] / L3
♀ [SS] Servicios subcontratados		
A [cloud] CSP	[10m] / L5	[10m] / L5
A [comms] conectividad (Internet)	[12h] / L4	[12h] / L4
♀ [L] Instalaciones		
A [local] instalaciones normales	[4d] / L3	[4d] / L3
♀ [P] Personal		
A [employees] empleados	[2d] / L2	[2d] / L2

Para cada elemento tenemos una estimación del tiempo de recuperación y una calificación de la madurez del proceso de recuperación (puesta en marcha del respaldo).

En el ejemplo anterior, el tapón es el local que tarda mucho en ser reemplazado, como podemos apreciar en una vista agregada:

[test] análisis de riesgos > Equipamiento de resp...		
activo	current	target
ACTIVOS		
[B] Activos esenciales		
is [operations] Unidad de negocio X	4d/L0-L5	4d/L0-L5
is [financial] Unidad de negocio Y	4d/L0-L5	4d/L0-L5
[E] Equipamiento		
A [equipment] medios habituales	[2d] / L3	[2d] / L3
[SS] Servicios subcontratados		
A [cloud] CSP	[10m] / L5	[10m] / L5
A [comms] conectividad (Internet)	[12h] / L4	[12h] / L4
[L] Instalaciones		
A [local] instalaciones normales	[4d] / L3	[4d] / L3
[P] Personal		
A [employees] empleados	[2d] / L2	[2d] / L2

Vamos a mejorar el plan.

[test] análisis de riesgos > Equipamiento de resp...		
activo	current	target
ACTIVOS		
[B] Activos esenciales		
is [operations] Unidad de negocio X	4d/L0-L5	2d/L0-L5
is [financial] Unidad de negocio Y	4d/L0-L5	2d/L0-L5
[E] Equipamiento		
A [equipment] medios habituales	[2d] / L3	[2d] / L3
[SS] Servicios subcontratados		
A [cloud] CSP	[10m] / L5	[10m] / L5
A [comms] conectividad (Internet)	[12h] / L4	[12h] / L4
[L] Instalaciones		
A [local] instalaciones normales	[4d] / L3	[1d] / L5
[P] Personal		
A [employees] empleados	[2d] / L2	[2d] / L2

Ahora el tapón está en la reposición del personal. Y así vamos mejorando poco a poco hasta tener algo convincente.

II.7. Medidas de seguridad

La continuidad del negocio se consigue por medio de recursos alternativos, pero se necesita algo más. Debemos protegernos de las amenazas como siempre: de forma preventiva (menos probables) y de forma reactiva (para limitar el daño, y para recuperarnos tras un desastre). Este es el papel de las salvaguardas.

as...	tdp	re...	salvaguarda	dudas	fuen...	aplica	com...	curr...	target	PILAR
			SALVAGUARDAS							
☐	G	EL	8		[IA] Identificación y autenticación			L1-L4	L3-L4	L2-L5
☐	T	EL	7		[AC] Control de acceso lógico		...	L0-L5	L3-L5	L2-L4
☐	G	PR	6		[D] Protección de la Información		...	L1-L5	L1-L5	L2-L4
☐	G	EL	8		[K] Protección de claves criptográficas		...	L3	L4	L2-L5
☐	G	PR	6		[S] Protección de los Servicios		...	L0-L5	L3-L5	L2-L4
☐	G	PR	7		[SW] Protección de las Aplicaciones Informáticas (SW)			L0-L5	L3-L5	L2-L4
☐	G	PR	7		[HW] Protección de los Equipos Informáticos (HW)		...	L0-L2	L0-L5	L2-L4
☐	G	PR	9		[COM] Protección de las Comunicaciones		...	L0-L3	L2-L5	L2-L5
☐	G	PR			[IP] Sistema de protección de frontera lógica		n.a.	n.a.	n.a.	n.a.
☐	G	PR	7		[MP] Protección de los Soportes de Información			L1-L2	L3-L5	L2-L4
☐	G	PR	6		[AUX] Elementos Auxiliares	phy...		L0-L2	L3-L5	L2-L4
☐	F	EL	6		[PPE] Protección física de los equipos		...	L2	L4-L5	L3-L4

Las medidas sirven para enfrentarse a los incidentes, en general, pero aquí nos centraremos en las que protegen la disponibilidad.

Las medidas se gestionan en 2 fases:

1. determine las que aplican (son de aplicación, valdrían para algo en nuestro sistema)
2. para las que aplican, evalúe su madurez

II.7.1. Recomendación

Para cada medida de seguridad, la columna [recomendación] es una estimación de PILAR sobre su importancia relativa.

Es un rango en el rango [nulo .. 10], estimado por PILAR teniendo en cuenta los activos, las dimensiones de seguridad y el nivel de riesgo abordado por esta salvaguarda.

La celda es gris si PILAR no encuentra ninguna razón para recomendar esta fila. Es decir, PILAR no sabe para qué riesgo es adecuada esta medida.

(O) - PILAR piensa que es una exageración ("demasiado").

(U) - PILAR piensa que es un underkill ("no es suficiente").

