MAGERIT – versión 3.0
Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Libro I - Método

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS
DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

TÍTULO: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método

Elaboración y coordinación de contenidos:
Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica

Equipo responsable del proyecto:
Director, Miguel Angel Amutio Gómez, Ministerio de Hacienda y Administraciones Públicas
Javier Candau, Centro Criptológico Nacional, Ministerio de la Presidencia
Consultor externo: José Antonio Mañas, Catedrático de la Universidad Politécnica de Madrid

Características: Adobe Acrobat 5.0
Responsable edición digital: Subdirección General de Información, Documentación y Publicaciones
(Jesús González Barroso)

Madrid, octubre de 2012
Disponible esta publicación en el Portal de Administración Electrónica (PAe):
http://administracionelectronica.gob.es/

Edita:

Secretaría General Técnica
Subdirección General de Información,
Documentación y Publicaciones
Centro de Publicaciones

Colección: administración electrónica
NIPO: 630-12-171-8

Índice

1. Introducción

El CSAE[1] ha elaborado y promueve Magerit[2] como respuesta a la percepción de que la Administración Pública (y en general toda la sociedad) depende de forma creciente de los sistemas de información para alcanzar sus objetivos. El uso de tecnologías de la información y comunicaciones (TIC) supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios.

1.1 Buen gobierno

La gestión de los riesgos es una piedra angular en las guías de buen gobierno [ISO 38500], público o privado, donde se considera un principio fundamental que las decisiones de gobierno se fundamenten en el conocimiento de los riesgos que implican:

> *1.6.12 Propuesta*
>
> *Recopilación de los beneficios, costos, riesgos, oportunidades, y otros factores que deben tenerse en cuenta en las decisiones que se tomen.*[3]

cubriendo riesgos en general y riesgos TIC en particular:

> *Esta norma establece los principios para el uso eficaz, eficiente y aceptable de las tecnologías de la información. Garantizando que sus organizaciones siguen estos principios ayudará a los directores a equilibrar riesgos y oportunidades derivados del uso de las TI.*[4]

Se insiste recurrentemente en el necesario equilibrio entre riesgos y oportunidades para tomar las mejores decisiones.

En pocas palabras, la gestión de los riesgos es nuclear al gobierno de las organizaciones. En particular, los riesgos que tienen su origen en el uso de tecnologías de la información deben trasladarse a los órganos de gobierno y contextualizarse en la misión de la organización.

El conocimiento de los riesgos permite calibrar la confianza en que los sistemas desempeñarán su función como la Dirección espera, habilitando un marco equilibrado de Gobierno, Gestión de Riesgos y Cumplimiento (GRC), tres áreas que deben estar integradas y alineadas para evitar conflictos, duplicación de actividades y zonas de nadie.

Los órganos de gobierno no deben tratar solamente riesgos TIC. Es más, no deben tratar los riesgos TIC por separado de los demás riesgos. Aunque Magerit se especializa en riesgos TIC, debemos ser muy conscientes de que es esencial transmitir a los órganos de gobiernos las oportunidades y los riesgos que conllevan las tecnologías de la información para que se puedan incluir en un marco global y tomar las mejores decisiones para la Organización.

1.2. Confianza

La confianza es la esperanza firme que se tiene de que algo responderá a lo previsto. La confianza es un valor crítico en cualquier organización que preste servicios. Las administraciones públicas son especialmente sensibles a esta valoración.

Por una parte dependemos fuertemente de los sistemas de información para cumplir nuestros objetivos; pero por otra parte, no deja de ser un tema recurrente la inquietud por su seguridad. Los afectados, que frecuentemente no son técnicos, se preguntan si estos sistemas merecen su confianza, confianza que se ve mermada por cada fallo y, sobre todo, cuando la inversión no se tra-

[1] CSAE: Consejo Superior de Administración Electrónica.
[2] MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
[3] 1.6.12 Proposal. Compilation of benefits, costs, risks, opportunities, and other factors applicable to decisions to be made. Includes business cases
[4] *This standard establishes principles for the effective, efficient and acceptable use of IT. Ensuring that their organisations follow these principles will assist directors in balancing risks and encouraging opportunities arising from the use of IT.*

duce en la ausencia de fallos. Lo ideal es que los sistemas no fallen. Pero lo cierto que se acepta convivir con sistemas que fallan. El asunto no es tanto la ausencia de incidentes como la confianza en que están bajo control: se sabe qué puede pasar y se sabe qué hacer cuando pasa. El temor a lo desconocido es el principal origen de la desconfianza y, en consecuencia, aquí se busca conocer para confiar: conocer los riesgos para poder afrontarlos y controlarlos.

1.3. Gestión

Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos.

En el periodo transcurrido desde la publicación de la primera versión de Magerit (1997) hasta la fecha, el análisis de riesgos se ha venido consolidando como paso necesario para la gestión de la seguridad. Así se recoge claramente en las Directrices de la OCDE [OCDE] que, en su principio 6 dicen:

> *6) Evaluación del riesgo. Los participantes deben llevar a cabo evaluaciones de riesgo.*

En el Esquema Nacional de Seguridad [RD 3/2010], el Capítulo II Principios Básicos, dice

> *Artículo 6. Gestión de la seguridad basada en los riesgos.*
>
> *1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.*
>
> *2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.*

1.4. Magerit

Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos". En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

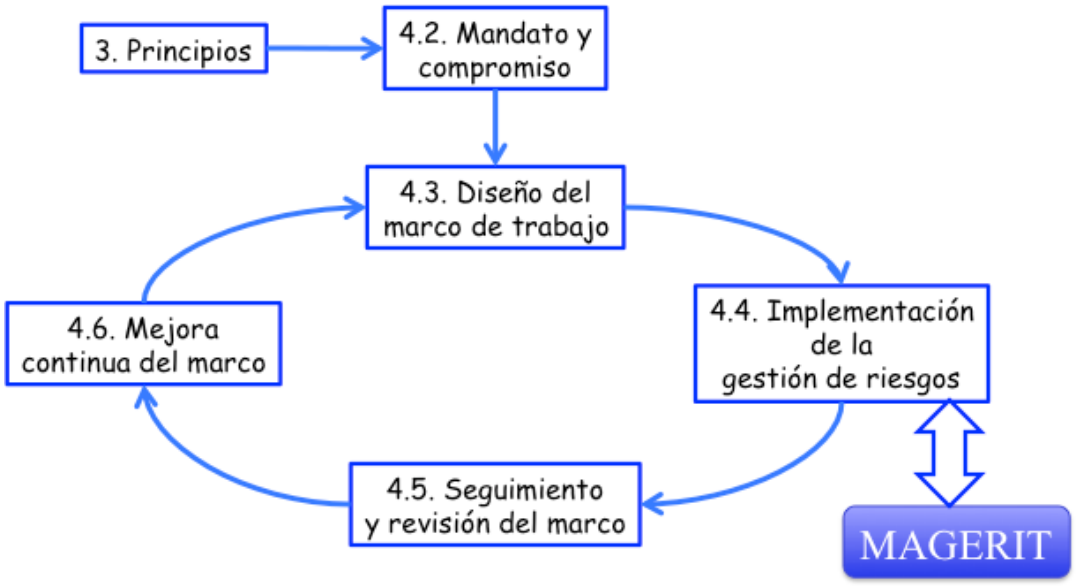

Ilustración 1. ISO 31000 - Marco de trabajo para la gestión de riesgos

Hay varias aproximaciones al problema de analizar los riesgos soportados por los sistemas TIC: guías informales, aproximaciones metódicas y herramientas de soporte. Todas buscan objetivar el análisis de riesgos para saber cuán seguros (o inseguros) son los sistemas y no llamarse a engaño. El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello que en Magerit se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Magerit persigue los siguientes objetivos:

Directos:

1. concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
2. ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
3. ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos:

4. preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

También se ha buscado la uniformidad de los informes que recogen los hallazgos y las conclusiones de las actividades de análisis y gestión de riesgos:

Modelo de valor
: Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.

Mapa de riesgos
: Relación de las amenazas a que están expuestos los activos.

Declaración de aplicabilidad
: Para un conjunto de salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.

Evaluación de salvaguardas
: Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

Estado de riesgo
: Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.

Informe de insuficiencias
: Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema. Es decir, recoge las vulnerabilidades del sistema, entendidas como puntos débilmente protegidos por los que las amenazas podrían materializarse.

Cumplimiento de normativa
: Satisfacción de unos requisitos. Declaración de que se ajusta y es conforme a la normativa correspondiente.

Plan de seguridad
: Conjunto de proyectos de seguridad que permiten materializar las decisiones de tratamiento de riesgos

1.5. Introducción al análisis y gestión de riesgos

Seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que compro-

metan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.[5]

El objetivo a proteger es la misión de la Organización, teniendo en cuenta las diferentes dimensiones de la seguridad:

Disponibilidad:

o disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

Integridad:

o mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

Confidencialidad:

o que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

A estas dimensiones canónicas de la seguridad se pueden añadir otras derivadas que nos acerquen a la percepción de los usuarios de los sistemas de información:

Autenticidad:

Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.

Trazabilidad:

Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.

Todas estas características pueden ser requeridas o no dependiendo de cada caso. Cuando se requieren, no es evidente que se disfruten sin más. Lo habitual que haya que poner medios y esfuerzo para conseguirlas. A racionalizar este esfuerzo se dedican las metodologías de análisis y gestión de riesgos que comienzan con una definición:

Riesgo:

estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema:

Análisis de riesgos:

proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

Sabiendo lo que podría pasar, hay que tomar decisiones:

[5] Reglamento (CE) n 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información.

Tratamiento de los riesgos

proceso destinado a modificar el riesgo.

Hay múltiples formas de tratar un riesgo: evitar las circunstancias que lo provocan, reducir las posibilidades de que ocurra, acotar sus consecuencias, compartirlo con otra organización (típicamente contratando un servicio o un seguro de cobertura), o, en última instancia, aceptando que pudiera ocurrir y previendo recursos para actuar cuando sea necesario.

Nótese que una opción legítima es aceptar el riesgo. Es frecuente oír que la seguridad absoluta no existe; en efecto, siempre hay que aceptar un riesgo que, eso sí, debe ser conocido y sometido al umbral de calidad que se requiere del servicio. Es más, a veces aceptamos riesgos operacionales para acometer actividades que pueden reportarnos un beneficio que supera al riesgo, o que tenemos la obligación de afrontar. Es por ello que a veces se emplean definiciones más amplias de riesgo:

> *Efecto de la incertidumbre sobre la consecución de los objetivos.*
> *[ISO Guía 73]*

Como todo esto es muy delicado, no es meramente técnico, e incluye la decisión de aceptar un cierto nivel de riesgo, deviene imprescindible saber en qué condiciones se trabaja y así poder ajustar la confianza que merece el sistema. Para ello, qué mejor que una aproximación metódica que permita tomar decisiones con fundamento y explicar racionalmente las decisiones tomadas.

1.6. El análisis y el tratamiento de los riesgos en su contexto

Las tareas de análisis y tratamiento de los riesgos no son un fin en sí mismas sino que se encajan en la actividad continua de gestión de la seguridad.

El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema. En coordinación con los objetivos, estrategia y política de la Organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la Dirección. Al conjunto de estas actividades se le denomina Proceso de Gestión de Riesgos.

La implantación de las medidas de seguridad requiere una organización gestionada y la participación informada de todo el personal que trabaja con el sistema de información. Es este personal el responsable de la operación diaria, de la reacción ante incidencias y de la monitorización en general del sistema para determinar si satisface con eficacia y eficiencia los objetivos propuestos.

Este esquema de trabajo debe ser repetitivo pues los sistemas de información rara vez son inmutables; más bien se encuentran sometidos a evolución continua tanto propia (nuevos activos) como del entorno (nuevas amenazas), lo que exige una revisión periódica en la que se aprende de la experiencia y se adapta al nuevo contexto.

El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento. La fase de tratamiento estructura las acciones que se acometen en materia de seguridad para satisfacer las necesidades detectadas por el análisis.

Los sistemas de gestión de la seguridad de la información (SGSI) [ISO 27001] formalizan cuatro etapas cíclicas:

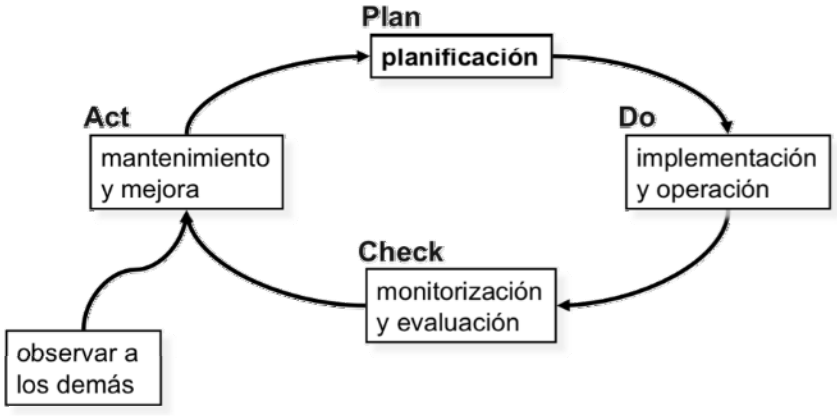

Ilustración 2. Ciclo PDCA

El análisis de riesgos es parte de las actividades de planificación, donde se toman decisiones de tratamiento. Estas decisiones se materializan en la etapa de implantación, donde conviene desplegar elementos que permitan la monitorización de las medidas desplegadas para poder evaluar la efectividad de las mismas y actuar en consecuencia, dentro de un círculo de excelencia o mejora continua.

1.6.1. Concienciación y formación

El mejor plan de seguridad se vería seriamente hipotecado sin una colaboración activa de las personas involucradas en el sistema de información, especialmente si la actitud es negativa, contraria a las medidas, o tienen la percepción de pasarse el día "luchando contra las [absurdas] medidas de seguridad". Es por ello que se requiere la creación de una "cultura de seguridad" que, emanando de la alta dirección, conciencie a todos los involucrados de su necesidad y pertinencia.

Son tres los pilares fundamentales para la creación de esta cultura:

- una política de seguridad corporativa que se entienda (escrita para los que no son expertos en la materia), que se difunda y que se mantenga al día
- una normativa se seguridad que, entrando en áreas específicas de actividad, aclare la postura de la Organización; es decir, defina lo que es uso correcto y lo que es incumplimiento
- una formación continua a todos los niveles, recordando las cautelas rutinarias y las actividades especializadas, según la responsabilidad adscrita a cada puesto de trabajo

A fin de que estas actividades cuajen en la organización, es imprescindible que la seguridad sea:

- mínimamente intrusiva: que no dificulte innecesariamente la actividad diaria ni hipoteque alcanzar los objetivos de productividad propuestos,
- sea "natural": que no de pie a errores gratuitos[6], que facilite el cumplimiento de las buenas prácticas propuestas y
- practicada por la Dirección: que dé ejemplo en la actividad diaria y reaccione con presteza a los cambios e incidencias.

1.6.2. Incidencias y recuperación

Las personas involucradas en la utilización y operación del sistema deben ser conscientes de su papel y relevancia continua para prevenir problemas y reaccionar cuando se produzcan. Es importante crear una cultura de responsabilidad donde los potenciales problemas, detectados por los que están cercanos a los activos afectados, puedan ser canalizados hacia los puntos de decisión. De esta forma el sistema de seguridad responderá con presteza a las circunstancias de cada momento.

[6] A menudo se oye hablar de "seguridad por defecto" o "seguridad sin manual" para recoger esta idea de que los sistemas son más seguros si la forma natural de utilizarlos es la forma segura de utilizarlos.

Cuando se produce una incidencia, el tiempo empieza a correr en contra del sistema: su supervivencia depende de la agilidad y corrección de las actividades de reporte y reacción. Cualquier error, imprecisión o ambigüedad en estos momentos críticos, se ve amplificado convirtiendo lo que podía ser un mero incidente en un desastre.

Conviene aprender continuamente, tanto de los éxitos como de los fracasos, e incorporar lo que vamos aprendiendo al proceso de gestión de riesgos. La madurez de una organización se refleja en la pulcritud y realismo de su modelo de valor y, consecuentemente, en la idoneidad de las salvaguardas de todo tipo, desde medidas técnicas hasta una óptima organización.

1.7. Organización de las guías

Esta versión 3 de Magerit se ha estructurado en dos libros y una guía de técnicas:

— Libro I – Método

— Libro II – Catálogo de elementos

— Guía de Técnicas – Recopilación de técnicas de diferente tipo que pueden ser de utilidad para la aplicación del método.

Este libro se estructura de la siguiente forma:

- El capítulo 2 presenta los conceptos informalmente. En particular se enmarcan las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos.
- El capítulo 3 concreta los pasos y formaliza las actividades de análisis de los riesgos.
- El capítulo 4 describe opciones y criterios de tratamiento de los riesgos y formaliza las actividades de gestión de riesgos.
- El capítulo 5 se centra en los proyectos de análisis de riesgos, proyectos en los que nos veremos inmersos para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente.
- El capítulo 6 formaliza las actividades de los planes de seguridad, a veces denominados planes directores o planes estratégicos.
- El capítulo 7 se centra en el desarrollo de sistemas de información y cómo el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo.
- El capítulo 8 se anticipa a algunos problemas que aparecen recurrentemente cuando se realizan análisis de riesgos.

Los apéndices recogen material de consulta:

1. un glosario,
2. referencias bibliográficas consideradas para el desarrollo de esta metodología,
3. referencias al marco legal que encuadra las tareas de análisis y gestión en la Administración Pública Española,
4. el marco normativo de evaluación y certificación
5. las características que se requieren de las herramientas, presentes o futuras, para soportar el proceso de análisis y gestión de riesgos,
6. una guía comparativa de cómo Magerit versión 1 ha evolucionado a la versión 2 y a esta versión 3.