II.7.2. Aplicabilidad

En la columna [aplica] puede marcar las filas que no son de aplicación a este sistema. Una salvaguarda no aplica si no hay ningún riesgo en el sistema que pueda ser contrarrestado por esta contramedida. Por ejemplo,

si no tiene servidor (por ejemplo, cuando se externaliza como un servicio en la nube), no hay nada que hacer para proteger un servidor no existente. PILAR marca en gris la recomendación.

Puede suceder también que la salvaguarda es aplicable, pero usted tiene una mejor medida.

Algunas contramedidas pueden ser una exageración, y usted puede argumentar que su uso no está justificado. No hace que la salvaguarda sea inaplicable. Si usted decide saltar (LO) una contramedida que no está justificada, el riesgo permanece, y PILAR lo presenta. Una contramedida no justificada coincide con un riesgo bajo aceptado (se dice que está justificado asumir el riesgo).

Puede usar la columna [recomendación] como guía; pero al final del día, es su mejor juicio lo que decide. Tenga en cuenta que un inspector necesitará una buena explicación para eliminar una salvaguarda. La explicación puede escribirse como un comentario en la columna [comentario].

II.7.3. Atributos de las salvaguardas

La columna [aspecto] presenta “G” para las medidas de gestión de la seguridad, “T” para las medidas técnicas, “F” para las de seguridad física y “PER” para la gestión del personal.

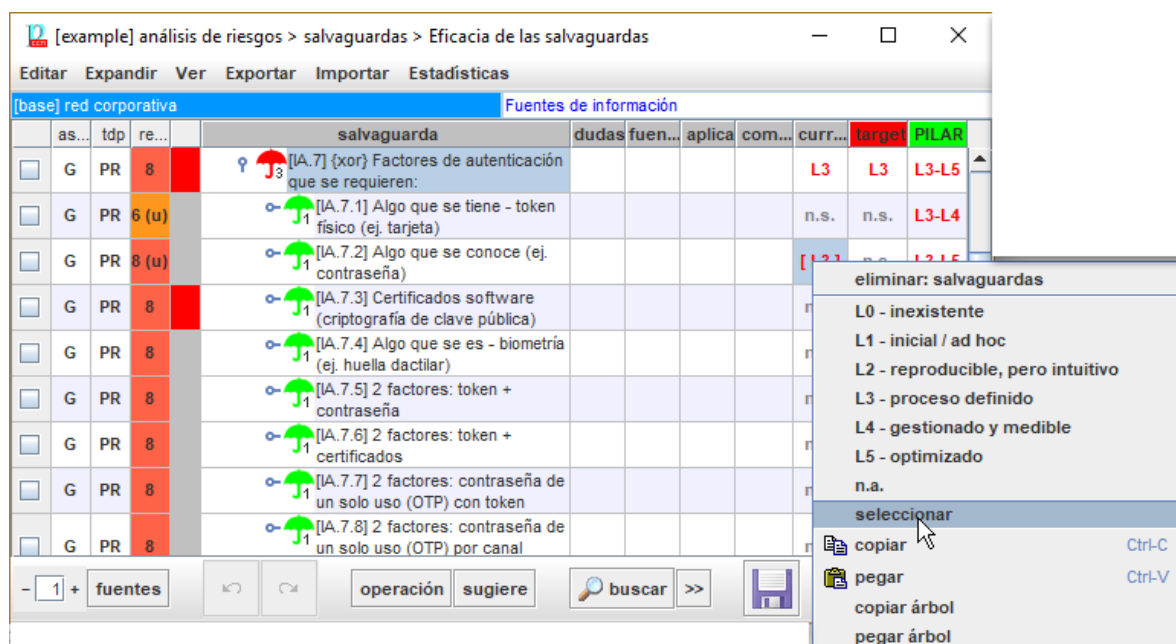
La columna [TDP] presenta el tipo de protección proporcionado por la medida:

- | | |
|---------------------------------|---------------------------------------|
| — PR – prevención | — AD – administrativa |
| — DR – disuasión | — AW – concienciación |
| — EL – eliminación | — DC – detección |
| — IM – minimización del impacto | — MN – monitorización |
| — CR – corrección | — std – norma |
| — RC – recuperación | — proc – procedimiento |
| | — cert – certificación o acreditación |

Las salvaguardas no son todas igual de importantes:

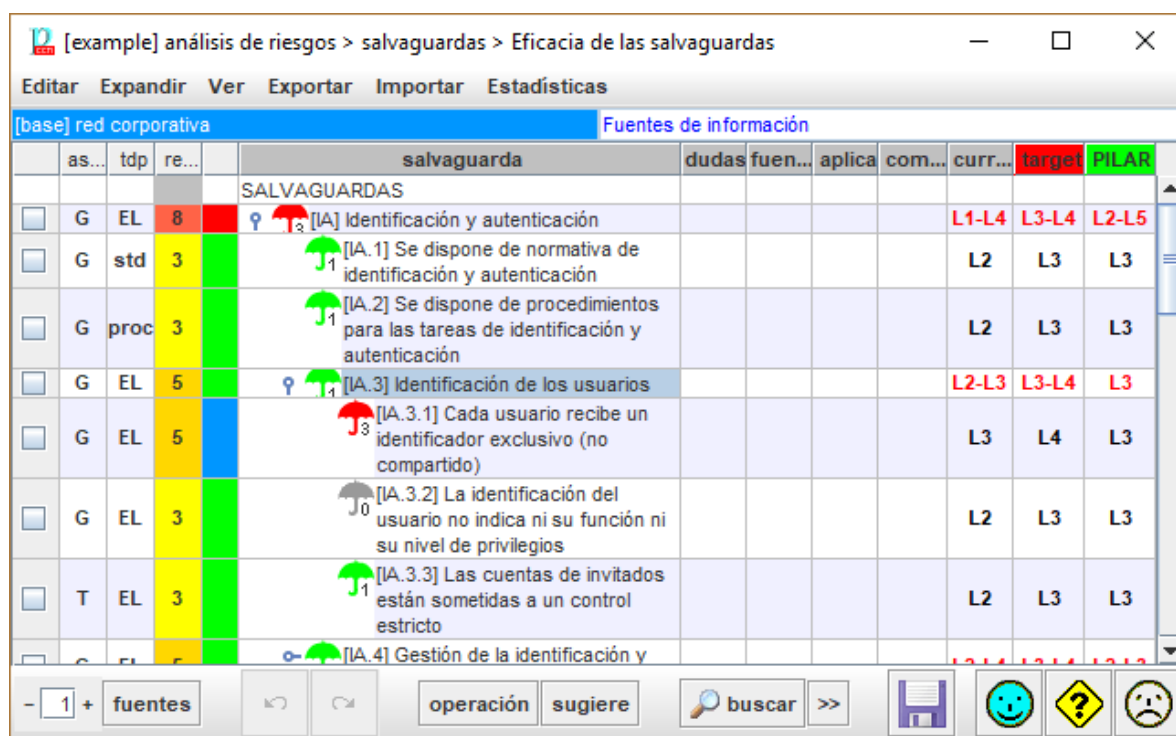
	máximo peso	crítica
	peso alto	muy importante
	peso normal	importante
	peso bajo	interesante
	aseguramiento: componentes certificados	

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



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

II.7.4. Valoración



Las columnas presentan fases (fotos en el tiempo) para evaluar las salvaguardas y registrar su progreso. Típicamente, hay 2 fases: actual y objetivo, y una fase especial, PILAR, calculada por la herramienta: lo que PILAR piensa que es un nivel prudente de madurez.

La valoración de las medidas se realiza por medio de niveles de madurez (ver Anexo A). Para salvaguardias individuales, tiene un valor de simple, entre L0 y L5. Para las salvaguardias compuestas de otras salvaguardias,

puede tener un rango (min-max). Existe la opción de presentar un valor aproximado de vencimiento que considere el nivel de madurez "promedio" de los hijos.

Se espera que el usuario proporcione niveles de madurez para cada medida de seguridad que sea aplicable para cada fase. Hay algunos trucos para simplificar la entrada de datos:

- IMPORTACIÓN: si ya ha realizado el ejercicio de evaluación, puede importarlo de otro análisis.
- SUGERENCIA: comenzar con una valoración general en el nivel superior, y luego ir profundizando en los hijos para un ajuste fino
- el valor en una fase se lleva a la siguiente fase a menos que haya una entrada manual
- si introduce un valor en una fila, se propagará a los hijos (las ramas de los árboles)
- si usted tiene valores en los hijos, el valor se recoge en el padre como un rango

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

	rec...	control	du...	apl...	co...	current	target	PILAR
☐	9	[K.comms] Protección de claves de comunicaciones				L3	L4	L2-L5
☐	3	[K.comms.1] Se dispone de normativa de gestión de claves				L3	L4	L3
☐	3	[K.comms.2] Se dispone de procedimientos de gestión de claves				L3	L4	L3
☐	3	[K.comms.3] Se identifican las personas responsables de cada clave				L3	L4	L3
☐	5	[K.comms.4] Operación				L3	L4	L3
☐	9	[K.comms.5] Las claves se generan en un entorno separado del de explotación				L3	L4	L5
☐	6	[K.comms.6] {xor} Generación de claves				L3	L4	L4
☐	5 (u)	[K.comms.6.1] Aplicación informática				[L3]	[L4]	L3
☐	6	[K.comms.6.2] Dispositivo criptográfico				n.s.	n.s.	[L4]
☐	8	[K.comms.7] {xor} Distribución de claves				L3	L4	L5
☐	8	[K.comms.7.1] Contenedor seguro				[L3]	[L4]	[L5]
☐	8	[K.comms.7.2] Canal seguro de comunicaciones				n.s.	n.s.	L5
☐	8	[K.comms.8] {xor} Almacenamiento de				L3	L4	L5

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).