1.7.1. Modo de empleo

Siempre se explican informalmente las actividades a realizar, y en ciertos casos se formalizan como tareas que permiten una planificación y seguimiento:

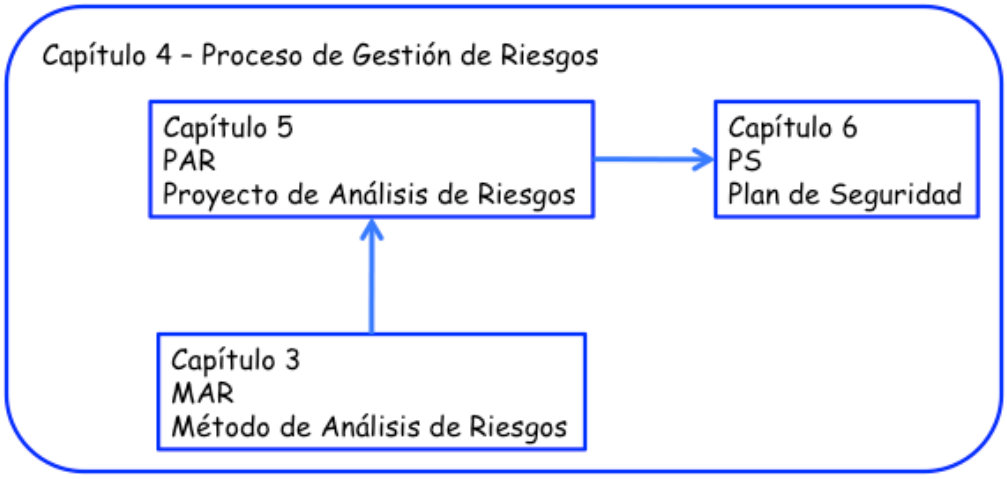

Ilustración 3. Actividades formalizadas

En sistemas pequeños, estas actividades pueden llevarse a cabo sin muchos formalismos; pero cuando el sistema adquiere envergadura e involucra a diferentes personas y equipos de trabajo durante varias semanas, meses o años, la planificación formal ayuda a mantener el proceso bajo control.

En el planteamiento de estas guías se ha seguido un criterio “de máximos”, reflejando todo tipo de situaciones. En la práctica, el usuario puede encontrarse ante situaciones donde el alcance es más restringido. Ante estas situaciones, conviene ser práctico y no pretender aplicar todas las tareas descritas en Magerit desde el primer momento. Suele ser prudente realizar una aproximación iterativa, aplicando el método primero con trazo grueso y luego ir revisando el modelo para entrar en detalles. El proceso de gestión de riesgos debe identificar y tratar urgentemente los riesgos críticos, pudiendo ir tratando progresivamente riesgos de menor criticidad. Como se dice popularmente “lo perfecto es enemigo de lo bueno”. Lo prudente es armonizar el esfuerzo al valor de la información y los servicios que se sustentan.

Entiéndase pues Magerit como una guía que se puede y se debe adaptar al caso y sus circunstancias.

1.7.2. El catálogo de elementos

En libro aparte, se propone un catálogo, abierto a ampliaciones, que marca unas pautas en cuanto a:

- tipos de activos
- dimensiones de valoración de los activos
- criterios de valoración de los activos
- amenazas típicas sobre los sistemas de información
- salvaguardas a considerar para proteger sistemas de información

Se persiguen dos objetivos:

1. Por una parte, facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.
2. Por otra, homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

Cada sección incluye una notación XML que se empleará para publicar regularmente los elementos en un formato estándar capaz de ser procesado automáticamente por herramientas de análisis y gestión.

Si el lector usa una herramienta de análisis y gestión de riesgos, este catálogo será parte de la misma; si el análisis se realiza manualmente, este catálogo proporciona una amplia base de partida para avanzar rápidamente sin distracciones ni olvidos.

1.7.3. La guía de técnicas

En libro aparte, aporta luz adicional y orientación sobre algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos:

- técnicas específicas para el análisis de riesgos
  - análisis mediante tablas
  - análisis algorítmico
  - árboles de ataque
- técnicas generales
  - técnicas gráficas
  - sesiones de trabajo: entrevistas, reuniones y presentaciones
  - valoración Delphi

Se trata de una guía de consulta. Según el lector avance por la tareas del proyecto, se le recomendará el uso de ciertas técnicas específicas, de las que esta guía busca ser una introducción, así como proporcionar referencias para que el lector profundice en las técnicas presentadas.

1.8. Evaluación, certificación, auditoría y acreditación

El análisis de riesgos es una piedra angular de los procesos de evaluación, certificación, auditoría y acreditación que formalizan la confianza que merece un sistema de información. Dado que no hay dos sistemas de información iguales, la evaluación de cada sistema concreto requiere amoldarse a los componentes que lo constituyen. El análisis de riesgos proporciona una visión singular de cómo es cada sistema, qué valor posee, a qué amenazas está expuesto y de qué salvaguardas se ha dotado. Es pues el análisis de riesgos paso obligado para poder llevar a cabo todas las tareas mencionadas, que se relacionan según el siguiente esquema:

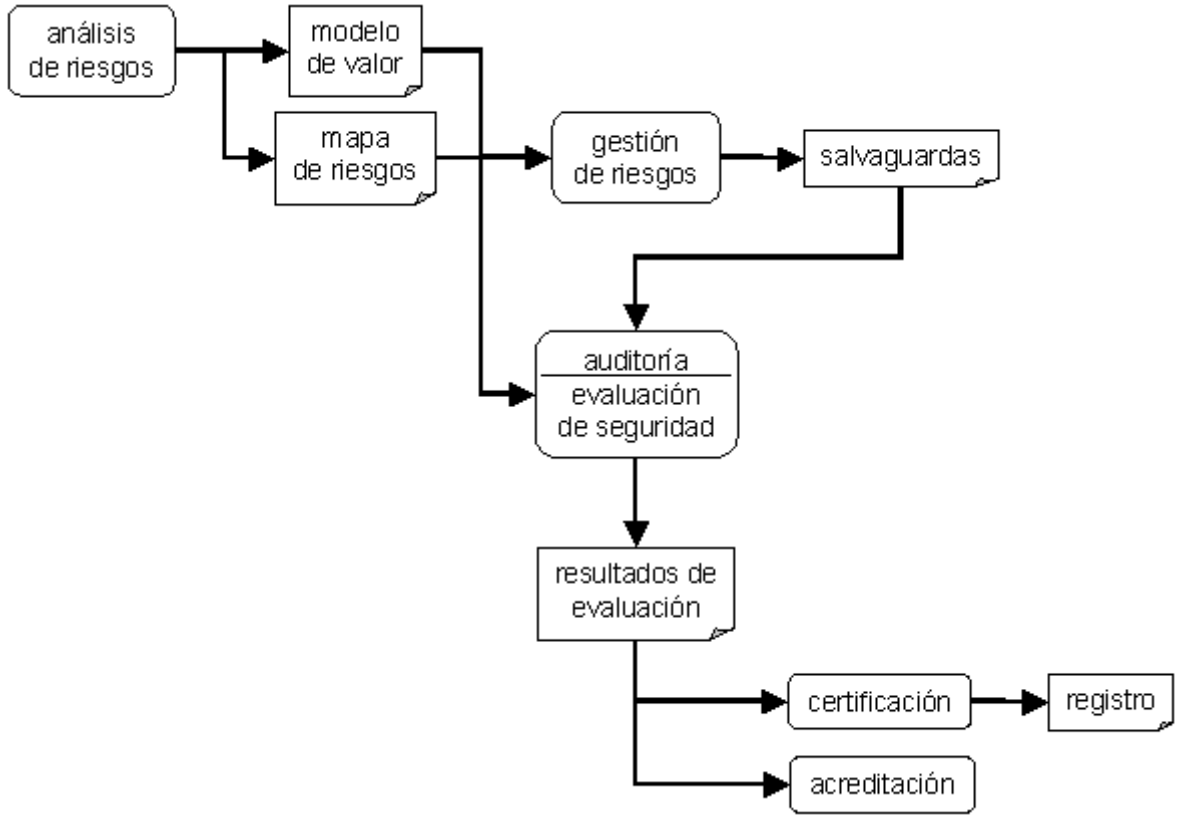

Ilustración 4. Contexto de certificación y acreditación de sistemas de información

En esta sección se hace una presentación conceptual de las actividades citadas. El lector encontrará en el apéndice 4 un tratamiento específico de los marcos normativos relativos a sistemas de gestión y productos de seguridad.

Evaluación

Es cada vez más frecuente la evaluación de la seguridad de los sistemas de información, tanto internamente como parte de los procesos de gestión, como por medio de evaluadores independientes externos. Las evaluaciones permiten medir el grado de confianza que merece o inspira un sistema de información.

Certificación

La evaluación puede llevar a una certificación o registro de la seguridad del sistema. En la práctica se certifican productos y se certifican sistemas de gestión de la seguridad. La certificación de productos es, de alguna forma, impersonal: “esto tiene estas características técnicas”. Sin embargo, la certificación de sistemas de gestión tiene que ver con el “componente humano” de las organizaciones buscando el análisis de cómo se explotan los sistemas[7].

Certificar es asegurar responsablemente y por escrito un comportamiento. Lo que se certifica, producto o sistema, se somete a una serie de evaluaciones orientadas por un objetivo ¿para qué lo quiere?[8]. Un certificado dice que un sistema es capaz de proteger unos datos de unas amenazas con una cierta calidad (capacidad de protección). Y lo dice en base a que ha observado la existencia y el funcionamiento de una serie de salvaguardas. Es decir que detrás de un certificado no hay sino los conceptos de un análisis de riesgos.

7 Hay vehículos con altas calificaciones técnicas y otros más humildes. Lo mismo que hay conductores que son verdaderos profesionales y otros de los que nunca nos explicaremos cómo es que están certificados como “aptos para el manejo de vehículos”. Lo ideal es poner un gran coche en manos de un gran conductor. De ahí para abajo, tenemos una gran variedad de situaciones de menor confianza: mayor riesgo de que algo vaya mal.

8 Y así tenemos sistemas aptos para “consumo humano” o “utilización en condiciones térmicas extremas”.

Antes de proceder a la certificación, debe haberse realizado un análisis de riesgos a fin de conocer los riesgos y de controlarlos mediante la adopción de los controles adecuados, además, será un punto de control de la gestión del producto o sistema.

Acreditación

Algunas certificaciones tienen como objetivo la acreditación del producto o sistema. La acreditación es un proceso específico cuyo objetivo es legitimar al sistema para formar parte de sistemas más amplios. Se puede ver como una certificación para un propósito específico.

Auditorías

Aunque no sea lo mismo, no están muy lejos de este mundo las auditorías, internas o externas, a las que se someten los sistemas de información

- unas veces requeridas por ley para poder operar en un cierto sector (cumplimiento),
- otras veces requeridas por la propia Dirección de la Organización,
- otras veces requeridas por entidades colaboradoras que ven su propio nivel de riesgo ligado al nuestro.

Una auditoría puede servirse de un análisis de riesgos que le permita (1) saber qué hay en juego, (2) saber a qué está expuesto el sistema y (3) valorar la eficacia y eficiencia de las salvaguardas.

Frecuentemente, los auditores parten de un análisis de riesgos, implícito o explícito, que, o bien realizan ellos mismos, o bien lo auditan. Siempre en la primera fase de la auditoría, pues es difícil opinar de lo que no se conoce. A partir del análisis de riesgos se puede analizar el sistema e informar a la gerencia de si el sistema está bajo control; es decir, si las medidas de seguridad adoptadas están justificadas, implantadas y monitorizadas, de forma que se puede confiar en el sistema de indicadores de que dispone la gerencia para gestionar la seguridad de los sistemas.

La conclusión de la auditoría es un informe de insuficiencias detectadas, que no son sino incoherencias entre las necesidades identificadas en el análisis de riesgos y la realidad detectada durante la inspección del sistema en operación.

> *El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas. [RD 1720/2007, artículo 96.2]*

En el caso de la Administración pública, existen algunos referentes fundamentales respecto de los cuales se puede y se debe realizar auditorías:

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. BOE de 29 de enero de 2010.

Las auditorías deben repetirse regularmente tanto para seguir la evolución del análisis de riesgos (que se debe actualizar regularmente) como para seguir el desarrollo del plan de seguridad determinado por las actividades de gestión de riesgos.

1.9. ¿Cuándo procede analizar y gestionar los riesgos?

Un análisis de riesgos TIC es recomendable en cualquier Organización que dependa de los sistemas de información y comunicaciones para el cumplimiento de su misión. En particular en cualquier entorno donde se practique la tramitación electrónica de bienes y servicios, sea en contexto público o privado. El análisis de riesgos permite tomar decisiones de gestión y asignar recursos con perspectiva, sean tecnológicos, humanos o financieros.

El análisis de riesgos es una herramienta de gestión que permite tomar decisiones. Las decisiones pueden tomarse antes de desplegar un servicio o con éste funcionando. Es muy deseable hacerlo antes, de forma que las medidas que haya que tomar se incorporen en el diseño del servicio, en la elección de componentes, en el desarrollo del sistema y en los manuales de usuario. Todo lo que sea corregir riesgos imprevistos es costoso en tiempo propio y ajeno, lo que puede ir en detrimento de la imagen prestada por la Organización y puede suponer, en último extremo, la pérdida de confianza en su capacidad. Siempre se ha dicho que es mejor prevenir que curar y aquí se aplica: no espere a que un servicio haga agua; hay que prever y estar prevenido.

Realizar un análisis de riesgos es laborioso y costoso. Levantar un mapa de activos y valorarlos requiere la colaboración de muchos perfiles dentro de la Organización, desde los niveles de gerencia hasta los técnicos. Y no solo es que haya que involucrar a muchas personas, sino que hay que lograr una uniformidad de criterio entre todos pues, si importante es cuantificar los riesgos, más importante aún es relativizarlos. Y esto es así porque típicamente en un análisis de riesgos aparecen multitud de datos. La única forma de afrontar la complejidad es centrarse en lo más importante (máximo impacto, máximo riesgo) y obviar lo que es secundario o incluso despreciable. Pero si los riesgos no están bien ordenados en términos relativos, su interpretación es imposible.

En resumen, que un análisis de riesgos no es una tarea menor que realiza cualquiera en sus ratos libres. Es una tarea mayor que requiere esfuerzo y coordinación. Por tanto debe ser planificada y justificada.

Certificación y acreditación

Si el sistema aspira a una certificación, el análisis de riesgos es un requisito previo que exigirá el evaluador. Es la fuente de información para determinar la relación de controles pertinentes para el sistema y que por tanto deben ser inspeccionados. Véase el apéndice 4.1 sobre certificación de sistemas de gestión de la seguridad de la información (SGSI).

El análisis de riesgos es así mismo un requisito exigido en los procesos de acreditación[9] de sistemas. Estos procesos son necesarios cuando se va a manejar en el sistema información clasificada nacional, UE, OTAN o de otros acuerdos internacionales. El primer paso del proceso es la realización del análisis de riesgos que identifique amenazas y salvaguardas y gestione satisfactoriamente los riesgos del sistema.

Por precepto legal

El análisis de riesgos puede venir requerido por precepto legal. Tal es el caso de 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. En el Capítulo II, Principios Básicos, se dice:

> Artículo 6. Gestión de la seguridad basada en los riesgos.
>
> 1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
> 2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

El mismo Real Decreto 3/2010, en el Capítulo III, Requisitos Mínimos, se dice:

> Artículo 13. Análisis y gestión de los riesgos.
>
> 1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información y las comunicaciones realizará su propia gestión de riesgos.
> 2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el Anexo II, se empleará alguna metodología reconocida internacionalmente.

9 En el sentido formal de autorización para manejar información clasificada. Los procesos de acreditación se ajustan a la normativa aplicable en cada caso.

3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, que en su Artículo 1, Objeto de la Ley, dice así:

2. Las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

La Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en su artículo 9 (Seguridad de los datos) dice así:

1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y *los riesgos a que están expuestos,* ya provengan de la acción humana o del medio físico o natural.

Por último, la gestión continua de los riesgos es uno de los principio básicos del Esquema Nacional de Seguridad, ya citado anteriormente.

En conclusión

Procede analizar y gestionar los riesgos cuando directa o indirectamente lo establezca un precepto legal y siempre que lo requiera la protección responsable de los activos de una organización.

2. Visión de conjunto

Hay dos grandes tareas a realizar:

I. análisis de riesgos,

que permite determinar qué tiene la Organización y estimar lo que podría pasar.

II. tratamiento de los riesgos,

que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume.

Ambas actividades, análisis y tratamiento se combinan en el proceso denominado **Gestión de Riesgos**.

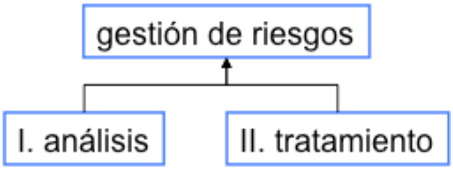

Ilustración 5. Gestión de riesgos

El análisis de riesgos considera los siguientes elementos:

1. activos, que son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización
2. amenazas, que son cosas que les pueden pasar a los activos causando un perjuicio a la Organización
3. salvaguardas (o contra medidas), que son medidas de protección desplegadas para que aquellas amenazas no causen [tanto] daño.

Con estos elementos se puede estimar:

1. el impacto: lo que podría pasar
2. el riesgo: lo que probablemente pase

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento y proceder a la fase de tratamiento.

Informalmente, se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión.

Formalmente, la gestión de los riesgos está estructurada de forma metódica en las normas ISO (ver Anexo 1). Se propone el siguiente esquema:

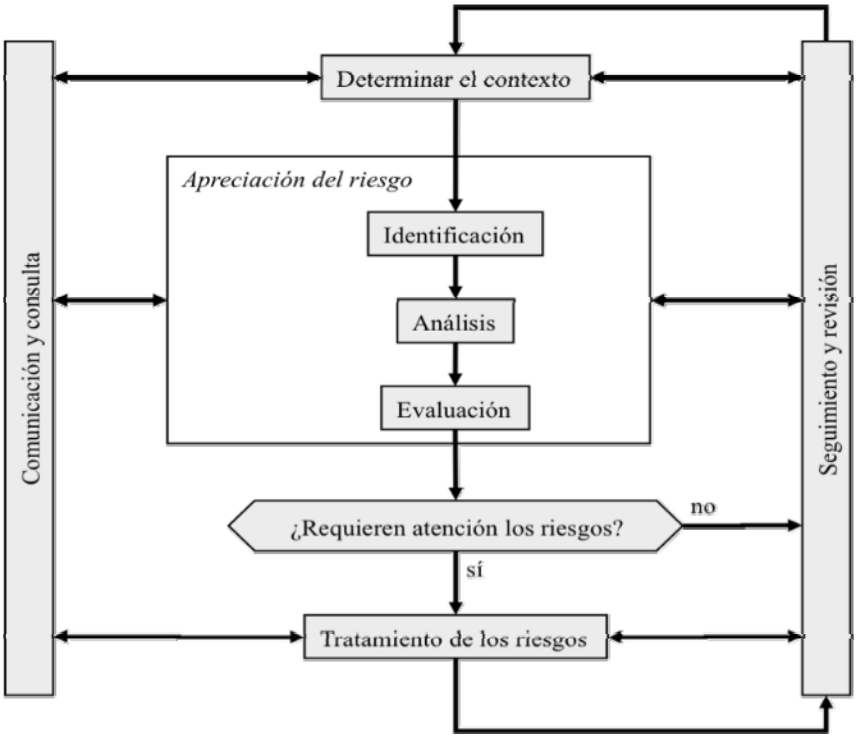

Ilustración 6. Proceso de gestión de riesgos (fuente: ISO 31000)

La **determinación del contexto** lleva a una determinación de los parámetros y condicionantes externos e internos que permiten encuadrar la política que se seguirá para gestionar los riesgos. Un elemento a destacar es el alcance del análisis, incluyendo obligaciones propias y obligaciones contraídas, así como las relaciones con otras organizaciones, sean para intercambio de información y servicios o proveedoras de servicios subcontratados. Véase la norma [ISO 31000] para un mayor desarrollo de los factores que determinan el contexto.

La **identificación de los riesgos** busca una relación de los posibles puntos de peligro. Lo que se identifique será analizado en la siguiente etapa. Lo que no se identifique quedará como riesgo oculto o ignorado.

El **análisis de los riesgos** busca calificar los riesgos identificados, bien cuantificando sus consecuencias (análisis cuantitativo), bien ordenando su importancia relativa (análisis cualitativo). De una u otra forma, como resultado del análisis tendremos una visión estructurada que nos permita centrarnos en lo más importante.

La **evaluación de los riesgos** va un paso más allá del análisis técnico y traduce las consecuencias a términos de negocio. Aquí entran factores de percepción, de estrategia y de política permitiendo tomar decisiones respecto de qué riesgos se aceptan y cuales no, así como de en qué circunstancias podemos aceptar un riesgo o trabajar en su tratamiento.

El **tratamiento de los riesgos** recopila las actividades encaminadas a modificar la situación de riesgo. Es una actividad que presenta numerosas opciones como veremos más adelante.

Comunicación y consulta. Es importante no olvidar nunca que los sistemas de información deben ser soporte de la productividad de la Organización. Es absurdo un sistema muy seguro pero que impide que la Organización alcance sus objetivos. Siempre hay que buscar un equilibrio entre seguridad y productividad y en ese equilibrio hay que contar con la colaboración de varios interlocutores:

- los usuarios cuyas necesidades deben ser tenidas en cuenta y a los que hay que informar para que colaboren activamente en la operación del sistema dentro de los parámetros de seguridad determinados por la Dirección
- los proveedores externos, a los que hay proporcionar instrucciones claras para poder exigirles tanto el cumplimiento de los niveles de servicio requeridos, como la gestión de los incidentes de seguridad que pudieran acaecer
- los órganos de gobierno para establecer canales de comunicación que consoliden la confianza de que el sistema de información responderá sin sorpresas para atender a la misión de la Organización y que los incidentes serán atajados de acuerdo el plan previsto

Seguimiento y revisión. Es importante no olvidar nunca que el análisis de riesgos es una actividad de despacho y que es imprescindible ver qué ocurre en la práctica y actuar en consecuencia, tanto reaccionando diligentemente a los incidentes, como mejorando continuamente nuestro conocimiento del sistema y de su entorno para mejorar el análisis y ajustarlo a la experiencia.

3. Método de análisis de riesgos

3.1. Conceptos paso a paso

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
2. determinar a qué amenazas están expuestos aquellos activos
3. determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
4. estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
5. estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza

Con el objeto de organizar la presentación, se introducen los conceptos de “impacto y riesgo potenciales” entre los pasos 2 y 3. Estas valoraciones son “teóricas”: en el caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas del paso 3, derivando estimaciones realistas de impacto y riesgo.

La siguiente figura recoge este primer recorrido, cuyos pasos se detallan en las siguientes secciones:

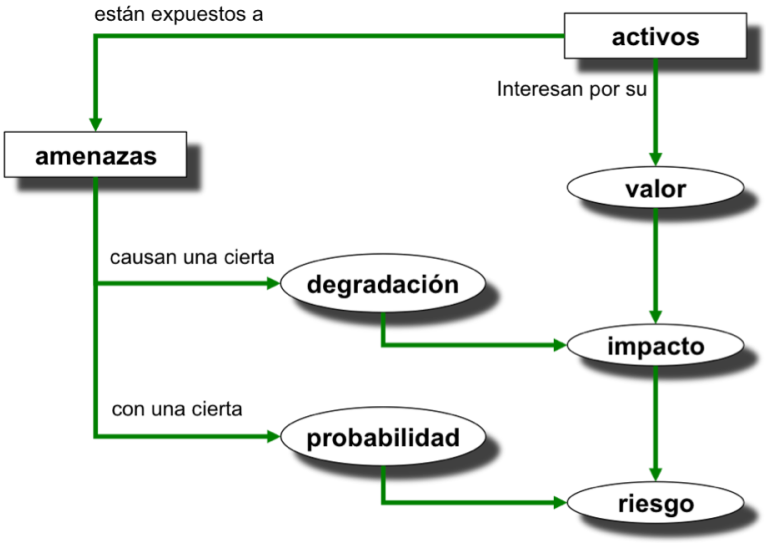

Ilustración 7. Elementos del análisis de riesgos potenciales

3.1.1. Paso 1: Activos

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008]

En un sistema de información hay 2 cosas esenciales:

- la **información** que maneja
- y los **servicios** que presta.

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.

Subordinados a dicha esencia se pueden identificar otros activos relevantes:

— **Datos** que materializan la información.

— **Servicios** auxiliares que se necesitan para poder organizar el sistema.

— **Las aplicaciones informáticas** *(software)* que permiten manejar los datos.

— **Los equipos informáti cos** *(hardware)* y que permiten hospedar datos, aplicaciones y servicios.

— **Los soportes de información** que son dispositivos de almacenamiento de datos.

— **El equipamiento auxiliar** que complementa el material informático.

— **Las redes de comunicaciones** que permiten intercambiar datos.

— **Las instalaciones** que acogen equipos informáticos y de comunicaciones.

— **Las personas** que explotan u operan todos los elementos anteriormente citados.

No todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y las salvaguardas son diferentes[10]. El capítulo 2 del "Catálogo de Elementos" presenta una relación de tipos de activos.

Dependencias

Los activos esenciales son la información y los servicios prestados; pero estos activos dependen de otros activos más prosaicos como pueden ser los equipos, las comunicaciones, las instalaciones y las frecuentemente olvidadas personas que trabajan con aquellos.

De manera que los activos vienen a formar árboles o grafos de dependencias donde la seguridad de los activos que se encuentran más arriba en la estructura o 'superiores' depende de los activos que se encuentran más abajo o 'inferiores'. Estas estructuras reflejan de arriba hacia abajo las dependencias, mientas que de abajo hacia arriba la propagación del daño caso de materializarse las amenazas.

Por ello aparece como importante el concepto de "dependencias entre activos" o la medida en que un activo *superior* se vería afectado por un incidente de seguridad en un activo *inferior*[11].

Se dice que un "activo superior" depende de otro "activo inferior" cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. O, dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior. Informalmente puede interpretarse que los activos inferiores son los pilares en los que se apoya la seguridad de los activos superiores.

Aunque en cada caso hay que adaptarse a la Organización objeto del análisis, con frecuencia se puede estructurar el conjunto de activos en capas, donde las capas superiores dependen de las inferiores:

- activos esenciales
    - información que se maneja
    - servicios prestados
- servicios internos
    - que estructuran ordenadamente el sistema de información
- el equipamiento informático
    - aplicaciones *(software)*

10 No se ataca ni se defiende de la misma manera un servicio telemático que un local de trabajo.

11 Un ejemplo puede ser mejor que mil palabras. Si se quema el local que hospeda los equipos, lo que no funciona es el servicio percibido por el usuario a kilómetros de distancia. Si roban el portátil de un ejecutivo con información estratégica de la Organización, lo que sufre es la confidencialidad de dicha información. Las instalaciones se reconstruyen; pero puede haberse pasado la oportunidad de prestar el servicio. El robo se subsana comprando otro portátil; pero el secreto ya está perdido.

    - equipos informáticos *(hardware)*
    - comunicaciones
    - soportes de información: discos, cintas, etc.
- el entorno: activos que se precisan para garantizar las siguientes capas
    - equipamiento y suministros: energía, climatización, etc.
    - mobiliario
- los servicios subcontratados a terceros
- las instalaciones físicas
- el personal
    - usuarios
    - operadores y administradores
    - desarrolladores

Valoración

¿Por qué interesa un activo? Por lo que vale.

No se está hablando de lo que cuestan las cosas, sino de lo que valen. Si algo no vale para nada, prescíndase de ello. Si no se puede prescindir impunemente de un activo, es que algo vale; eso es lo que hay que averiguar pues eso es lo que hay que proteger.

La valoración se puede ver desde la perspectiva de la '**necesidad de proteger'** pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes.

El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

El valor nuclear suele estar en la información que el si stema maneja y los servicios que se prestan (activos denominados esenciales), quedando los demás activos subordinados a las necesidades de explotación y protección de lo esencial.

Por otra parte, los sistemas de información explotan los datos para proporcionar servicios, internos a la Organización o destinados a terceros, apareciendo una serie de datos necesarios para prestar un servicio. Sin entrar en detalles técnicos de cómo se hacen las cosas, el conjunto de información y servicios esenciales permite caracterizar funcionalmente una organización. Las dependencias entre activos permiten relacionar los demás activos con datos y servicios.

Dimensiones

De un activo puede interesar calibrar diferentes dimensiones:

- su **confidencialidad**: ¿qué daño causaría que lo conociera quien no debe?

  Esta valoración es típica de datos.
- su **integridad**: ¿qué perjuicio causaría que estuviera dañado o corrupto?

  Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.
- su **disponibilidad**: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?

  Esta valoración es típica de los servicios[12].

12 Hay servicios finales que materializan la misión última de la Organización. Hay servicios internos de los que la Organización se sirve para estructurar su propia distribución de responsabilidades. Por último, hay servicios que se adquieren de otras organizaciones: suministros externos.

En sistemas dedicados a servicios de la sociedad de la información como puedan ser los de administración electrónica o comercio electrónico, el conocimiento de los actores es fundamental para poder prestar el servicio correctamente y poder perseguir los fallos (accidentales o deliberados) que pudieran darse. Así pues, en los activos esenciales, frecuentemente es útil valorar:

- la **autenticidad:** ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

  Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar)
- la **trazabilidad** del uso del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?
- la **trazabilidad** del acceso a los datos: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Se reconocen habitualmente como dimensiones básicas la confidencialidad, integridad y disponibilidad. En esta metodología se han añadido la autenticidad y el concepto de trazabilidad (del inglés, *accountability*), que a efectos técnicos se traducen en mantener la integridad y la confidencialidad de ciertos activos del sistema que pueden ser los servicios de directorio, las claves de firma digital, los registros de actividad, etc.

El capítulo 3 del "Catálogo de Elementos" presenta una relación de dimensiones de seguridad.

En un árbol de dependencias, donde los activos superiores dependen de los inferiores, es imprescindible valorar los activos superiores, los que son importantes por sí mismos. Automáticamente este valor se acumula en los inferiores, lo que no es óbice para que también puedan merecer, adicionalmente, su valoración propia.

¿Cuánto vale la "salud" de los activos?

Una vez determinadas qué dimensiones (de seguridad) interesan de un activo hay que proceder a valorarlo. La valoración es la determinación del coste que supondría recuperarse de una incidencia que destrozara el activo. Hay muchos factores a considerar:

- coste de reposición: adquisición e instalación
- coste de mano de obra (especializada) invertida en recuperar (el valor) del activo
- lucro cesante: pérdida de ingresos
- capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas
- sanciones por incumplimiento de la ley u obligaciones contractuales
- daño a otros activos, propios o ajenos
- daño a personas
- daños medioambientales

La valoración puede ser cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles). Los criterios más importantes a respetar son:

- la **homogeneidad**: es importante poder comparar valores aunque sean de diferentes dimensiones a fin de poder combinar valores propios y valores acumulados, así como poder determinar si es más grave el daño en una dimensión o en otra
- la **relatividad**: es importante poder relativizar el valor de un activo en comparación con otros activos

Ambos criterios se satisfacen con valoraciones económicas (coste dinerario requerido para "curar" el activo) y es frecuente la tentación de ponerle precio a todo. Si se consigue, excelente. Incluso es fácil ponerle precio a los aspectos más tangibles (equipamiento, horas de trabajo, etc.); pero al entrar en valoraciones más abstractas (intangibles como la credibilidad de la Organización) la valoración económica exacta puede ser escurridiza y motivo de agrias disputas entre expertos.

El capítulo 4 del "Catálogo de Elementos" presenta unas pautas para la valoración sistemática de activos.

Valoración cualitativa

Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como “órdenes de magnitud” y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo.

La limitación de las valoraciones cualitativas es que no permiten comparar valores más allá de su orden relativo. No se pueden sumar valores.

La "Guía de Técnicas" presenta un modelo de análisis basado en valoraciones cualitativas.

Valoración cuantitativa

Las valoraciones numéricas absolutas cuestan mucho esfuerzo; pero permiten sumar valores numéricos de forma absolutamente “natural”. La interpretación de las sumas no es nunca motivo de controversia.

Si la valoración es dineraria, además se pueden hacer estudios económicos comparando lo que se arriesga con lo que cuesta la solución respondiendo a las preguntas:

- ¿Vale la pena invertir tanto dinero en esta salvaguarda?
- ¿Qué conjunto de salvaguardas optimizan la inversión?
- ¿En qué plazo de tiempo se recupera la inversión?
- ¿Cuánto es razonable que cueste la prima de un seguro?

La "Guía de Técnicas" presenta un modelo de análisis basado en valoraciones cuantitativas.

El valor de la interrupción del servicio

Casi todas las dimensiones mencionadas anteriormente permiten una valoración simple, cualitativa o cuantitativa. Pero hay una excepción, la disponibilidad.

No es lo mismo interrumpir un servicio una hora o un día o un mes. Puede que una hora de detención sea irrelevante, mientras que un día sin servicio causa un daño moderado; pero un mes detenido suponga la terminación de la actividad. Y lo malo es que no existe proporcionalidad entre el tiempo de interrupción y las consecuencias.

En consecuencia, para valorar la [interrupción de la] disponibilidad de un activo hay que usar una estructura más compleja que se puede resumir en algún gráfico como el siguiente:

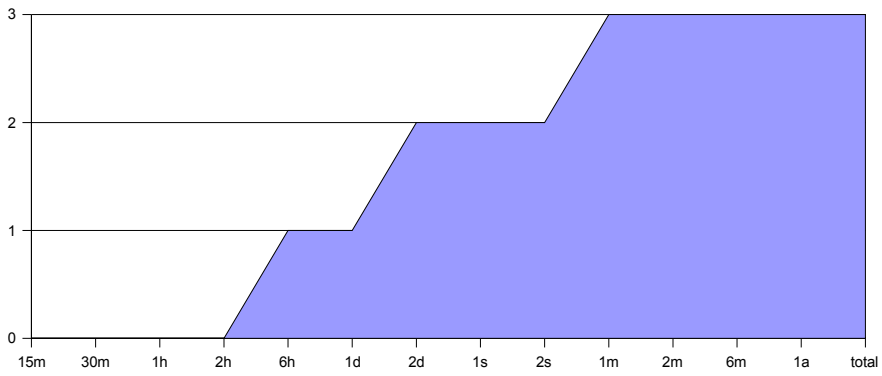

Ilustración 8. Coste de la [interrupción de la] disponibilidad

donde aparece una serie de escalones de interrupción que terminan con la destrucción total o permanente del activo. En el ejemplo anterior, paradas de hasta 6 horas se pueden asumir sin consecuencias. Pero a las 6 horas se disparan las alarmas que aumentan si la parada supera los 2 días. Y si la parada supera el mes, se puede decir que la Organización ha perdido su capacidad de operar: ha muerto. Desde el punto de vista de los remedios, la gráfica dice directamente que no

hay que gastarse ni un euro por evitar paradas de menos de 6 horas. Vale la pena un cierto gasto por impedir que una parada supere las 6 horas o los 2 días. Y cuando se valore lo que cuesta impedir que la parada supera el mes, hay que poner en la balanza todo el valor de la Organización frente al coste de las salvaguardas. Pudiera ser que no valiera la pena.

3.1.2. Paso 2: Amenazas

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.

Amenaza
Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008]

Identificación de las amenazas

El capítulo 5 del "Catálogo de Elementos" presenta una relación de amenazas típicas.

De origen natural

Hay accidentes naturales (terremotos, inundaciones, ...). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.

Del entorno (de origen industrial)

Hay desastres industriales (contaminación, fallos eléctricos, ...) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.

Defectos de las aplicaciones

Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, ‘vulnerabilidades’[13].

Causadas por las personas de forma accidental

Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

Causadas por las personas de forma deliberada

Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

No todas las amenazas afectan a todos los activos[14], sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

Valoración de las amenazas

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

[13] Estos defectos se clasifican habitualmente bajo la taxonomía conocida como CVE *(Common Vulnerability Enumeration),* una norma internacional de facto. La mayor parte de estos defectos suelen afectar a aplicaciones *software*.

[14] Las instalaciones pueden incendiarse; pero las aplicaciones, no. Las personas pueden ser objeto de un ataque bacteriológico; pero los servicios, no. Sin embargo, los virus informáticos afectan a las aplicaciones, no a las personas.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos:

degradación: cuán perjudicado resultaría el [valor del] activo

probabilidad: cuán probable o improbable es que se materialice la amenaza

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera.

La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto "totalmente degradado", o "degradado en una pequeña fracción". Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

La probabilidad de ocurrencia es más compleja de determinar y de expresar. A veces se modela cualitativamente por medio de alguna escala nominal:

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Tabla 1. Degradación del valor

A veces se modela numéricamente como una frecuencia de ocurrencia. Es habitual usar 1 año como referencia, de forma que se recurre a la tasa anual de ocurrencia[15] como medida de la probabilidad de que algo ocurra. Son valores típicos:

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Tabla 2. Probabilidad de ocurrencia

3.1.3. Determinación del impacto potencial

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema se centre en la información que maneja y los servicios que presta; pero las amenazas suelen materializarse en los medios. Para enlazar unos con otros recurriremos al grafo de dependencias.

Impacto acumulado

Es el calculado sobre un activo teniendo en cuenta

- su valor acumulado (el propio mas el acumulado de los activos que dependen de él)
- las amenazas a que está expuesto

[15] ARO – Annual Rate of Occurrence.

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada.

El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo.

El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.

El impacto acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

Impacto repercutido

Es el calculado sobre un activo teniendo en cuenta

- su valor propio
- las amenazas a que están expuestos los activos de los que depende

El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada.

El impacto es tanto mayor cuanto mayor es el valor propio de un activo.

El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.

El impacto es tanto mayor cuanto mayor sea la dependencia del activo atacado.