II.7.5. Semáforo

El semáforo [tercera columna] compara la valoración en la fase de referencia [ROJA] con la valoración en la fase objetivo [VERDE], siguiendo este código de colores:

ROJO	el valor en la fase de referencia está muy por debajo del objetivo
AMARILLO	el valor en la fase de referencia está algo por debajo del objetivo
VERDE	el valor en la fase de referencia está a la altura del objetivo
AZUL	el valor en la fase de referencia está por encima del objetivo

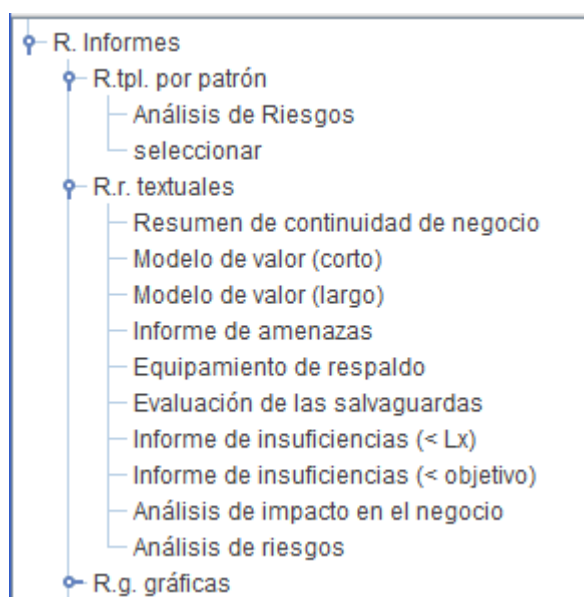
Haga clic con el ratón en las cabeceras de las fases para seleccionar cuál es la referencia (botón izquierdo) y cuál es el objetivo (botón derecho).

II.7.6. Dudas y comentarios

En la columna [dudas] puede marcar una fila para recordar que falta información.

II.8. Informes

PILAR se distribuye con varios informes predefinidos. Algunos informes están cableados (texto y gráficas) mientras que otros se generan por medio de patrones. Los patrones usan el formato RTF, que puede editarse con muchos editores de texto.



Las gráficas son útiles para presentaciones: copie de PILAR y péguela donde la necesite.

Algunos informes textuales son valiosos por sí mismos, bien como informes finales, bien como material de trabajo (por ejemplo, en entrevistas con los responsables de los activos) para recolectar información o para validarla.

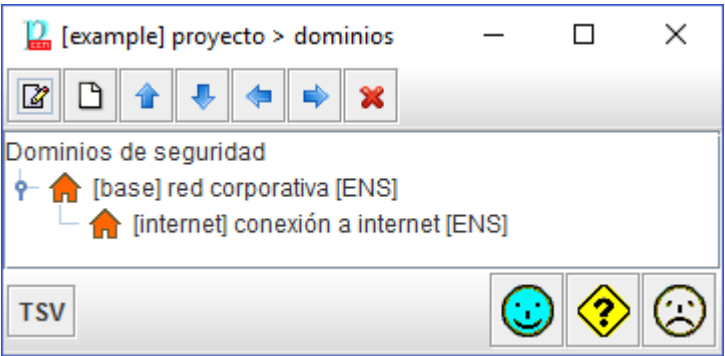
Capítulo III – Usuario medio

III.1. Dominios de seguridad

Los activos pueden distribuirse en dominios. Cada dominio puede tener asociado un perfil de ataques propio, así como un conjunto propio de medidas de seguridad.

Proyecto > Dominios de seguridad

Para identificar dominios



Los dominios de seguridad pueden anidarse: un dominio aparece como hijo de otro dominio. El anidamiento se utiliza en la valoración de salvaguardas y perfiles de seguridad. Los dominios anidados heredan el nivel de madurez del dominio padre. De tal manera que puede valorar el dominio base y, a continuación, refinarlo según sea necesario en dominios anidados.

Para valorar activos, debe calificar activos esenciales y su valor se traslada a cada activo en el mismo dominio ya otros dominios a los que se asocia el activo esencial.

activo / dominio de seguridad	[1d]	[2d]	[3d]	[4d]	[5d]	[6d]	[7d]	[8d]	[9d]	[10d]
[test]										
[essential] Activos esenciales		[4]		[5]		[7]				
is [operations] Unidad de negocio		[4]				[7]				
is [financial] Unidad de negocio				[5]						
Dominios de seguridad										
[base] Base		[4]		[5]		[7]				
[critical]		[4]				[7]				

III.2. Fases del proyecto

Las medidas de seguridad van evolucionando con el tiempo. Las fases son fotos para recoger esta evolución. Por ejemplo, anualmente.

Proyecto > Fases

Para identificar y reordenar las fases en una lista

[example] proyecto > fases

[current] situación actual {}
[target] situación objetivo {info_owner}

[example] proyecto > fases

[2015] {}
[2016] {}
[2017] {info_owner}

Las fases se usan en la valoración de las salvaguardas y los controles. La valoración en una fase es automáticamente trasladada a la siguiente fase hasta que se modifica explícitamente

Puede valorar la madurez de las salvaguardas aplicables por dominio de seguridad y por fase. Recuerde que los valores en un dominio se heredan en sus hijos y que los valores en una fase se propagan a las fases siguientes. Hasta que introduce un nuevo valor.