El impacto repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Agregación de valores de impacto

Los párrafos anteriores determinan el impacto que sobre un activo tendría una amenaza en una cierta dimensión. Estos impactos singulares pueden agregarse bajo ciertas condiciones:

- puede agregarse el impacto repercutido sobre diferentes activos,
- puede agregarse el impacto acumulado sobre activos que no sean dependientes entre sí, y no hereden valor de un activo superior común,
- no debe agregarse el impacto acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el impacto al incluir varias veces el valor acumulado de activos superiores,
- puede agregarse el impacto de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes,
- puede agregarse el impacto de una amenaza en diferentes dimensiones.

3.1.4. Determinación del riesgo potencial

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 a 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

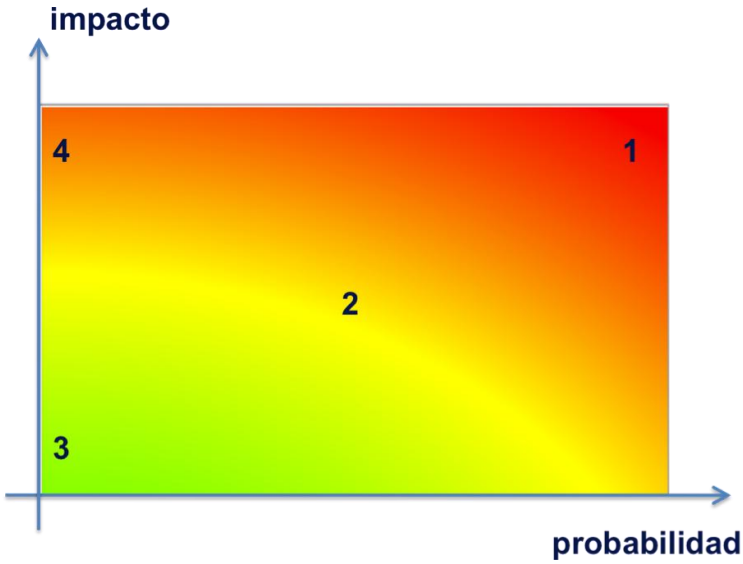

Ilustración 9. El riesgo en función del impacto y la probabilidad

Riesgo acumulado

Es el calculado sobre un activo teniendo en cuenta

- el impacto acumulado sobre un activo debido a una amenaza y
- la probabilidad de la amenaza

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la probabilidad de la amenaza.

El riesgo acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

Riesgo repercutido

Es el calculado sobre un activo teniendo en cuenta

- el impacto repercutido sobre un activo debido a una amenaza y
- la probabilidad de la amenaza

El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la probabilidad de la amenaza.

El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Agregación de riesgos

Los párrafos anteriores determinan el riesgo que sobre un activo tendría una amenaza en una cierta dimensión. Estos riesgos singulares pueden agregarse bajo ciertas condiciones:

- puede agregarse el riesgo repercutido sobre diferentes activos,
- puede agregarse el impacto acumulado sobre activos que no sean dependientes entre sí, y no hereden valor de un activo superior común,

- no debe agregarse el riesgo acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el riesgo al incluir varias veces el valor acumulado de activos superiores,
- puede agregarse el riesgo de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes,
- puede agregarse el riesgo de una amenaza en diferentes dimensiones.

3.1.5. Paso 3: Salvaguardas

En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto. En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otras seguridad física y, por último, está la política de personal.

El capítulo 6 del "Catálogo de Elementos" presenta una relación de salvaguardas adecuadas para cada tipo de activos.

Selección de salvaguardas

Ante el amplio abanico de posibles salvaguardas a considerar, es necesario hacer una criba inicial para quedarnos con aquellas que son relevantes para lo que hay que proteger. En esta criba se deben tener en cuenta los siguientes aspectos:

1. tipo de activos a proteger, pues cada tipo se protege de una forma específica
2. dimensión o dimensiones de seguridad que requieren protección
3. amenazas de las que necesitamos protegernos
4. si existen salvaguardas alternativas

Además, es prudente establecer un principio de proporcionalidad y tener en cuenta:

1. el mayor o menor valor propio o acumulado sobre un activo, centrándonos en lo más valioso y obviando lo irrelevante
2. la mayor o menor probabilidad de que una amenaza ocurra, centrándonos en los riesgos más importantes (ver zonas de riesgo)
3. la cobertura del riesgo que proporcionan salvaguardas alternativas

Esto lleva a dos tipos de declaraciones para excluir una cierta salvaguarda del conjunto de las que conviene analizar:

- **no aplica** – se dice cuando una salvaguarda no es de aplicación porque técnicamente no es adecuada al tipo de activos a proteger, no protege la dimensión necesaria o no protege frente a la amenaza en consideración
- **no se justifica** – se dice cuando la salvaguarda aplica, pero es desproporcionada al riesgo que tenemos que proteger

Como resultado de estas consideraciones dispondremos de una **“declaración de aplicabilidad”** o relación de salvaguardas que deben ser analizadas como componentes nuestro sistema de protección.

Efecto de las salvaguardas

Las salvaguardas entran en el cálculo del riesgo de dos formas:

Reduciendo la probabilidad de las amenazas.

Se llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice.

Limitando el daño causado.

Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.

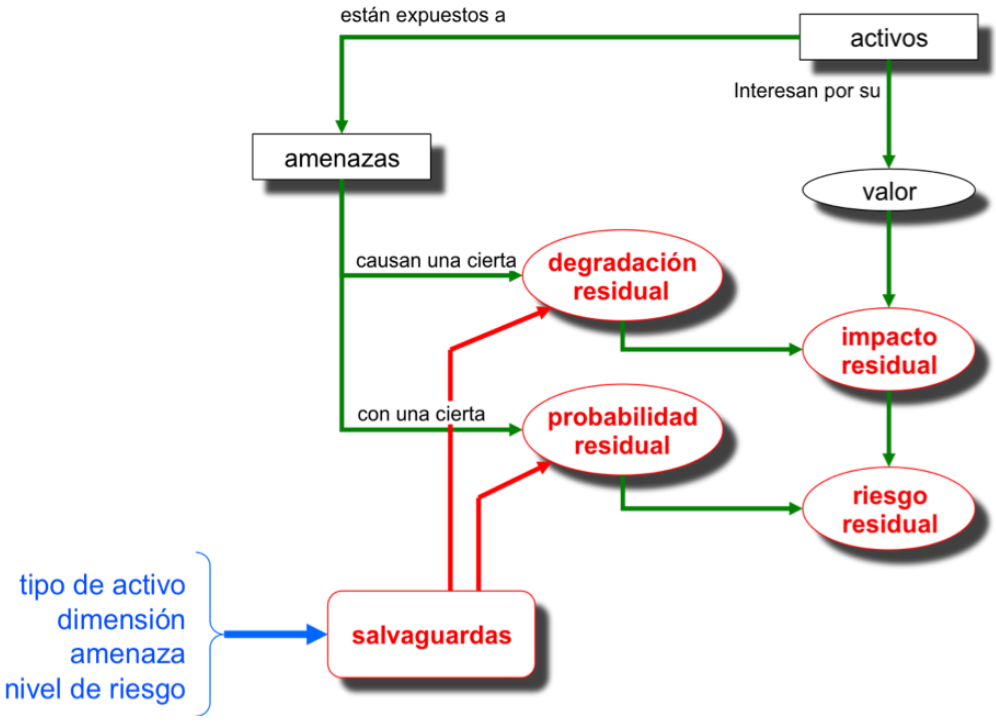

Ilustración 10. Elementos de análisis del riesgo residual

Tipo de protección

Esta aproximación a veces resulta un poco simplificadora, pues es habitual hablar de diferentes tipos de protección prestados por las salvaguardas:

[PR] prevención

Diremos que una salvaguarda es preventiva cuando reduce las oportunidades de que un incidente ocurra. Si la salvaguarda falla y el incidente llega a ocurrir, los daños son los mismos.

Ejemplos: autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, metodología segura de desarrollo de software, pruebas en pre-producción, segregación de tareas, ...

[DR] disuasión

Diremos que una salvaguarda es disuasoria cuando tiene un efecto tal sobre los atacantes que estos no se atreven o se lo piensan dos veces antes de atacar. Son salvaguardas que actúan antes del incidente, reduciendo las probabilidades de que ocurra; pero que no tienen influencia sobre los daños causados caso de que el atacante realmente se atreva.

Ejemplos: vallas elevadas, guardias de seguridad, avisos sobre la persecución del delito o persecución del delincuente, ...

[EL] eliminación

Diremos que una salvaguarda elimina un incidente cuando impide que éste tenga lugar. Son salvaguardas que actúan antes de que el incidente se haya producido. No reducen los daños caso de que la salvaguarda no sea perfecta y el incidente llegue a ocurrir.

Ejemplos: eliminación de cuentas estándar, de cuentas sin contraseña, de servicios innecesarios, …; en general, todo lo que tenga que ver con la fortificación o bastionado, ..., cifrado de la información, ..., armarios ignífugos, ...

[IM] minimización del impacto / limitación del impacto

Se dice que una salvaguarda minimiza o limita el impacto cuando acota las consecuencias de un incidente.

Ejemplos: desconexión de redes o equipos en caso de ataque, detención de servicios en caso de ataque, seguros de cobertura, cumplimiento de la legislación vigente

[CR] corrección

Diremos que una salvaguarda es correctiva cuando, habiéndose producido un daño, lo repara. Son salvaguardas que actúan después de que el incidente se haya producido y por tanto reducen los daños.

Véase: recuperación más abajo.

Ejemplos: gestión de incidentes, líneas de comunicación alternativas, fuentes de alimentación redundantes, ...

[RC] recuperación

Diremos que una salvaguarda ofrece recuperación cuando permite regresar al estado anterior al incidente. Son salvaguardas que no reducen las probabilidades del incidente, pero acotan los daños a un periodo de tiempo.

Ejemplos: copias de seguridad (back-up)

[MN] monitorización

Son las salvaguardas que trabajan monitorizando lo que está ocurriendo o lo que ha ocurrido. Si se detectan cosas en tiempo real, podemos reaccionar atajando el incidente para limitar el impacto; si se detectan cosas a posteriori, podemos aprender del incidente y mejorar el sistema de salvaguardas de cara al futuro.

Ejemplos: registros de actividad, registro de descargas de web, ...

[DC] detección

Diremos que una salvaguarda funciona detectando un ataque cuando informa de que el ataque está ocurriendo. Aunque no impide el ataque, sí permite que entren en operación otras medidas que atajen la progresión del ataque, minimizando daños.

Ejemplos: anti-virus, IDS, detectores de incendio, ...

[AW] concienciación

Son las actividades de formación de las personas anexas al sistema que pueden tener una influencia sobre él. La formación reduce los errores de los usuarios, lo cual tiene un efecto preventivo. También mejora las salvaguardas de todo tipo pues los que las operan lo hacen con eficacia y rapidez, potenciando su efecto o, al menos, no menoscabándolo por una mala operación.

Ejemplos: cursos de concienciación, cursos de formación, ...

[AD] administración

Se refiere a las salvaguardas relacionadas con los componentes de seguridad del sistema. Una buena administración evita el desconocimiento de lo que hay y por tanto impide que

hayan puertas desconocidas por las que pudiera tener éxito un ataque. En general pueden considerarse medidas de tipo preventivo.

Ejemplos: inventario de activos, análisis de riesgos, plan de continuidad, ...

La siguiente tabla relaciona cada uno de estos tipos de protección con el modelo anterior de reducción de la degradación y de la probabilidad:

efecto	tipo
preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Tabla 3. Tipos de salvaguardas

Eficacia de la protección

Las salvaguardas se caracterizan, además de por su existencia, por su eficacia frente al riesgo que pretenden conjurar. La salvaguarda ideal es 100% eficaz, eficacia que combina 2 factores:

desde el punto de vista técnico

- es técnicamente idónea para enfrentarse al riesgo que protege
- se emplea siempre

desde el punto de vista de operación de la salvaguarda

- está perfectamente desplegada, configurada y mantenida
- existen procedimientos claros de uso normal y en caso de incidencias
- los usuarios están formados y concienciados
- existen controles que avisan de posibles fallos

Entre una eficacia del 0% para aquellas que faltan y el 100% para aquellas que son idóneas y que están perfectamente implantadas, se estimará un grado de eficacia real en cada caso concreto. Para medir los aspectos organizativos, se puede emplear una escala de madurez que recoja en forma de factor corrector la confianza que merece el proceso de gestión de la salvaguarda:

factor	nivel	significado
0%	**L0**	inexistente
	L1	inicial / ad hoc
	L2	reproducible, pero intuitivo
	L3	proceso definido
	L4	gestionado y medible
100%	**L5**	optimizado

Tabla 4. Eficacia y madurez de las salvaguardas

Vulnerabilidades

Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial.

Traducido a los términos empleados en los párrafos anteriores, son vulnerabilidades todas las ausencias o ineficacias de las salvaguardas pertinentes para salvaguardar el valor propio o acumulado sobre un activo. A veces se emplea el término “insuficiencia” para resaltar el hecho de que la eficacia medida de la salvaguarda es insuficiente para preservar el valor del activo expuesto a una amenaza.

3.1.6. Paso 4: impacto residual

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual.

El cálculo del impacto residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación.

La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

3.1.7. Paso 5: riesgo residual

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual.

El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la probabilidad de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia.

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual.

La magnitud de la probabilidad residual tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

3.2. Formalización de las actividades

Este conjunto de actividades tiene los siguientes objetivos:

- Levantar un modelo del valor del sistema, identificando y valorando los activos relevantes.
- Levantar un mapa de riesgos del sistema, identificando y valorando las amenazas sobre aquellos activos.
- Levantar un conocimiento de la situación actual de salvaguardas.
- Evaluar el impacto posible sobre el sistema en estudio, tanto el impacto potencial (sin salvaguardas), como el impacto residual (incluyendo el efecto de las salvaguardas desplegadas para proteger el sistema).
- Evaluar el riesgo del sistema en estudio, tanto el riesgo potencial (sin salvaguardas), como el riesgo residual (incluyendo el efecto de las salvaguardas desplegadas para proteger el sistema).

- Informar de las áreas del sistema con mayor impacto y/o riesgo a fin de que se puedan tomar las decisiones de tratamiento con motivo justificado.

El análisis de los riesgos se lleva a cabo por medio de las siguientes tareas:

MAR – Método de Análisis de Riesgos
MAR.1 – Caracterización de los activos
MAR.11 – Identificación de los activos
MAR.12 – Dependencias entre activos
MAR.13 – Valoración de los activos
MAR.2 – Caracterización de las amenazas
MAR.21 – Identificación de las amenazas
MAR.22 – Valoración de las amenazas
MAR.3 – Caracterización de las salvaguardas
MAR.31 – Identificación de las salvaguardas pertinentes
MAR.32 – Valoración de las salvaguardas
MAR.4 – Estimación del estado de riesgo
MAR.41 – Estimación del impacto
MAR.42 – Estimación del riesgo

MAR.1: Caracterización de los activos

Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia.

El resultado de esta actividad es el informe denominado “modelo de valor”.

Sub-tareas:

Tarea MAR.11: Identificación de los activos

Tarea MAR.12: Dependencias entre activos

Tarea MAR.13: Valoración de los activos

MAR.2: Caracterización de las amenazas

Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación).

El resultado de esta actividad es el informe denominado “mapa de riesgos”.

Sub-tareas:

Tarea MAR.21: Identificación de las amenazas

Tarea MAR.22: Valoración de las amenazas

MAR.3: Caracterización de las salvaguardas

Esta actividad busca identificar las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que pretenden mitigar.

El resultado de esta actividad se concreta en varios informes:

— declaración de aplicabilidad

— evaluación de salvaguardas

— insuficiencias (o vulnerabilidades del sistema de protección)

Sub-tareas:

Tarea MAR.31: Identificación de las salvaguardas pertinentes

Tarea MAR.32: Valoración de las salvaguardas

MAR.4: Estimación del estado de riesgo

Esta actividad procesa todos los datos recopilados en las actividades anteriores para

- realizar un informe del estado de riesgo: estimación de impacto y riesgo
- realizar un informe de insuficiencias: deficiencias o debilidades en el sistema de salvaguardas

Sub-tareas:

Tarea MAR.41: Estimación del impacto

Tarea MAR.42: Estimación del riesgo

Es frecuente que las tareas relacionadas con los activos (MAR.1) se realicen concurrentemente con las tareas relacionadas con las amenazas sobre dichos activos (MAR.2) e identificación de las salvaguardas actuales (MAR.3), simplemente porque suelen coincidir las personas y es difícil que el interlocutor no tienda de forma natural a tratar cada activo “verticalmente”, viendo todo lo que le afecta antes de pasar al siguiente.

3.2.1. Tarea MAR.1: Caracterización de los activos

Esta actividad consta de tres sub-tareas:

MAR.11: Identificación de los activos

MAR.12: Dependencias entre activos

MAR.13: Valoración de los activos

El objetivo de estas tareas es reconocer los activos que componen el sistema, definir las dependencias entre ellos, y determinar que parte del valor del sistema se soporta en cada activo. Podemos resumirlo en la expresión “conócete a ti mismo”.