Podemos pedir a PILAR que sugiera medidas para un cierto dominio y fase, teniendo en cuenta las necesidades de seguridad del sistema y la potencia protectora de cada salvaguarda:

[example] análisis de riesgos > salvaguardas > Eficacia de las salvaguardas

Editar Expandir Exportar Importar Estadísticas

[base] red corporativa Fuentes de información

as...	tdp	salvaguarda	dudas	fuen...	com...	reco...	cur...	target	PILAR
G	CR	de incidentes				4	L0-L2	L2-L3	L2-L3
G	IM	[IR.3] Contención del incidente				6	-L2	-L5	L3-L4
G	AD	[IR.3.1] El personal designado cubre las 24h los 7 días de la semana				3	L1	L3	L3
G	IM	[IR.3.2] El fallo del sistema deja a este en un estado controlado				3	L1	L3	L3
G	IM	[IR.3.3] Se suspenden cautelarmente los trabajos en el sistema afectado				6	L2	L5	L4
G	IM	[IR.3.4] Se aísla cautelarmente el sistema afectado				6			L4

[IA.7.3.2] El certificado se inhabilita cuando se ve comprometido o hay sospecha de ello
[IR.3.4] Se aísla cautelarmente el sistema afectado
[L.3.5.3.4] Existe un plan de emergencia para hacer frente a la violencia
[L.6.8] Eliminación residuos
[tools.AV.b] Se bloquea el acceso a sitios web peligrosos (blacklisting)

- 1 + fuentes operación sugiere buscar >>

Capítulo IV – Uso avanzado

IV.1. Dependencias

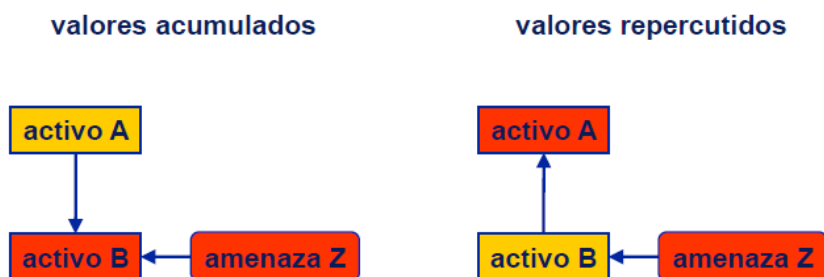
La aproximación de trasladar uniformemente los requisitos de seguridad a todos los activos en el mismo dominio es muy rápida, pero a veces puede resultar excesivamente simplista. Por ejemplo, cuando cada información y cada servicio usan sólo algunos servidores, no todos.

Las dependencias proporcionan una transferencia controlada de valor.

Hay que activar el uso de dependencias:

Editar > Opciones > Valoración > activos + dependencias

Ahora podemos indicar a PILAR que un activo A depende de un activo B:

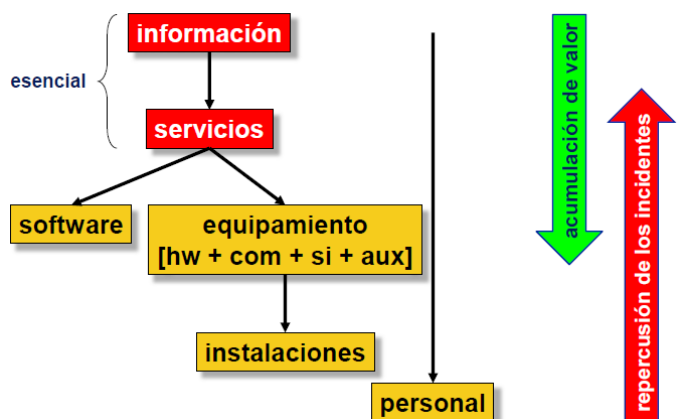


- los requisitos de seguridad (niveles de valoración) del activo A se transfieren al activo B
- los ataques en el activo B tienen un efecto directo sobre el valor acumulado en B
- los ataques en el activo B tienen un efecto indirecto (repercutido) en el activo A

Establecer un sistema correcto de dependencias lleva tiempo, y es difícil de mantener; pero proporciona un análisis ajustado de los riesgos.

Como reglas generales:

- la información esencial depende de los servicios esenciales
- los servicios esenciales dependen del equipamiento (hw, sw, comunicaciones y soportes de información)
- los equipos materiales dependen de las instalaciones
- todos los activos dependen de los usuarios que puede dañarlos con sus actividades

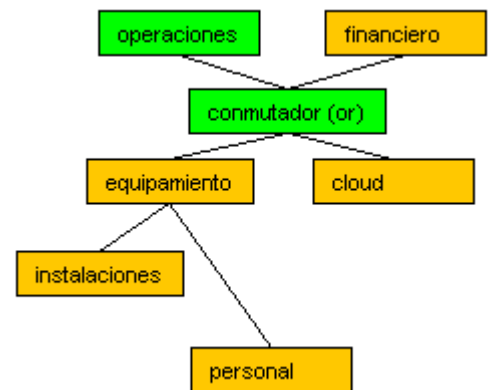


IV.1.1. Nodos OR

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

- La disponibilidad no se transmite a los hijos de los nodos OR, excepto a aquellos nodos descendientes a los que se pueda llegar a través de todas las ramas (hijos) del nodo OR

Es decir, los nodos OR representan formas alternativas de provisionar un servicio. Todas las ramas deben mantener los requisitos de seguridad de la información (confidencialidad, integridad, etc.) pero la disponibilidad o se traslada ya que cada rama tiene una alternativa que la respalda. Solamente los nodos compartidos (puntos únicos de fallo) reciben los requisitos de disponibilidad del nodo OR.



IV.2. Valoración activo a activo

Puede incluso evitar la valoración por dominios y no establecer ninguna dependencia. Ahora cada activo debe ser valorado individualmente. Es muy laborioso y difícil de mantener cuando el sistema cambia. Y PILAR no puede calcular riesgos repercutidos.

IV.3. Amenazas

Por defecto, PILAR aplica 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.

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

También puede modificar las amenazas manualmente dentro de PILAR

Editar > Opciones > Amenazas > manual

Se desactiva el uso del perfil TSV y se controlan manualmente los valores.

Editar > Opciones > Amenazas > mix

Modo semi-manual. Primero se marcan qué amenazas se quieren sacar del modo automático, y luego podemos modificar manualmente su probabilidad y consecuencias. El TSV se sigue aplicando a las demás amenazas.

Capítulo V – Personalización

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

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

“Personalización” en <https://www.pilar-tools.com/doc/>

V.1. Fichero de configuración

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

STIC_es.car

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

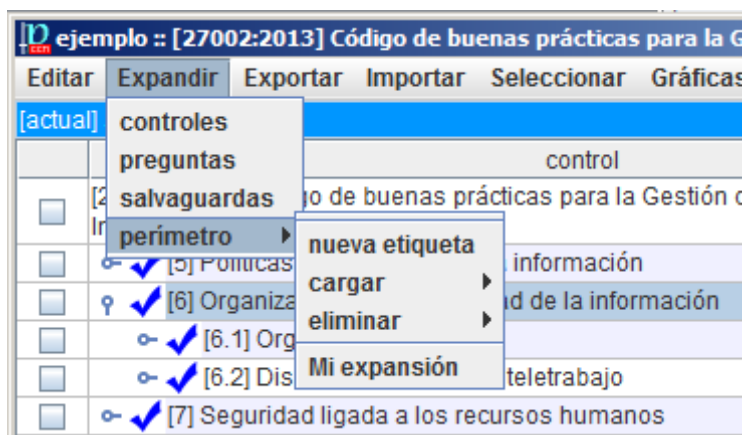
Algunos ajustes que se pueden hacer:

- 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)
- ...

V.2. Perímetros

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.

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



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

Para usar una etiqueta

Expandir > perímetro > su etiqueta

Para eliminar una etiqueta

Expandir > perímetro > eliminar > su etiqueta

V.3. Patrones para informes

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

Ver “Patrones” en <https://www.pilar-tools.com/doc/>

Puede establecer los patrones por defecto para sus análisis:

Ver “Personalización” en <https://www.pilar-tools.com/doc/>

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

Capítulo VI – Otros temas

VI.1. DRP – Plan de Recuperación de Desastres

DRP - Disaster Recovery Plan

Un plan de recuperación de desastres es un plan de acción para reconstruir un sistema de información después de un desastre. Es un programa acerca de cuándo entra en servicio cada activo alternativo.

PILAR utiliza la valoración de los servicios esenciales para establecer objetivos y dependencias (ya sea explícita o mediante dominios de seguridad) para vincular los recursos necesarios.

Vamos a comentar un ejemplo:

[test] proyecto > plan de recuperación de desastres												
activo	tiem...	[0s]	[1d]	[2d]	[3d]	[4d]	[5d]	[6d]	[7d]	[8d]	[9d]	[10d]
		[0]	[0]	[4]	[4]	[5]	[5]	[7]	[7]	[7]	[7]	[7]
		[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
ACTIVOS												
♀ [B] Activos esenciales												
is [operations] Unidad de negocio X				obje...		obje...						
is [financial] Unidad de negocio Y						obje...						
♀ [E] Equipamiento												
A [equipment] medios habituales	2d			disp...								
♀ [SS] Servicios subcontratados												
A [cloud] CSP	10m		disp...									
A [comms] conectividad (Internet)	12h		disp...									
♀ [L] Instalaciones												
A [local] instalaciones normales	4d					disp...						
♀ [P] Personal												
A [employees] empleados	2d			disp...								
- 5 + cargar guardar csv informe 😊 ⚠												

La columna tiempo indica el tiempo esperado para que cada activo esté disponible. En la planificación, puede ver el punto en el tiempo en el que cada activo está disponible. Para las unidades de negocio, marcamos objetivos que solamente podremos satisfacer con la recuperación prevista de los activos de soporte. En conjunto, el servicio X se reinicia en 2 días, y el servicio Y en 4 días, ambos están disponibles antes de que las consecuencias sean relevantes.

[0s]	[1d]	[2d]	[3d]	[4d]	[5d]	[6d]	[7d]	[8d]	[9d]	[10d]
[0]	[0]	[4]	[4]	[5]	[5]	[7]	[7]	[7]	[7]	[7]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]

En conjunto, podemos decir que es un buen plan que recupera la actividad del negocio sin consecuencias negativas relevantes.

Un sistema puede requerir varios planes de recuperación para diferentes escenarios de desastre

- hay que reconstruir todo el sistema (como en el ejemplo anterior)
- los servidores no están operativos, pero sí los servicios de comunicaciones y la nube
- las instalaciones no se ven afectadas
- solamente nos falta el personal
- ...

VI.2. Zonas

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.