MAR: Análisis de riesgos ***MAR.1: Caracterización de los activos*** ***MAR.11: Identificación de los activos***
Objetivos • Identificar los activos que componen el sistema, determinando sus características, atributos y clasificación en los tipos determinados
Productos de entrada • Inventario de datos manejados por el sistema • Inventario de servicios prestados por el sistema • Procesos de negocio • Diagramas de uso • Diagramas de flujo de datos • Inventarios de equipamiento lógico • Inventarios de equipamiento físico • Locales y sedes de la Organización • Caracterización funcional de los puestos de trabajo

MAR: Análisis de riesgos ***MAR.1: Caracterización de los activos*** ***MAR.11: Identificación de los activos***
Productos de salida • Relación de activos a considerar • Caracterización de los activos: valor propio y acumulado • Relaciones entre activos
Técnicas, prácticas y pautas • Ver “Libro II – Catálogo”. • Diagramas de flujo de datos • Diagramas de procesos • Entrevistas (ver "Guía de Técnicas") • Reuniones

Esta tarea es crítica. Una buena identificación es importante desde varios puntos de vista:

- materializa con precisión el alcance del proyecto
- permite las interlocución con los grupos de usuarios: todos hablan el mismo lenguaje
- permite determinar las dependencias precisas entre activos
- permite valorar los activos con precisión
- permite identificar y valorar las amenazas con precisión
- permite determinar qué salvaguardas serán necesarias para proteger el sistema

Caracterización de los activos

Para cada activo hay que determinar una serie de características que lo definen:

- código, típicamente procedente del inventario
- nombre (corto)
- descripción (larga)
- tipo (o tipos) que caracterizan el activo
- unidad responsable. A veces hay más de una unidad. Por ejemplo, en el caso de aplicaciones cabe diferenciar entre la unidad que la mantiene y la que la explota.
- persona responsable. Especialmente relevante en el caso de datos. A veces hay más de un responsable. Por ejemplo en caso de datos de carácter personal cabe diferenciar entre el responsable del dato y el operador u operadores que lo manejan.
- ubicación, técnica (en activos intangibles) o geográfica (en activos materiales)
- cantidad, si procede como puede ser en el caso de la informática personal (por ejemplo 350 equipos de sobremesa)
- otras características específicas del tipo de activo

MAR: Análisis de riesgos
MAR.1: Caracterización de los activos
MAR.12: Dependencias entre activos

Objetivos
- Identificar y valorar las dependencias entre activos, es decir la medida en que un activo de orden superior se puede ver perjudicado por una amenaza materializada sobre un activo de orden inferior

Productos de entrada
- Resultados de la tarea T1.2.1, Identificación
- Procesos de negocio
- Diagramas de flujo de datos
- Diagramas de uso

Productos de salida
- Diagrama de dependencias entre activos

Técnicas, prácticas y pautas
- Diagramas de flujo de datos
- Diagramas de procesos
- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- Valoración Delphi (ver "Guía de Técnicas")

Para cada dependencia conviene registrar la siguiente información:

- estimación del grado de dependencia: hasta un 100%
- explicación de la valoración de la dependencia
- entrevistas realizadas de las que se ha deducido la anterior estimación

MAR: Análisis de riesgos
MAR.1: Caracterización de los activos
MAR.13: Valoración de los activos

Objetivos
- Identificar en qué dimensión es valioso el activo
- Valorar el coste que para la Organización supondría la destrucción del activo

Productos de entrada
- Resultados de la tarea MAR.11, Identificación de los activos
- Resultados de la tarea MAR.12, Dependencias entre activos

Productos de salida
- **Modelo de valor**: informe de valor de los activos

Técnicas, prácticas y pautas
- Ver “Libro II – Catálogo”.
- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- Valoración Delphi (ver "Guía de Técnicas")

Para la adquisición de este conocimiento puede ser necesario entrevistar a diferentes colectivos dentro de la Organización:

- dirección o gerencia, que conocen las consecuencias para la misión de la Organización
- responsables de los datos, que conocen las consecuencias de sus fallos de seguridad
- responsables de los servicios, que conocen las consecuencias de la no prestación del servicio o de su prestación degradada
- responsables de sistemas de información y responsables de operación, que conocen las consecuencias de un incidente

Para cada valoración conviene registrar la siguiente información:

- dimensiones en las que el activo es relevante
- estimación de la valoración en cada dimensión
- explicación de la valoración
- entrevistas realizadas de las que se han deducido las anteriores estimaciones

3.2.2. Tarea MAR.2: Caracterización de las amenazas

Esta actividad consta de dos sub-tareas:

MAR.21: Identificación de las amenazas

MAR.22: Valoración de las amenazas

El objetivo de estas tareas es caracterizar el entorno al que se enfrenta el sistema, qué puede pasar, qué consecuencias se derivarían y cómo de probable es que pase. Podemos resumirlo en la expresión “conoce a tu enemigo”.

MAR: Análisis de riesgos ***MAR.2: Caracterización de las amenazas*** ***MAR.21: Identificación de las amenazas***
Objetivos • Identificar las amenazas relevantes sobre cada activo
Productos de entrada • Resultados de la actividad MAR.1, Caracterización de los activos • Informes relativos a defectos en los productos. Esto es, informes de vulnerabilidades.
Productos de salida • Relación de amenazas posibles
Técnicas, prácticas y pautas • Catálogos de amenazas (ver "Catálogo de Elementos") • Árboles de ataque (ver "Guía de Técnicas") • Entrevistas (ver "Guía de Técnicas") • Reuniones • Valoración Delphi (ver "Guía de Técnicas")

En esta tarea se identifican las amenazas significativas sobre los activos identificados, tomando en consideración:

- el tipo de activo
- las dimensiones en que el activo es valioso
- la experiencia de la Organización
- los defectos reportados por los fabricantes y organismos de respuesta a incidentes de seguridad (CERTS)

Para cada amenaza sobre cada activo conviene registrar la siguiente información:

- explicación del efecto de la amenaza
- entrevistas realizadas de las que se ha deducido la anterior estimación
- antecedentes, si los hubiera, bien en la propia Organización, bien en otras organizaciones que se haya considerado relevantes

MAR: Análisis de riesgos
MAR.2: Caracterización de las amenazas
MAR.22: Valoración de las amenazas

Objetivos

- Estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo
- Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse

Productos de entrada

- Resultados de la tarea MAR2.1, Identificación de las amenazas
- Series históricas de incidentes
- Informes de defectos en los productos
- Antecedentes: incidentes en la Organización

Productos de salida

- **Mapa de riesgos**: informe de amenazas posibles, caracterizadas por su frecuencia de ocurrencia y la degradación que causarían en los activos

Técnicas, prácticas y pautas

- Árboles de ataque (ver "Guía de Técnicas")
- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- Valoración Delphi (ver "Guía de Técnicas")

En esta tarea se valoran las amenazas identificadas en la tarea anterior, tomando en consideración:

- la experiencia (historia) universal
- la experiencia (historia) del sector de actividad
- la experiencia (historia) del entorno en que se ubican los sistemas
- la experiencia (historia) de la propia Organización
- los informes anexos a los reportes de defectos proporcionados por los fabricantes y organismos de respuesta a incidentes de seguridad (CERTS)

Sabiendo que existen una serie de posibles agravantes, como se describe en la sección X.

Para cada amenaza sobre cada activo conviene registrar la siguiente información:

- estimación de la frecuencia de la amenaza
- estimación del daño (degradación) que causaría su materialización
- explicación de las estimaciones de frecuencia y degradación
- entrevistas realizadas de las que se han deducido las anteriores estimaciones

3.2.3. Tarea MAR.3: Caracterización de las salvaguardas

Esta actividad consta de dos sub-tareas:

MAR.31: Identificación de las salvaguardas pertinentes

MAR.32: Valoración de las salvaguardas

El objetivo de estas tareas es doble: saber qué necesitamos para proteger el sistema y saber si tenemos un sistema de protección a la altura de nuestras necesidades.

MAR: Análisis de riesgos ***MAR.3: Caracterización de las salvaguardas*** ***MAR.31: Identificación de las salvaguardas pertinentes***
Objetivos • Identificar las salvaguardas convenientes para proteger el sistema
Productos de entrada • modelo de activos del sistema • modelo de amenazas del sistema • indicadores de impacto y riesgo residual • informes de productos y servicios en el mercado
Productos de salida • Declaración de aplicabilidad: relación justificada de las salvaguardas necesarias • Relación de salvaguardas desplegadas
Técnicas, prácticas y pautas • Catálogos de salvaguardas (ver "Catálogo de Elementos") • Árboles de ataque (ver "Guía de Técnicas") • Entrevistas (ver "Guía de Técnicas") • Reuniones

Para cada salvaguarda conviene registrar la siguiente información:

- descripción de la salvaguarda y su estado de implantación
- descripción de las amenazas a las que pretende hacer frente
- entrevistas realizadas de las que se ha deducido la anterior información

Para determinar las salvaguardas pertinentes es frecuente recurrir a catálogos de salvaguardas o al consejo de personas expertas. De una u otra forma dispondremos de una colección de salvaguardas para elegir, de forma que el complejo problema de encontrar lo que necesitamos se reduce al problema más sencillo de descartar lo que no necesitamos.

En el proceso de descarte hay varias razones para eliminar una salvaguarda propuesta:

- porque no es apropiada para el activo que necesitamos defender
- porque no es apropiada para la dimensión de seguridad que necesitamos defender
- porque no es efectiva oponiéndose a la amenaza que necesitamos contrarrestar
- porque es excesiva para el valor que tenemos que proteger (desproporcionada)
- porque disponemos de medidas alternativas

MAR: Análisis de riesgos
MAR.3: Caracterización de las salvaguardas
MAR.32: Valoración de las salvaguardas

Objetivos

- Determinar la eficacia de las salvaguardas pertinentes

Productos de entrada

- Inventario de salvaguardas derivado de la tarea MAR.31

Productos de salida

- **Evaluación de salvaguardas** : informe de salvaguardas desplegadas, caracterizadas por su grado de efectividad
- **Informe de insuficien cias (o vul nerabilidades)**: relación de salvaguardas que deberían estar pero no están desplegadas o están desplegadas de forma insuficiente

Técnicas, prácticas y pautas

- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- Valoración Delphi (ver "Guía de Técnicas")

En esta tarea se valora la efectividad de las salvaguardas identificadas en la tarea anterior, tomando en consideración:

- la idoneidad de la salvaguarda para el fin perseguido
- la calidad de la implantación
- la formación de los responsables de su configuración y operación
- la formación de los usuarios, si tienen un papel activo
- la existencia de controles de medida de su efectividad
- la existencia de procedimientos de revisión regular

Para cada salvaguarda conviene registrar la siguiente información:

- estimación de su eficacia para afrontar aquellas amenazas
- explicación de la estimación de eficacia
- entrevistas realizadas de las que se ha deducido la anterior estimación

3.2.4. Tarea MAR.4: Estimación del estado de riesgo

En esta tarea se combinan los descubrimientos de las tareas anteriores (MAR.1, MAR.2 y MAR.3) para derivar estimaciones del estado de riesgo de la Organización.

Esta actividad consta de tres tareas:

MAR.41: Estimación del impacto

MAR.42: Estimación del riesgo

El objetivo de estas tareas es disponer de una estimación fundada de lo que puede ocurrir (impacto) y de lo que probablemente ocurra (riesgo).

MAR: Análisis de riesgos
MAR.4: Estimación del estado de riesgo
MAR.41: Estimación del impacto

Objetivos
- Determinar el impacto potencial al que está sometido el sistema
- Determinar el impacto residual al que está sometido el sistema

Productos de entrada
- Resultados de la actividad MAR.1, Caracterización de los activos
- Resultados de la actividad MAR.2, Caracterización de las amenazas
- Resultados de la actividad MAR.3, Caracterización de las salvaguardas

Productos de salida
- Informe de impacto (potencial) por activo
- Informe de impacto residual por activo

Técnicas, prácticas y pautas
- Análisis mediante tablas (ver "Guía de Técnicas")
- Análisis algorítmico (ver "Guía de Técnicas")

En esta tarea se estima el impacto al que están expuestos los activos del sistema:

- el impacto potencial, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas
- el impacto residual, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas

MAR: Análisis de riesgos
MAR.4: Estimación del estado de riesgo
MAR.42: Estimación del riesgo

Objetivos
- Determinar el riesgo potencial al que está sometido el sistema
- Determinar el riesgo residual al que está sometido el sistema

Productos de entrada
- Resultados de la actividad MAR.1, Caracterización de los activos
- Resultados de la actividad MAR.2, Caracterización de las amenazas
- Resultados de la actividad MAR.3, Caracterización de las salvaguardas
- Resultados de la actividad MAR.4, Estimaciones de impacto

MAR: Análisis de riesgos *MAR.4: Estimación del estado de riesgo* *MAR.42: Estimación del riesgo*
Productos de salida • Informe de riesgo (potencial) por activo • Informe de riesgo residual por activo
Técnicas, prácticas y pautas • Análisis mediante tablas (ver "Guía de Técnicas") • Análisis algorítmico (ver "Guía de Técnicas")

En esta tarea se estima el riesgo al que están sometidos los activos del sistema:

- el riesgo potencial, al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas
- el riesgo residual, al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas

3.3. Documentación

Documentación intermedia

- Resultados de las entrevistas.
- Documentación de otras fuentes: estadísticas, observaciones de expertos y observaciones de los analistas.
- Información existente utilizable por el proyecto (por ejemplo inventario de activos)
- Documentación auxiliar: planos, organigramas, requisitos, especificaciones, análisis funcionales, cuadernos de carga, manuales de usuario, manuales de explotación, diagramas de flujo de información y de procesos, modelos de datos, etc.
- Informes y evaluaciones de defectos de los productos, procedentes de fabricantes o de centros de respuesta a incidentes de seguridad (CERTs).

Documentación final

- **Modelo de valor**

  Informe que detalla los activos, sus dependencias, las dimensiones en las que son valiosos y la estimación de su valor en cada dimensión.

- **Mapa de riesgos**:

  Informe que detalla las amenazas significativas sobre cada activo, caracterizándolas por su frecuencia de ocurrencia y por la degradación que causaría su materialización sobre el activo.

- **Declaración de aplicabilidad:**

  Informe que recoge las contramedidas que se consideran apropiadas para defender el sistema de información bajo estudio.

- **Evaluación de salvaguardas:**

  Informe que detalla las salvaguardas existentes calificándolas en su eficacia para reducir el riesgo que afrontan.

- **Informe de insuficiencias o vulnerabilidades:**

  Informe que detalla las salvaguardas necesarias pero ausentes o insuficientemente eficaces.

- **Estado de riesgo:**

  Informe que detalla para cada activo el impacto y el riesgo, potenciales y residuales, frente a cada amenaza.

Esta documentación es un fiel reflejo del estado de riesgo y de las razones por la que este riesgo no es aceptable. Es fundamental entender las razones que llevan a una valoración determinada de riesgo para que el proceso de gestión de riesgos esté bien fundamentado. El proceso de gestión de riesgos partirá de estas valoraciones para atajar el riesgo o reducirlo a niveles aceptables.

3.4. Lista de control

√	**actividad**	**tarea**
	Se han identificado los activos esenciales: información que se trata y servicios que se prestan	MAR.11
	Se han valorado las necesidades o niveles de seguridad requeridos por cada activo esencial en cada dimensión de seguridad	MAR.13
	Se han identificado los demás activos del sistema	MAR.11
	Se han establecido el valor (o nivel requerido de seguridad) de los demás activos en función de su relación con los activos esenciales (por ejemplo, mediante identificación de las dependencias)	MAR.12
	Se han identificado las amenazas posibles sobre los activos	MAR.21
	Se han estimado las consecuencias que se derivarían de la materialización de dichas amenazas	MAR.22
	Se ha estimado la probabilidad de que dichas amenazas se materialicen	MAR.23
	Se han estimado los impactos y riesgos potenciales, inherentes al sistema	MAR.4
	Se han identificado las salvaguardas apropiadas para atajar los impactos y riesgos potenciales	MAR.31
	Se ha valorado el despliegue de las salvaguardas identificadas	MAR.32
	Se han estimado los valores de impacto y riesgo residuales, que es el nivel de impacto y riesgo que aún soporta el sistema tras el despliegue de las salvaguardas	MAR.4

4. Proceso de gestión de riesgos

A la vista de los impactos y riesgos a que está expuesto el sistema, hay que tomar una serie de decisiones condicionadas por diversos factores:

- la gravedad del impacto y/o del riesgo
- las obligaciones a las que por ley esté sometida la Organización
- las obligaciones a las que por reglamentos sectoriales esté sometida la Organización
- las obligaciones a las que por contrato esté sometida la Organización

Dentro del margen de maniobra que permita este marco, pueden aparecer consideraciones adicionales sobre la capacidad de la Organización para aceptar ciertos impactos de naturaleza intangible[16] tales como:

- imagen pública de cara a la Sociedad (aspectos reputacionales)
- política interna: relaciones con los propios empleados, tales como capacidad de contratar al personal idóneo, capacidad de retener a los mejores, capacidad de soportar rotaciones de personas, capacidad de ofrecer una carrera profesional atractiva, etc.
- relaciones con los proveedores, tales como capacidad de llegar a acuerdos ventajosos a corto, medio o largo plazo, capacidad de obtener trato prioritario, etc.
- relaciones con los clientes o usuarios, tales como capacidad de retención, capacidad de incrementar la oferta, capacidad de diferenciarse frente a la competencia, ...
- relaciones con otras organizaciones, tales como capacidad de alcanzar acuerdos estratégicos, alianzas, etc.
- nuevas oportunidades de negocio, tales como formas de recuperar la inversión en seguridad
- acceso a sellos o calificaciones reconocidas de seguridad

Todas las consideraciones anteriores desembocan en una calificación de cada riesgo significativo, determinándose si ...

1. es **crítico** en el sentido de que requiere atención urgente
2. es **grave** en el sentido de que requiere atención
3. es **apreciable** en el sentido de que pueda ser objeto de estudio para su tratamiento
4. es **asumible** en el sentido de que no se van a tomar acciones para atajarlo

La opción 4, aceptación del riesgo, siempre es arriesgada y hay que tomarla con prudencia y justificación. Las razones que pueden llevar a esta aceptación son:

- cuando el impacto residual es asumible
- cuando el riesgo residual es asumible
- cuando el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales

La calificación de los riesgos tendrá consecuencias en las tareas subsiguientes, siendo un factor básico para establecer la prioridad relativa de las diferentes actuaciones.

16 La metodología de análisis y gestión de riesgos, al centrarse en la evaluación de daños, no captura plenamente los beneficios de la ausencia de daños que, generando un ambiente de confianza, permite un mejor desempeño de las funciones de la Organización en su entorno de operación.

4.1. Conceptos

El análisis de riesgos determina impactos y riesgos. Los impactos recogen daños absolutos, independientemente de que sea más o menos probable que se dé la circunstancia. En cambio, el riesgo pondera la probabilidad de que ocurra. El impacto refleja el daño posible (lo peor que puede ocurrir), mientras que el riesgo refleja el daño probable (lo que probablemente ocurra).

El resultado del análisis es sólo un análisis. A partir de el disponemos de información para tomar decisiones conociendo lo que queremos proteger (activos valorados=, de qué lo queremos proteger (amenazas valoradas) y qué hemos hecho por protegerlo (salvaguardas valoradas). Todo ello sintetizado en los valores de impacto y riesgo.

A partir de aquí, las decisiones son de los órganos de gobierno de la Organización que actuarán en 2 pasos:

- paso 1: evaluación
- paso 2: tratamiento

La siguiente figura resume las posibles decisiones que se pueden tomar tras haber estudiado los riesgos. La caja 'estudio de los riesgos' pretende combinar el análisis con la evaluación.

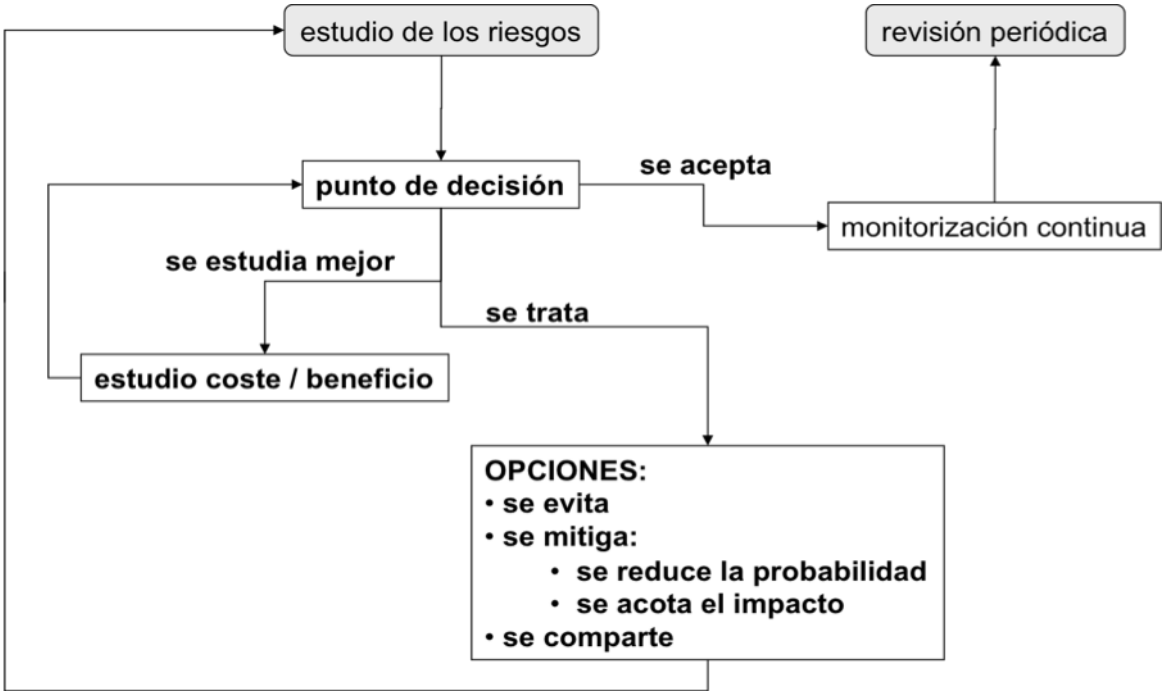

Ilustración 11. Decisiones de tratamiento de los riesgos

Todos estos aspectos se desarrollan en las secciones siguientes.

4.1.1. Evaluación: interpretación de los valores de impacto y riesgo residuales

Impacto y riesgo residual son una medida del estado presente, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores aceptables.

Los párrafos siguientes se refieren conjuntamente a impacto y riesgo.

Si el valor residual es igual al valor potencial, las salvaguardas existentes no valen para nada, típicamente no porque no haya nada hecho, sino porque hay elementos fundamentales sin hacer.

Es importante entender que un valor residual es sólo un número. Para su correcta interpretación debe venir acompañado de la relación de lo que se debería hacer y no se ha hecho; es decir, de las vulnerabilidades que presenta el sistema. Los responsables de la toma de decisiones deberán prestar cuidadosa atención a esta relación de tareas pendientes, que se denomina **Informe de Insuficiencias o de vulnerabilidades**.

4.1.2. Aceptación del riesgo

La Dirección de la Organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable. Más propiamente dicho, debe aceptar la responsabilidad de las insuficiencias. Esta decisión no es técnica. Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios. Estos niveles de aceptación se pueden establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión, ...)

Cualquier nivel de impacto y/o riesgo es aceptable si lo conoce y acepta formalmente la Dirección[17].

4.1.3. Tratamiento

La Dirección puede decidir aplicar algún tratamiento al sistema de seguridad desplegado para proteger el sistema de información. Hay dos grandes opciones:

- reducir el riesgo residual (aceptar un menor riesgo)
- ampliar el riesgo residual (aceptar un mayor riesgo)

Para tomar una u otra decisión hay que enmarcar los riesgos soportados por el sistema de información dentro de un contexto más amplio que cubre un amplio espectro de consideraciones de las que podemos apuntar algunas sin pretender ser exhaustivos:

- cumplimiento de obligaciones; sean legales, regulación pública o sectorial, compromisos internos, misión de la Organización, responsabilidad corporativa, etc.
- posibles beneficios derivados de una actividad que en sí entraña riesgos
- condicionantes técnicos, económicos, culturales, políticos, etc.
- equilibrio con otros tipos de riesgos: comerciales, financieros, regulatorios, medioambientales, laborales, …

En condiciones de **riesgo residual extremo**, casi la única opción es reducir el riesgo.

En condiciones de **riesgo residual aceptable**, podemos optar entre aceptar el nivel actual o ampliar el riesgo asumido. En cualquier caso hay que mantener una monitorización continua de las circunstancias para que el riesgo formal cuadre con la experiencia real y reaccionemos ante cualquier desviación significativa.

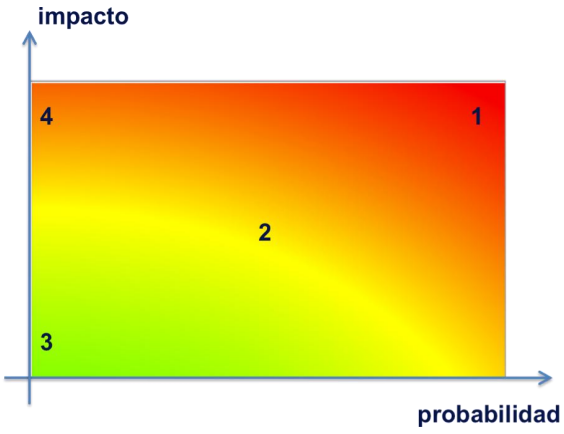

Ilustración 12. Zonas de riesgo

[17] Hablar de Dirección es pecar de simplificar la realidad. En inglés suele emplearse el término *"stakeholders"* (o tenedores de la estaca) para referirse a los afectados por las decisiones estratégicas de una Organización: dueños, gerentes, usuarios, empleados e incluso la sociedad en general. Porque al final si se aceptan riesgos imprudentemente elevados, el perjudicado puede no ser sólo el que dirige, sino todos los que tienen su confianza puesta en la Organización y cuyo lamentable desempeño oscurecería sus legítimas expectativas. En última instancia puede verse afectada la confianza en un sector o en una tecnología por la imprudente puesta en escena de algunos actores.

En condiciones de **riesgo residual medio**, podemos observar otras características como las pérdidas y ganancias que pueden verse afectadas por el escenario presente, o incluso analizar el estado del sector en el que operamos para compararnos con la “norma”.

En términos de las zonas de riesgo que se expusieron anteriormente,

- zona 1 – riesgos muy probables y de muy alto impacto; posiblemente nos planteemos sacarlos de esta zona
- zona 2 – riesgos de probabilidad relativa e impacto medio; se pueden tomar varias opciones
- zona 3 – riesgos improbables y de bajo impacto; o los dejamos como están, o permitimos que suban a mayores si ello nos ofreciera alguna ventaja o beneficio en otro terreno
- zona 4 – riesgos improbables pero de muy alto impacto; suponen un reto de decisión pues su improbabilidad no justifica que se tomen medidas preventivas, pero su elevado impacto exige que tengamos algo previsto para reaccionar; es decir, hay que poner el énfasis en medidas de reacción para limitar el daño y de recuperación del desastre si ocurriera.

También conviene considerar la incertidumbre del análisis. Hay veces que sospechamos las consecuencias, pero hay un amplio rango de opiniones sobre su magnitud (incertidumbre en el impacto). En otras ocasiones la incertidumbre afecta a la probabilidad. Estos escenarios suelen afectar a las zonas 4 y 3, pues cuando la probabilidad es alta, normalmente adquirimos experiencia, propia o ajena, con rapidez y salimos de la incertidumbre. En cualquier caso, toda incertidumbre debe considerarse como mala y debemos hacer algo:

- buscar formas de mejorar la previsión, típicamente indagando en foros, centros de respuesta a incidentes o expertos en la materia;
- evitar el riesgo cambiando algún aspecto, componente o arquitectura del sistema; o
- tener preparados sistemas de alerta temprana y procedimientos flexibles de contención, limitación y recuperación del posible incidente.

A veces que estos escenarios de incertidumbre ocurren en un terreno en el que hay obligaciones de cumplimiento y la propia normativa elimina o reduce notablemente las opciones disponibles; es decir, el sistema se protege por obligación más que por certidumbre del riesgo.

A la vista de estas consideraciones se tomarán las decisiones de tratamiento.

4.1.4. Estudio cuantitativo de costes / beneficios

Es de sentido común que no se puede invertir en salvaguardas más allá del valor que queremos proteger.

Aparecen en la práctica gráficos como el siguiente que ponen uno frente al otro el coste de la inseguridad (lo que costaría no estar protegidos) y el coste de las salvaguardas.

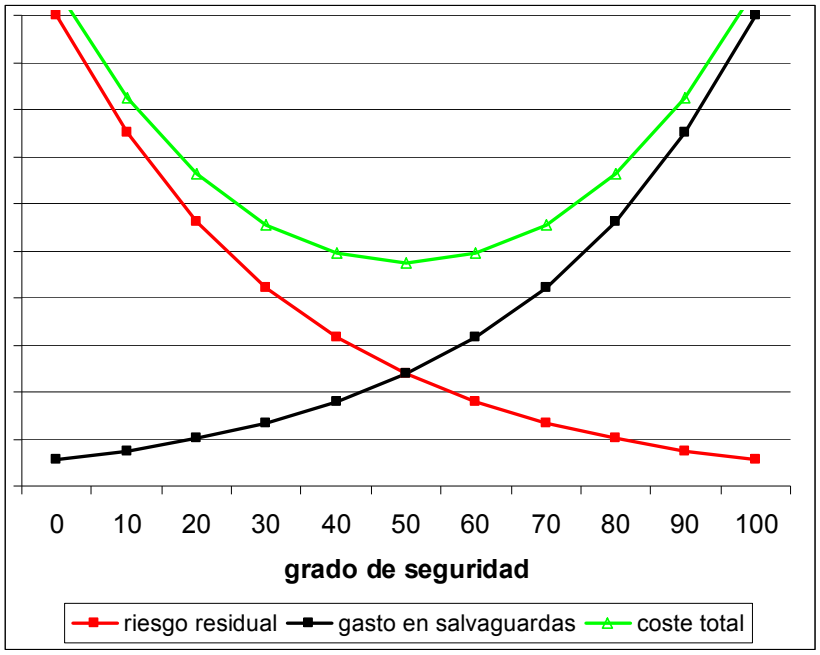

Ilustración 13. Relación entre el gasto en seguridad y el riesgo residual

Este tipo de gráficas intentan reflejar cómo al avanzar de un grado de seguridad 0 hacia un grado de seguridad del 100%, el coste de la inseguridad (el riesgo) disminuye, mientras que el coste de la inversión en salvaguardas aumenta. Es intencionado el hecho de que el riesgo caiga fuertemente con pequeñas inversiones[18] y que el coste de las inversiones se dispare para alcanzar niveles de seguridad cercanos al 100%[19]. La curva central suma el coste para la Organización, bien derivado del riesgo (baja seguridad), bien derivado de la inversión en protección. De alguna forma existe un punto de equilibrio entre lo que se arriesga y lo que se invierte en defensa, punto al que hay que tender si la única consideración es económica.

Pero llevar el sentido común a la práctica no es evidente, ni por la parte del cálculo del riesgo, ni por la parte del cálculo del coste de las salvaguardas. En otras palabras, la curva anterior es conceptual y no se puede dibujar en un caso real.

En la práctica, cuando hay que protegerse de un riesgo que se considera significativo, aparecen varios escenarios hipotéticos:

E0: si no se hace nada

E1: si se aplica un cierto conjunto de salvaguardas

E2: si se aplica otro conjunto de salvaguardas

Y así N escenarios con diferentes combinaciones de salvaguardas.

El análisis económico tendrá como misión decidir entre estas opciones, siendo E0 (seguir como estamos) una opción posible, que pudiera estar justificada económicamente.

En cada escenario hay que estimar a lo largo del tiempo el coste que va a suponer. Para poder agregar costes, se contabilizan como valores negativos las pérdidas de dinero y como valores positivos las entradas de dinero. Considerando los siguientes componentes:

- (recurrente) riesgo residual[20]
- (una vez) coste de las salvaguardas[21]

[18] Medidas básicas de seguridad suponen un importante descenso del riesgo. Por ello son inexcusables.
[19] Reflejando una vez más que la seguridad absoluta (riesgo cero) no existe.
[20] Si la frecuencia de las amenazas se ha estimado como tasa anual, los datos de riesgo residual estarán automáticamente anualizados. Si se hubiera empleado otra escala, habría que convertirla a términos anuales.

- (recurrente) coste anual de mantenimiento de las salvaguardas
+ (recurrente) mejora en la productividad[22]
+ (recurrente) mejoras en la capacidad de la Organización para prestar nuevos servicios, conseguir mejores condiciones de los proveedores, entrar en asociación con otras organizaciones, etc.

El escenario E0 es muy simple: todos los años se afronta un gasto marcado por el riesgo, que se acumula año tras año.

En los demás escenarios, hay cosas que suman y cosas que restan, pudiendo darse varias situaciones[23] como las recogidas en la gráfica siguiente. Se presentan valores acumulados a lo largo de un periodo de 5 años. La pendiente de la recta responde a los costes recurrentes. El valor el primer año corresponde a los costes de implantación.

	riesgo (anual)	coste (inicial)	coste (anual)	mejora (anual)	otros (anual)	año 1	2	3	4	5
E0	10	0	0	0	0	-10	-20	-30	-40	-50
E1	5	20	5	0	0	-30	-40	-50	-60	-70
E2	2	50	10	20	0	-42	-34	-26	-18	-10
E3	1	70	15	35	0	-51	-32	-13	6	25

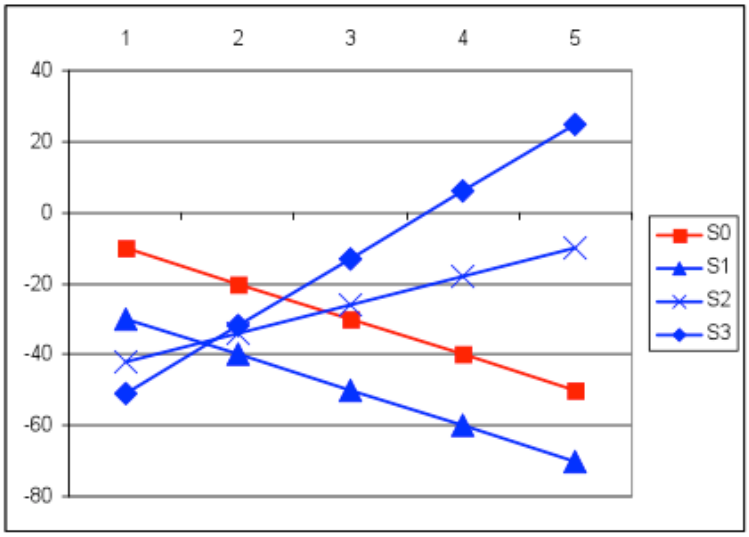

Ilustración 14. Ejemplos de decisiones de tratamiento del riesgo

- En E0 se sabe lo que cada año (se estima que) se pierde
- El escenario E1 aparece como mala idea, pues supone un gasto añadido el primer año; pero este gasto no se recupera en años venideros.
- No así el escenario E2 que, suponiendo un mayor desembolso inicial, empieza a ser rentable a partir del cuarto año.
- Más atractivo aún es el escenario E3 en el que a costa de un mayor desembolso inicial, se empieza a ahorrar al tercer año, e incluso se llega a obtener beneficios operativos a partir del quinto año. Se puede decir que en escenario E3 se ha hecho una buena inversión.

21 Si la salvaguarda ya existe, coste de mejora. Si no existiera, coste de adquisición e instalación. En cualquier caso hay que imputar costes de formación de los operadores, usuarios, etc.

22 Este epígrafe puede ser positivo si la Organización mejora su productividad; o puede ser negativo, si empeora. Como ejemplo típico de salvaguardas que mejoran la productividad podemos citar la introducción de dispositivos de autenticación en sustitución de la clásica contraseña. Como ejemplo típico de salvaguardas que minoran la productividad podemos citar la clasificación de documentación con control de acceso restringido.

23 En el eje X se muestran años, en referencia al año 0 en que se realiza el análisis de riesgos. En ordenadas aparecen costes en unidades arbitrarias.

4.1.5. Estudio cualitativo de costes / beneficios

Cuando el análisis es cualitativo, en la balanza de costes beneficios aparecen aspectos intangibles que impiden el cálculo de un punto numérico de equilibrio.

Entre los aspectos intangibles se suelen contemplar:

— aspectos reputacionales o de imagen

— aspectos de competencia: comparación con otras organizaciones de mismo ámbito de actividad

— cumplimiento normativo, que puede ser obligatorio o voluntario

— capacidad de operar

— productividad

Estas consideraciones nos llevan a contemplar diversos escenarios para determinar el balance neto. Por ejemplo, el no adoptar medidas puede exponernos a un cierto riesgo que causaría mala imagen; pero si la solución preventiva causa también mala imagen o supone un merma notable de oportunidades o de productividad, hay que buscar un punto de equilibrio, eligiendo una combinación de medidas que sea asumible.

4.1.6. Estudio mixto de costes / beneficios

En análisis de riesgos meramente cualitativos, la decisión la marca el balance de costes y beneficios intangibles, si bien siempre hay que hacer un cálculo de lo que cuesta la solución y cerciorarse de que el gasto es asumible. De o contrario, la supuesta solución no es una opción. Es decir, primero hay que pasar el filtro económico y luego elegir la mejor de las soluciones factibles.

4.1.7. Opciones de tratamiento del riesgo: eliminación

La eliminación de la fuente de riesgo es una opción frente a un riesgo que no es aceptable.

En un sistema podemos eliminar varias cosas, siempre que no afecten a la esencia de la Organización. Es extremadamente raro que podamos prescindir de la información o los servicios esenciales por cuanto constituyen la misión de la Organización. Cambiar estos activos supone reorientar la misión de la Organización.

Más viable es prescindir de otros componentes no esenciales, que están presentes simple y llanamente para implementar la misión, pero no son parte constituyente de la misma. Esta opción puede tomar diferentes formas:

- Eliminar cierto tipo de activos, emplean otros en su lugar. Por ejemplo: cambiar de sistema operativo, de fabricante de equipos, …
- Reordenar la arquitectura del sistema (el esquema de dependencias en nuestra terminología) de forma que alteremos el valor acumulado en ciertos activos expuestos a grandes amenazas. Por ejemplo: segregar redes, desdoblar equipos para atender a necesidades concretas, alejando lo más valioso de lo más expuesto, …

Las decisiones de eliminación de las fuentes de riesgo suponen realizar un nuevo análisis de riesgos sobre el sistema modificado.

4.1.8. Opciones de tratamiento del riesgo: mitigación

La mitigación del riesgo se refiere a una de dos opciones:

- reducir la degradación causada por una amenaza (a veces se usa la expresión ‘acotar el impacto’)
- reducir la probabilidad de que una amenaza de materializa

En ambos casos lo que hay que hacer es ampliar o mejorar el conjunto de salvaguardas. En términos de madurez de las salvaguardas: subir de nivel.