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

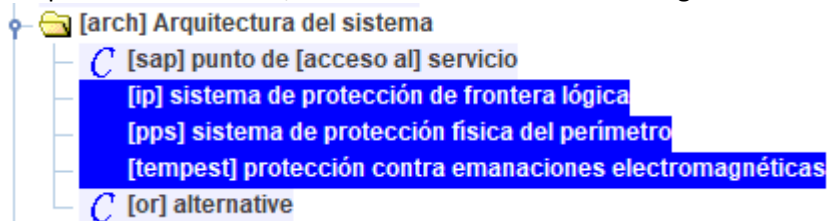
- tenemos 2 zonas
 - dentro del área
 - fuera del área
- y una frontera, el local



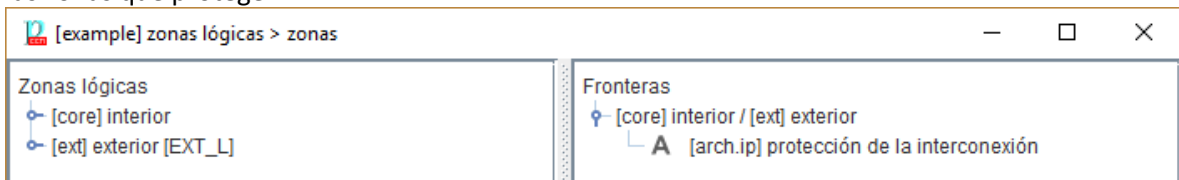
El atacante necesita entrar, superando el perímetro de protección física (la protección que aportan paredes, puertas, ventanas, etc.) y luego podría atacar el servidor.

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)
- Respecto de la frontera, los activos de frontera son de alguno de estos tipos

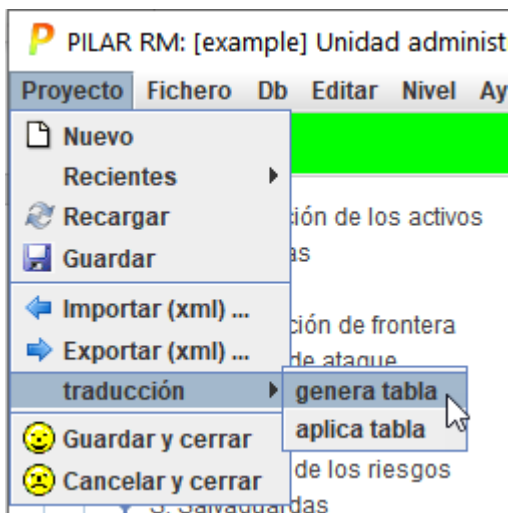
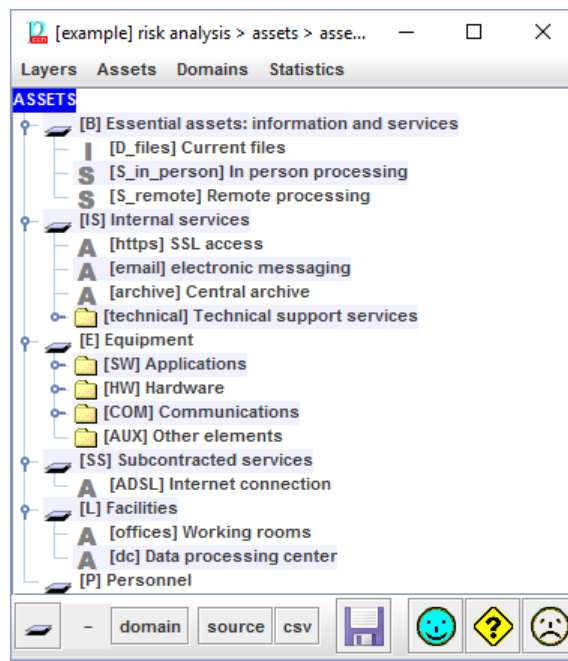
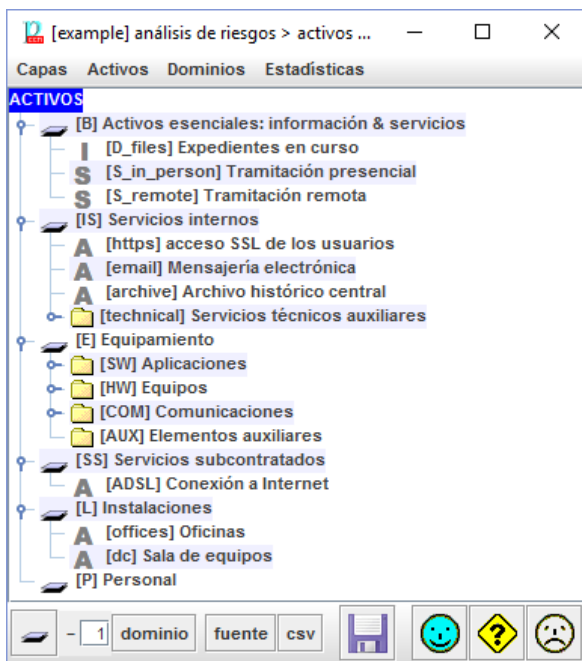


- Nótese que la frontera puede ser un activo singular (como un cortafuegos) o un conjunto de elementos singulares (varios cortafuegos, un proxy, servidores en la DMZ, etc.). En este último caso se recomienda definir un activo que defina la funcionalidad de la frontera como una función integrada. En el caso de una frontera lógica, este activo basta que sea de tipo [arch.ip] y que esté ubicado entre las zonas que protege



VI.3. Idiomas

Se puede partir de un proyecto escrito en un idioma I1 y verlo en otro idioma I2. PILAR utiliza los códigos de los elementos como claves y les asocia diferentes nombres en diferentes idiomas.