Algunas salvaguardas, notablemente las de tipo técnico, se traducen en el despliegue de más equipamiento[24] que se convierte a su vez en un activo del sistema. Estos nuevos activos también acumularán valor del sistema y estarán a su vez sujetos a amenazas que pueden perjudicar a los activos esenciales.

Hay pues que repetir el análisis de riesgos, ampliándolo con el nuevo despliegue de medios y, por supuesto, cerciorarse de que el riesgo del sistema ampliado es menor que el del sistema original; es decir, que las salvaguardas efectivamente disminuyen el estado de riesgo de la Organización.

4.1.9. Opciones de tratamiento del riesgo: compartición

Tradicionalmente se ha hablado de 'transferir el riesgo'. Como la transferencia puede ser parcial o total, es más general hablar de 'compartir el riesgo'.

Hay dos formas básicas de compartir riesgo:

- Riesgo cualitativo: se comparte por medio de la externalización de componentes del sistema, de forma que se reparten responsabilidades: unas técnicas para el que opera el componente técnico; y otras legales según el acuerdo que se establezca de prestación del servicio.
- Riesgo cuantitativo: se comparte por medio de la contratación de seguros, de forma que a cambio de una prima, el tomador reduce el impacto de las posibles amenazas y el asegurador corre con las consecuencias. Hay multitud de tipos y cláusulas de seguros para concretar el grado de responsabilidad de cada una de las partes.

Cuando se comparten riesgos cambia, bien el conjunto de componentes del sistema, bien su valoración, requiriéndose un nuevo análisis del sistema resultante.

4.1.10. Opciones de tratamiento del riesgo: financiación

Cuando se acepta un riesgo, la Organización hará bien en reservar fondos para el caso de que el riesgo se concrete y haya que responder de sus consecuencias. A veces de habla de 'fondos de contingencia' y también puede ser parte de los contratos de aseguramiento.

Normalmente esta opción no modifica nada del sistema y nos vale el análisis de riesgos disponible.

4.2. Formalización de las actividades

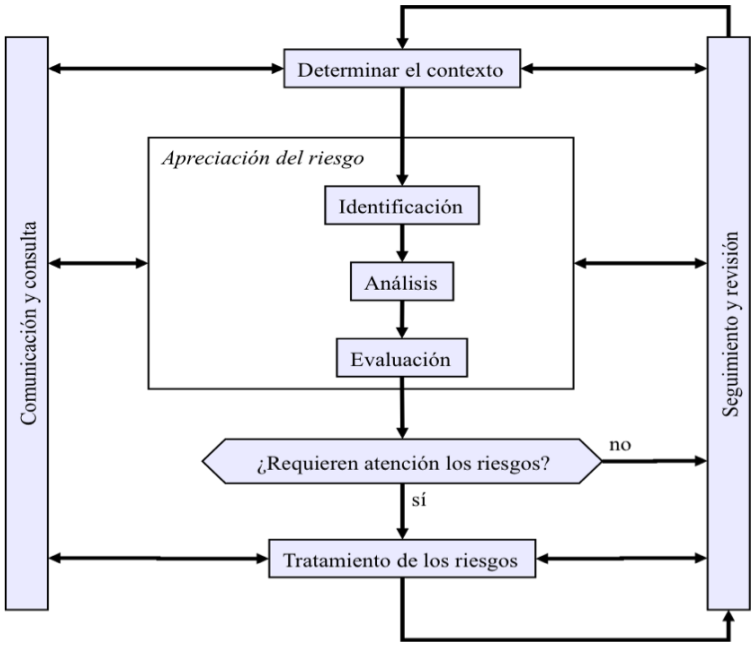

Ilustración 15. Proceso de gestión de riesgos

24 Ejemplos típicos pueden ser un equipo cortafuegos, un sistema de gestión de redes privadas virtuales, tarjetas inteligentes de identificación de los usuarios, una PKI de clave pública, etc.

4.2.1. Roles y funciones

En el proceso de gestión de riesgos aparecen varios actores. Los siguientes párrafos intentan identificarlos de forma somera y explicitar cuales son sus funciones y responsabilidades.

Órganos de gobierno

En este epígrafe se incluyen aquellos que órganos colegiados o unipersonales que deciden la misión y los objetivos de la Organización.

Típicamente se incluyen en esta categoría los altos cargos de los organismos.

Cuando existe un Comité de Seguridad de la Información, suele aparecer en este nivel.

Estos órganos tienen la autoridad última para aceptar los riesgos con que se opera. Se dice que son los “propietarios del riesgo”.

Dirección ejecutiva

En este epígrafe se incluyen aquellos órganos colegiados o unipersonales que toman decisiones que concretan cómo alcanzar los objetivos de negocio marcados por los órganos de gobierno.

Típicamente se incluyen en esta categoría los responsables de unidades de negocio, los responsables de la calidad de los servicios prestados por la organización, etc.

Dirección operacional

En este epígrafe se incluyen aquellos órganos colegiados o unipersonales que toman decisiones prácticas para materializar las indicaciones dadas por los órganos ejecutivos.

Típicamente se incluyen en esta categoría los responsables de operaciones, de producción, de explotación y similares.

Esquema Nacional de Seguridad

En el Esquema Nacional de Seguridad de identifican ciertos roles que pueden verse involucrados en el proceso de gestión de riesgos:

Responsable de la información

Típicamente a nivel de gobierno. Tiene la responsabilidad última sobre qué seguridad requiere una cierta información manejada por la Organización.

A este nivel se suele concretar la responsabilidad sobre datos de carácter personal y sobre la clasificación de la información.

A veces este role lo ejerce el Comité de Seguridad de la Información.

Responsable del servicio

Típicamente a nivel de gobierno, aunque a veces baja a nivel ejecutivo. Tiene la responsabilidad última de determinar los niveles de servicio aceptables por la Organización.

A veces este role lo asume el Comité de Seguridad de la Información.

Responsable de la seguridad

Típicamente a nivel ejecutivo, actuando como engranaje entre las directrices emanadas de los responsables de la información y los servicios, y el responsable del sistema. A su vez funciona como supervisor de la operación del sistema y vehículo de reporte al Comité de Seguridad de la Información.

A veces se denomina a esta figura CISO (*Chief Information Security Officer*).

En lo que respecta al proceso de gestión de riesgos, es la persona que traslada la valoración de los activos esenciales, que aprueba la declaración de aplicabilidad de salvaguardas, los procedimientos operativos, los riesgos residuales y los planes de seguridad. En esta fun-

ción de informante, suele ser la persona encargada de elaborar los indicadores del esto de seguridad del sistema.

Responsable del sistema

A nivel operacional. Toma decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día.

En lo que respecta al proceso de gestión de riesgos, es la persona que propone la arquitectura de seguridad, la declaración de aplicabilidad de salvaguardas, los procedimientos operativos y los planes de seguridad. También es la persona responsable de la implantación y correcta operación de las salvaguardas.

Administradores y operadores

Son las personas encargadas de ejecutar las acciones diarias de operación del sistema según las indicaciones recibidas de sus superiores jerárquicos.

Matriz RACI

La matriz que se expone a continuación es orientativa y cada organismo deberá adecuarla a su organización particular.

La matriz de la asignación de responsabilidades (RACI por las iniciales, en inglés, de los tipos de responsabilidad) se utiliza generalmente en la gestión de proyectos para relacionar actividades con recursos (individuos o equipos de trabajo). De esta manera se logra asegurar que cada una de las tareas esté asignada a un individuo o a un órgano colegiado.

	rol	descripción
R	Responsible	Este rol realiza el trabajo y es responsable por su realización. Lo más habitual es que exista sólo un R, si existe más de uno, entonces el trabajo debería ser subdividido a un nivel más bajo, usando para ello las matrices RASCI. Es quien debe ejecutar las tareas.
A	Accountable	Este rol se encarga de aprobar el trabajo finalizado y a partir de ese momento, se vuelve responsable por él. Sólo puede existir un A por cada tarea. Es quien debe asegurar que se ejecutan las tareas.
C	Consulted	Este rol posee alguna información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información (comunicación bidireccional).
I	Informed	Este rol debe ser informado sobre el progreso y los resultados del trabajo. A diferencia del Consultado, la comunicación es unidireccional.

Tabla 5. Roles en procesos distribuidos

Tarea	Dirección	RINFO	RSERV	RSEG	RSIS	ASS
niveles de seguridad requeridos por la información		A	I	R	C	
niveles de seguridad requeridos por el servicio		I	A	R	C	
análisis de riesgos		I	I	A/R	C	
declaración de aplicabilidad		I	I	A/R	C	
aceptación del riesgo residual	I	A	A	R	I	
implantación de las medidas de seguridad		I	I	C	A	R
					C	R

Tarea	Direc-ción	RINFO	RSERV	RSEG	RSIS	ASS
estado de seguridad del sistema	I	I	I	A	I	R
planes de mejora de la seguridad				A	C	
planes de concienciación y formación				A	C	
planes de continuidad				C	A	
seguridad en el ciclo de vida				C	A	

Tabla 6. Matriz RACI - Tareas relacionadas con la gestión de riesgos

Siendo

Dirección – Alta Dirección, Órganos de Gobierno

RINFO – Responsable de la Información

RSERV – Responsable del Servicio

RSEG – Responsable de la Seguridad

RSIS – Responsable (operacional) del Sistema

ASS – Administrador(es) de la Seguridad del Sistema

4.2.2. Contexto

Hay que documentar el entorno externo en el que opera la Organización: cultural, social y político. Esto incluye tanto aspectos nacionales como internacionales, viniendo marcados por el ámbito de actividad de la Organización.

Hay que identificar las obligaciones legales, reglamentarias y contractuales. Por ejemplo, suele haber obligaciones asociadas a

- tratamiento de datos de carácter personal,
- tratamiento de información clasificada,
- tratamiento de información y productos sometidos a derechos de propiedad intelectual
- prestación de servicios públicos
- operación de infraestructuras críticas
- etc.

Hay que identificar el entorno en cuanto competencia y posicionamiento respecto de la competencia.

Hay que identificar el contexto interno en el que se desenvuelve la actividad de la Organización: política interna, compromisos con los accionistas y con los trabajadores o sus representantes.

La identificación del contexto en el que se desarrolla el proceso de gestión de riesgos debe ser objeto de una revisión continua para adaptarse a las circunstancias de cada momento.

4.2.3. Criterios

Múltiples aspectos relacionados con los riesgos son objeto de estimaciones. Conviene que las estimaciones sean lo más objetivas que sea posible o. al menos, que sean repetibles, explicables y comparables.

En particular conviene establecer escalas de valoración para

- valorar los requisitos de seguridad de la información
- valorar los requisitos de disponibilidad de los servicios

- estimar la probabilidad de una amenaza
- estimar las consecuencias de un incidente de seguridad
- estimar el nivel de riesgo a partir de las estimaciones de impacto y probabilidad
- … (ver “Libro II – Catálogo de Elementos”)

Hay que establecer reglas y/o criterios para tomar decisiones de tratamiento:

- umbrales de impacto
- umbrales de probabilidad
- umbrales combinados de impacto y probabilidad
- umbrales de nivel de riesgo
- impacto en la reputación de la Organización o de las personas responsables
- impacto en la posición de competencia
- impacto comparado con otras áreas de riesgo: financiero, regulatorio, medioambiental, seguridad industrial, etc
- combinaciones o concurrencia de riesgos que pudieran tener un efecto combinado
- amenazas especialmente sensibles (puede ser por motivos técnicos, porque adolecen de una amplia incertidumbre o porque su ocurrencia causaría una notable alarma social con grave daño para la reputación o la continuidad de las operaciones de la Organización, incluso si sus consecuencia técnicas o materiales son modestas)
- …

4.2.4. Evaluación de los riesgos

Se sigue la metodología descrita en el capítulo anterior.

La primera vez que se ejecuta esta actividad puede ser conveniente lanzar un proyecto específico de análisis de riesgos. Ver capítulo siguiente.

4.2.5. Decisión de tratamiento

Se pueden tomar las diferentes opciones mencionadas al principio de este capítulo.

Hay múltiples formas de reducir el riesgo:

- eliminar el riesgo eliminando sus causas: información tratada, servicios prestados, arquitectura del sistema,
- reducir o limitar el impacto
- reducir la probabilidad de que la amenaza ocurra
- en el caso de amenazas derivadas de defectos de los productos (vulnerabilidades técnicas): reparar el producto (por ejemplo, aplicar los parches del fabricante)
- implantar nuevas salvaguardas o mejorar la calidad de las presentes
- externalizar partes del sistema
- contratar seguros de cobertura

A veces la decisión consiste en aceptar un incremento del riesgo:

- aceptando trabajar con nueva información o prestar nuevos servicios
- alterando la arquitectura del sistema
- reduciendo las salvaguardas presentes
- reduciendo la calidad de las salvaguardas presentes (es decir, dedicando menos recursos)

En última instancia siempre hay que acabar aceptando un cierto riesgo residual, en cuyo caso es posible que se decide reservar fondos para hacer frente a alguna contingencia.

4.2.6. Comunicación y consulta

Antes de tomar ninguna decisión relativa al tratamiento de un riesgo hay que entender para qué se usa el sistema y cómo se usa.

Esto quiere decir mantener un contacto fluido con varios actores

- los órganos de gobierno y decisión, pues toda decisión debe estar alineada con la misión de la Organización
- los usuarios y técnicos de sistemas, pues toda decisión debe tener en cuenta su impacto en la productividad y sobre la usabilidad del sistema
- los proveedores, pues toda decisión debe contar con su colaboración

Hay que tener en cuenta que cualquier medida de seguridad que merme la productividad, dificulte la operación del sistema, o requiera una elaborada formación de los usuarios, está condenada al fracaso,

Toda medida de seguridad debe estar

- apoyada por la Dirección
- amparada por la Política de Seguridad de la Organización
- apoyada por normativa clara y legible, ampliamente divulgada
- explicada de forma breve, clara y directa en procedimientos operativos de seguridad

Por último es interesante disponer de indicadores que midan el grado de aceptación por parte de los usuarios, identificando tanto el grado de cumplimiento como los problemas que causa su seguimiento.

4.2.7. Seguimiento y revisión

El análisis de los riesgos es un ejercicio formal, basado en múltiples estimaciones y valoraciones que pueden no compadecerse con la realidad. Es absolutamente necesario que el sistema esté bajo monitorización permanente. Los indicadores de impacto y riesgo potenciales son útiles para decidir qué puntos deben ser objeto de monitorización.

Y debe estar preparado un sistema de detección precoz de posibles incidentes (en base a indicadores predictivos) así como un sistema de reacción a incidentes de seguridad.

Se procurará disponer de un conjunto de indicadores clave de riesgo (*KRI – Key Risk Indicators*). Estos indicadores:

- son propuestos por el Responsable de la Seguridad;
- su definición es acordada por el Responsable de la Seguridad y el propietario del riesgo; la definición indicará exactamente:
  - en qué medidas se basan,
  - cuál es el algoritmo de cálculo,
  - la periodicidad de evaluación y
  - los umbrales de aviso y alarma (atención urgente)
- se le presentan al responsable correspondiente
  - rutinariamente, con la periodicidad establecida,
  - puntualmente, por demanda del propietario del riesgo medido,
  - y extraordinariamente cuando se supera un umbral de riesgo
- estos indicadores estarán a disposición de los auditores

La responsabilidad de monitorizar un riesgo recae en su propietario, sin perjuicio de que la función puede ser delegada en el día a día, retomando el control de la situación cuando hay que tomar medidas para atajar un riesgo que se ha salido de los márgenes tolerables.

Cada vez que la realidad difiere de nuestras estimaciones conviene hacer un ciclo de revisión del análisis y las decisiones de tratamiento.

Servicios subcontratados

Cuando dependemos de terceros es especialmente importante conocer el desempeño de nuestros proveedores, tanto con un buen sistema de reporte, escalado y resolución de los incidentes de seguridad, como en el establecimiento de indicadores predictivos. Del análisis de dependencias realizado durante el análisis de riesgos, tenemos información de en qué medida y en qué dimensiones de seguridad dependemos de cada proveedor externo. De esta información se sigue qué elementos debemos monitorizar para asegurarnos que satisfacen nuestros requisitos de seguridad.

4.3. Documentación del proceso

Documentación interna

- Definición de roles, funciones y esquemas de reporte
- Criterios de valoración de la información
- Criterios de valoración de los servicios
- Criterios de evaluación de los escenarios de impacto y riesgo

Documentación para otros

- Plan de Seguridad

4.4. Indicadores de control del proceso de gestión de riesgos

√	**actividad**	**tarea**
	Se han definido los roles y responsabilidades respecto de la gestión de riesgos	4.2.1
	Se ha establecido el contexto de gestión de riesgos	4.2.2
	Se han establecido los criterios de valoración de riesgos y toma de decisiones de tratamiento	4.2.3
	Se han interpretado los riesgos residuales en términos de impacto en el negocio o misión de la Organización	4.2.4
	Se han identificado y valorado opciones de tratamiento de los riesgos residuales (propuesta de programas de seguridad)	4.2.5
	Los órganos de gobierno han adoptado una propuesta de tratamiento — evitar el riesgo — prevenir: mitigar la probabilidad de que ocurra — mitigar el impacto si ocurriera — compartir el riesgo con un tercero — asumir el riesgo	4.2.5
	Se han previsto recursos para acometer el plan de seguridad	4.2.5

√	**actividad**	**tarea**
	Se han previsto recursos para atender a contingencias	4.2.5
	Se han comunicado las decisiones a las partes afectadas	4.2.6
	Se ha desplegado un sistema de monitorización constante para detectar modificaciones en los supuestos de análisis de riesgos	4.2.7
	Se han establecido las normas y procedimientos de actuación en caso de detectar desviaciones de los supuestos	4.2.7

5. Proyectos de análisis de riesgos

Las actividades de análisis de riesgo son recurrentes dentro del proceso de gestión, ya que hay que estar continuamente revisando el análisis y manteniéndolo al día. Podemos llamar 'análisis de riesgos marginales' a las salidas de estas actividades que, generalmente, requieren poco volumen de trabajo en cada iteración.

Pero antes de pasar a las iteraciones marginales, hay que disponer de un análisis de riesgos que sirva de plataforma de trabajo. Esto ocurre la primera vez que se realiza un análisis de riesgos y cuando la política de la organización marque que se prepare una nueva plataforma, sea por razones formales o porque los cambios acumulados justifican una revisión completa.

Cuando se realiza un análisis de riesgos partiendo de cero, se consumen una serie de recursos apreciables y conviene planificar estas actividades dentro de un proyecto, sea interno o se subcontrate a una consultora externa.

En esta sección se presentan las consideraciones que se deben tener en cuenta para que este proyecto llegue a buen término.