En la ventana principal

Proyecto > Traducción > generación

Seleccione un fichero

ejemplo.rw

El resultado es un fichero de texto con reglas de traducción, una por línea, que el usuario puede editar. Las reglas se aplican secuencialmente.

Por ejemplo,

```
asset: [mission] System mission -> [] Misión del sistema
```

PILAR busca un activo de código 'mission'. El código no cambia, pero el nombre se traduce a español. También puede escribir un nuevo código en la parte derecha

```
asset: [mission] System mission -> [misión] Misión del sistema
```

VI.4. Control de acceso

PILAR proporciona medios para proteger el proyecto de modificaciones no autorizadas. Para ello recurre a las fuentes de información, a las que asocia una contraseña.

Conceptos básicos:

- una fuente de información puede tener una contraseña asociada;
- los usuarios pueden abrir una sesión en la fuente si conocen la contraseña
- los elementos pueden asociarse a una o más fuentes de información; se necesitará tener una sesión abierta en al menos una de las fuentes asociadas para tener derechos de escritura sobre el elemento; de lo contrario el elemento aparece como "solo lectura"

Los siguientes elementos tienen control de acceso

- dominios de seguridad
- zonas (lógicas, físicas y tempest)
- fases del proyecto

VI.4.1. Contraseñas



Las fuentes “info_owner” y “service_owner” tienen una contraseña. Tenemos una sesión abierta en “info_owner” y no en “service_owner”.

Proyecto > Fuentes de información > [clic derecho] > contraseña

Para establecer o eliminar una contraseña.

Proyecto > Fuentes de información > [clic derecho] > abrir

Para abrir una sesión. Se solicita la contraseña.

Proyecto > Fuentes de información > [clic derecho] > cerrar

Para cerrar una sesión.

VI.4.2. Restricciones de acceso: dominios de seguridad

Cuando un dominio de seguridad tiene fuentes de información asociadas, necesita abrir una sesión en al menos una de dichas fuentes para

- modificar las fuentes
- modificar el código, el nombre o la descripción
- modificar activos (en ese dominio)
 - crear, cambiar de dominio o eliminar
 - modificar fuentes
 - modificar el código, el nombre, la descripción o atributos administrativos
 - modificar las clases
- modificar las salvaguardas para el dominio
 - modificar las fuentes
 - modificar aplicabilidad, comentarios o valoración
- modificar controles para el dominio
 - modificar las fuentes
 - modificar aplicabilidad, comentarios o valoración

VI.4.3. Restricciones de acceso: fases del proyecto

Cuando una fase del proyecto tiene fuentes de información asociadas, necesita abrir una sesión en al menos una de dichas fuentes para

- modificar las fuentes
- modificar el código, el nombre o la descripción
- modificar las salvaguardas para la fase

- modificar las fuentes
 - modificar aplicabilidad, comentarios o valoración
- modificar controles para la fase
 - modificar las fuentes
 - modificar aplicabilidad, comentarios o valoración

VI.4.4. Restricciones de acceso: zonas

Cuando una zona tiene fuentes de información asociadas, necesita abrir una sesión en al menos una de dichas fuentes para

- modificar las fuentes
- modificar el código, el nombre o la descripción

VI.5. Bases de datos

Se puede usar una base de datos externa. En principio, es válida cualquier base de datos SQL con una interfaz JDBC.

En la base de datos se pueden almacenar proyectos y resultados del análisis de datos. Es útil para compartir proyectos entre varios usuarios y para explotar los datos generados en informes por medio de herramientas que trabajen sobre datos SQL.

Ver “tablas SQL” en <https://www.pilar-tools.com/doc/>

VI.6. Modo batch

PILAR puede ejecutarse en modo “batch”; es decir, sin interfaz gráfica de usuario. Este modo es útil para:

- cálculos programados (por ejemplo, a media noche)
- análisis de riesgo reactivo (por ejemplo, como consecuencia del descubrimiento de una vulnerabilidad)

Ver “modo batch” en <https://www.pilar-tools.com/doc/>

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.

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.

Las 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.

información

Una instancia de un tipo de información.

Una categoría específica de información (por ejemplo, administración de seguridad privada, médica, de propiedad, financiera, de investigación, sensible al contratista) definida por una organización o, en algunos casos, por una ley específica, Orden ejecutiva, directiva, política o regulación.

[<https://csrc.nist.gov/glossary/term/information-type>]

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]

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.

servicio

Una capacidad o función proporcionada por una entidad.

[<https://csrc.nist.gov/glossary/term/service>]

sistema de información

Un conjunto discreto de recursos de información organizados para la recopilación, procesamiento, mantenimiento, uso, intercambio, difusión y disposición de la información.

[<https://csrc.nist.gov/glossary/term/System>]

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 la materialización de una amenaza.

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.
- ISO 22301:2012
Societal security – Business continuity management systems – Requirements
- ISO/IEC 27031:2011
Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 24762:2008
Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services