PAR.1 – Actividades preliminares

PAR.2 – Elaboración del análisis de riesgos

PAR.3 – Comunicación de resultados

5.1. Roles y funciones

Durante la ejecución del proyecto es frecuente que se creen algunos roles específicos para llevar el proyecto a buen fin.

Comité de Seguimiento

Está constituido por los responsables de las unidades afectadas por el proyecto; así como por los responsables de la informática y de la gestión dentro de dichas unidades. También será importante la participación de los servicios comunes de la Organización (planificación, presupuesto, recursos humanos, administración, etc.) En cualquier caso la composición del comité depende de las características de las unidades afectadas.

Las responsabilidades de este comité consisten en

- resolver las incidencias durante el desarrollo del proyecto
- asegurar la disponibilidad de recursos humanos con los perfiles adecuados y su participación en las actividades donde es necesaria su colaboración
- aprobar los informes intermedios y finales de cada proceso
- elaborar los informes finales para el comité de dirección

Este comité se suele nombrar por el Comité de Seguridad de la Información, y dicho comité reporta el avance del proyecto. A veces el Comité de Seguimiento toma la forma de subcomité del Comité de Seguridad de la Información.

Equipo de proyecto

Formado por personal experto en tecnologías y sistemas de información y personal técnico cualificado del dominio afectado, con conocimientos de gestión de seguridad en general y de la aplicación de la metodología de análisis y gestión de riesgos en particular. Si el proyecto se hace con asistencia técnica mediante contratación externa, el subsiguiente personal especialista en seguridad de sistemas de información se integrará en este equipo de proyecto.

Las responsabilidades de este equipo consisten en

- llevar a cabo las tareas del proyecto
- recopilar, procesar y consolidar datos
- elaborar los informes

El Equipo de Proyecto reporta al Comité de Seguimiento a través del Director del Proyecto.

Grupos de Interlocutores

Está formado por usuarios representativos dentro de las unidades afectadas por el proyecto. Lo constituyen varios posibles subgrupos:

- Responsables de servicio, conscientes de la misión de la Organización y sus estrategias a medio y largo plazo
- Responsables de servicios internos
- Personal de explotación y operación de los servicios informáticos, conscientes de los medios desplegados (de producción y salvaguardas) y de las incidencias habituales

Además de dichos órganos colegiados, hay que identificar algunos roles singulares:

Promotor

Es una figura singular que lidera las primeras tareas del proyecto, perfilando su oportunidad y alcance para lanzar el proyecto de análisis de riesgos propiamente dicho.

Debe ser una persona con visión global de los sistemas de información y su papel en las actividades de la Organización, sin necesidad de conocer los detalles; pero si al tanto de las incidencias.

Director del Proyecto

Debe ser un directivo de alto nivel, con responsabilidades en seguridad dentro de la Organización, de sistemas de información o, en su defecto, de planificación, de coordinación o de materias, servicios o áreas semejantes.

Es la cabeza visible del equipo de proyecto e interlocutor con el Responsable de la Seguridad de la Organización..

Enlace operacional

Será una persona de la Organización con buen conocimiento de las personas y de las unidades implicadas en el proyecto, que tenga capacidad para conectar al equipo de proyecto con el grupo de usuarios.

Es el interlocutor visible del comité de seguimiento con los grupos de usuarios.

Conviene recordar que un proyecto de análisis de riesgos siempre es mixto por su propia naturaleza; es decir, requiere la colaboración permanente de especialistas y usuarios tanto en las fases preparatorias como en su desarrollo. La figura del enlace operacional adquiere una relevancia permanente que no es habitual en otro tipo de proyectos más técnicos.

El proyecto de análisis de los riesgos se lleva a cabo por medio de las siguientes tareas:

PAR – Proyecto de Análisis de Riesgos
PAR.1 – Actividades preliminares
PAR.11 – Estudio de oportunidad
PAR.12 – Determinación del alcance del proyecto
PAR.13 – Planificación del proyecto
PAR.14 – Lanzamiento del proyecto
PAR.2 – Elaboración del análisis de riesgos
PAR.3 – Comunicación de resultados

5.2. PAR.1 – Actividades preliminares

Tarea PAR.11: Estudio de oportunidad

Se fundamenta la oportunidad de la realización, ahora, del proyecto de análisis de riesgos, enmarcándolo en el desarrollo de las demás actividades de la Organización.

El resultado de esta actividad es el informe denominado “preliminar”.

Tarea PAR.12: Determinación del alcance del proyecto

Se definen los objetivos finales del proyecto, su dominio y sus límites.

El resultado de esta actividad es un perfil de proyecto de análisis de riesgos.

Tarea PAR.13: Planificación del proyecto

Se determinan las cargas de trabajo que supone la realización del proyecto. Normalmente la evolución del proyecto viene marcada por una serie de entrevistas con los interlocutores que conocen la información relativa a algún activo o grupo de activos del sistema bajo análisis. Se planifican las entrevistas que se van a realizar para la recogida de información: quiénes van a ser entrevistados. Se elabora el plan de trabajo para la realización del proyecto.

En esta actividad se determinan los participantes y se estructuran los diferentes grupos y comités para llevar a cabo el proyecto.

El resultado de esta actividad está constituido por:

- un plan de trabajo para el proyecto
- procedimientos de trabajo

Tarea PAR.14: Lanzamiento del proyecto

Se adaptan los cuestionarios para la recogida de información adaptándolos al proyecto presente. Para ello se parte de los criterios establecidos dentro del Proceso de Gestión de Riesgos.

También se realiza una campaña informativa de sensibilización a los afectados sobre las finalidades y requerimientos de su participación.

El resultado de esta actividad está constituido por:

- los cuestionarios para las entrevistas
- el catálogo de tipos de activos
- la relación de dimensiones de seguridad y
- los criterios de valoración

5.2.1. Tarea PAR.11: Estudio de oportunidad

PAR: Proyecto de análisis de riesgos ***PAR.1: Actividades preliminares*** ***PAR.11: Determinar la oportunidad***
Objetivos • Identificar o suscitar el interés de la Dirección de la Organización en la realización de un proyecto de análisis de riesgos
Productos de entrada

PAR: Proyecto de análisis de riesgos
PAR.1: Actividades preliminares
PAR.11: Determinar la oportunidad

Productos de salida

- **Informe preliminar** recomendando la elaboración del proyecto
- Sensibilización y apoyo de la Dirección a la realización del proyecto
- Creación del comité de seguimiento

Técnicas, prácticas y pautas

-

Participantes

- El promotor

La Dirección suele ser muy consciente de las ventajas que aportan las técnicas electrónicas, informáticas y telemáticas a su funcionamiento; pero no tanto de los nuevos problemas de seguridad que estas técnicas implican, o de las obligaciones legales o reglamentarias que les afectan

En toda Organización pública o privada es importante transformar en medidas concretas la creciente preocupación por la falta de seguridad de los sistemas de información, por su soporte y entorno, puesto que sus efectos no sólo afectan a dichos sistemas, sino al propio funcionamiento de la Organización y, en las situaciones críticas, a su propia misión y capacidad de supervivencia.

Desarrollo

La iniciativa para la realización de un proyecto de análisis de riesgos parte de un promotor interno o externo a la Organización, consciente de los problemas relacionados con la seguridad de los sistemas de información, como por ejemplo:

- Incidentes continuados relacionados con la seguridad.
- Inexistencia de previsiones en cuestiones relacionadas con la evaluación de necesidades y medios para alcanzar un nivel aceptable de seguridad de los sistemas de información que sea compatible con el cumplimiento correcto de la misión y funciones de la Organización.
- Reestructuraciones en los productos o servicios proporcionados.
- Cambios en la tecnología utilizada.
- Desarrollo de nuevos sistemas de información.

El promotor puede elaborar un **cuestionario-marco** (documento poco sistematizable que deberá crear en cada caso concreto) para provocar la reflexión sobre aspectos de la seguridad de los sistemas de información por parte de :

Los responsables de las unidades operativas (responsables de servicios).

El cuestionario permite proceder a un examen informal de la situación en cuanto a la seguridad de sus sistemas de información; deben poder expresar su opinión por los proyectos de seguridad ya realizados (con su grado de satisfacción o con las limitaciones de éstos), así como sus expectativas ante la elaboración de un proyecto de análisis de riesgos[25]. Esta aproximación de alto nivel permite obtener una primera visión de los objetivos concretos y las opciones que tendrían que subyacer a la elaboración del proyecto.

25 Probablemente no se conozca lo que esto significa y haya que incluir en el cuestionario marco una sucinta explicación de qué es y qué objetivos persigue el análisis de riesgos en general y el proyecto en particular.

Los responsables de informática.

El cuestionario permite obtener una panorámica técnica para la elaboración del proyecto y posibilita abordar el estudio de oportunidad de realización, tras integrar las opciones anteriores.

De las respuestas al cuestionario-marco y de las entrevistas mantenidas con los responsables y colectivos anteriores, el promotor obtiene una primera aproximación sobre las funciones, los servicios y los productos implicados en cuestiones de seguridad de los sistemas de información, la ubicación geográfica de aquéllos, los medios técnicos, los medios humanos, etc.

Con estos elementos el promotor realiza el **informe preliminar** recomendando la elaboración del proyecto de análisis de riesgos e incluyendo estos elementos:

- Exposición de los argumentos básicos.
- Relación de antecedentes sobre la seguridad de los sistemas de información (Plan Estratégico, Plan de Actuación, etc.).
- Primera aproximación al dominio a incluir en el proyecto en función de
  - las finalidades de las unidades o departamentos
  - las orientaciones gerenciales y técnicas
  - la estructura de la Organización
  - el entorno técnico.
- Primera aproximación de los medios, tanto humanos como materiales, para la realización del proyecto.

El promotor presenta este informe preliminar a la Dirección que puede decidir:

- aprobar el proyecto, o bien
- modificar su dominio y/o sus objetivos, o bien
- retrasar el proyecto.

5.2.2. Tarea PAR.12: Determinación del alcance del proyecto

Una vez que se ha constatado la oportunidad de realizar el proyecto y se cuenta con el apoyo de la Dirección, esta actividad estima los elementos de planificación del proyecto, es decir los participantes y sus cargas de trabajo.

En dicha estimación se ha de tener en cuenta la posible existencia de otros planes (por ejemplo un Plan Estratégico de Sistemas de Información o de Seguridad general en las unidades que pueden ser afectadas o en la Organización) y el plazo de tiempo considerado para la puesta en práctica del proyecto. En particular, la existencia de un Plan Estratégico de Sistemas de Información para las unidades que pueden ser afectadas dentro de la Organización puede determinar en gran medida el alcance y la extensión de las actividades que se realicen en esta actividad.

PAR: Proyecto de análisis de riesgos
PAR.1: Actividades preliminares
PAR.12: Determinación del alcance del proyecto

Objetivos

- Determinar los objetivos del proyecto, diferenciados según horizontes temporales a corto y medio plazo
- Determinar las restricciones generales que se imponen sobre el proyecto
- Determinar el dominio, alcance o perímetro del proyecto

PAR: Proyecto de análisis de riesgos
PAR.1: Actividades preliminares
PAR.12: Determinación del alcance del proyecto

Productos de entrada

- Recopilación de la documentación pertinente de la Organización

Productos de salida

- Especificación detallada de los objetivos del proyecto
- Relación de restricciones generales
- Relación de unidades de la Organización que se verán afectadas como parte del proyecto
- Lista de roles relevantes en la unidades incluidas en el alcance del proyecto
- los activos esenciales
- los puntos de interconexión con otros sistemas
- los proveedores externos

Técnicas, prácticas y pautas

- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- *31010:B.1: Brainstorming*
- *31010:B.2: Structured or semi-structured interviews*
- *31010:B.3: Delphi technique*

Participantes

- El comité de seguimiento

Un proyecto de análisis de riesgos puede perseguir objetivos a muy corto plazo tales como el aseguramiento de cierto sistema o un cierto proceso de negocio, o puede pretender objetivos más amplios como fuera el análisis global de la seguridad de la Organización. En todo caso, hay que determinarlo.

Especialmente a la hora de tomar acciones correctoras, hay que tener en cuenta que “no todo vale”, sino que el proyecto se encontrará con una serie de restricciones, no necesariamente técnicas, que establecen un marco al que atenerse. Para incorporar las restricciones al análisis y gestión de riesgos, estas se agrupan por distintos conceptos, típicamente:

Restricciones políticas o gerenciales

Típicas de organizaciones gubernamentales o fuertemente relacionadas con organismos gubernamentales, bien como proveedores o como suministradores de servicios.

Restricciones estratégicas

Derivadas de la evolución prevista de la estructura u objetivos de la Organización.

Restricciones geográficas

Derivadas de la ubicación física de la Organización o de su dependencia de medios físicos de comunicaciones. Islas, emplazamientos fuera de las fronteras, etc.

Restricciones temporales

Que toman en consideración situaciones coyunturales: conflictividad laboral, crisis internacional, cambio de la propiedad, reingeniería de procesos, etc.

Restricciones estructurales

Tomando en consideración la organización interna: procedimientos de toma de decisiones, dependencia de casas matrices internacionales, etc.

Restricciones funcionales

Que tienen en cuenta los objetivos de la Organización.

Restricciones legales

Leyes, reglamentos, regulaciones sectoriales, contratos externos e internos, etc.

Restricciones relacionadas con el personal

Perfiles laborales, compromisos contractuales, compromisos sindicales, carreras profesionales, etc.

Restricciones metodológicas

Derivadas de la naturaleza de la organización y sus hábitos o habilidades de trabajo que pueden imponer una cierta forma de hacer las cosas.

Restricciones culturales

La “cultura” o forma interna de trabajar puede ser incompatible con ciertas salvaguardas teóricamente ideales.

Restricciones presupuestarias

La cantidad de dinero es importante; pero también la forma de planificar el gasto y de ejecutar el presupuesto

Alcance

Esta tarea identifica las unidades objeto del proyecto y especifica las características generales de dichas unidades en cuanto a responsables, servicios proporcionados y ubicaciones geográficas. También identifica las principales relaciones de las unidades objeto del proyecto con otras entidades, por ejemplo el intercambio de información en diversos soportes, el acceso a medios informáticos comunes, etc.

La tarea presume un principio básico: el análisis y la gestión de riesgos debe centrarse en un dominio limitado, que puede incluir varias unidades o mantenerse dentro de una sola unidad (según la complejidad y el tipo de problema a tratar), ya que un proyecto de ámbito demasiado amplio o indeterminado podría ser inabarcable, por excesivamente generalista o por demasiado extendido en el tiempo, con perjuicio en las estimaciones de los elementos del análisis.

Para que el alcance quede determinado debemos concretar:

- **los activos esenciales**: información que se maneja y servicios que se prestan
- **los puntos de intercambio** de interconexión con otros sistemas, aclarando qué información se intercambia y qué servicios se prestan mutuamente
- **los proveedores externos** en los que se apoya nuestro sistema de información

5.2.3. Tarea PAR.13: Planificación del proyecto

Proyecto de análisis de riesgos
PAR.1: Actividades preliminares
PAR.13: Planificación del proyecto

Objetivos

- Definir los grupos de interlocutores: usuarios afectados en cada unidad
- Planificar las entrevistas de recogida de información
- Determinar el volumen de recursos necesarios para la ejecución del proyecto: humanos, temporales y financieros
- Elaborar el calendario concreto de realización de las distintas etapas, actividades y tareas del proyecto
- Establecer un calendario de seguimiento que defina las fechas tentativas de reuniones del comité de dirección, el plan de entregas de los productos del proyecto, las posibles modificaciones en los objetivos marcados, etc

Productos de entrada

- Resultados de la actividad A1.2, Determinación del alcance del proyecto

Productos de salida

- Relación de participantes en los grupos de interlocutores
- Plan de entrevistas
- Informe de recursos necesarios
- Informe de cargas

Técnicas, prácticas y pautas

- Planificación de proyectos

Participantes

- El director de proyecto
- El comité de seguimiento

El plan de entrevistas debe detallar a qué persona se va a entrevistar, cuándo y con qué objetivo. Este plan permite determinar la carga que el proyecto va a suponer para las unidades afectadas, bien del dominio, bien del entorno.

El plan de entrevistas es especialmente importante cuando los sujetos a entrevistar se hayan en diferentes localizaciones geográficas y la entrevista requiere el desplazamiento de una o ambas partes.

También conviene ordenar las entrevistas de forma que primero se recaben las opiniones más técnicas y posteriormente las gerenciales, de forma que el entrevistador pueda evolucionar las preguntas tomando en consideración hechos (experiencia histórica) antes que valoraciones y perspectivas de servicio a terceros.

5.2.4. Tarea PAR.14: Lanzamiento del proyecto

Esta actividad completa las tareas preparatorias del lanzamiento del proyecto: empezando por seleccionar y adaptar los cuestionarios que se utilizarán en la recogida de datos y por realizar la campaña informativa de sensibilización a los implicados.

Proyecto de análisis de riesgos *PAR.1: Actividades preliminares* *PAR.14: Lanzamiento del proyecto*
Objetivos • Disponer de los elementos de trabajo para acometer el proyecto
Productos de entrada • Marco de trabajo establecido en el Proceso de Gestión de Riesgos: criterios y relaciones con las partes afectadas
Productos de salida • Cuestionarios adaptados • Determinar el catálogo de tipos de activos • Determinar las dimensiones de valoración de activos • Determinar los niveles de valoración de activos, incluyendo una guía unificada de criterios para asignar un cierto nivel a un cierto activo • Determinar los niveles de valoración de las amenazas: frecuencia y degradación • Asignar los recursos necesarios (humanos, de organización, técnicos, etc.) para la realización del proyecto • Informar a las unidades afectadas • Crear un ambiente de conocimiento general de los objetivos, responsables y plazos
Técnicas, prácticas y pautas • Cuestionarios (ver "Catálogo de Elementos")
Participantes • El director del proyecto • El equipo de proyecto

La tarea adapta los cuestionarios a utilizar en la recogida de información en el proceso P1 en función de los objetivos del proyecto, del dominio y de los temas a profundizar con los usuarios.

Los cuestionarios se adaptan con el objetivo de identificar correctamente los elementos de trabajo: activos, amenazas, vulnerabilidades, impactos, salvaguardas existentes, restricciones generales, etc. en previsión de las necesidades de las actividades A2.1 (caracterización de los activos), A2.2 (caracterización de las amenazas) y A2.3 (caracterización de las salvaguardas).

La necesidad de una adaptación siempre existe (debido al amplísimo espectro de los problemas de seguridad que puede y debe tratar Magerit). Pero el grado mayor o menor de adaptación depende además de las condiciones en que se realice la explotación de dichos cuestionarios. No habrá la misma profundidad de adaptación para entrevistas guiadas por el especialista en seguridad, que para cuestionarios auto administrados por el responsable del dominio o por los usuarios de sus sistemas de información.

5.3. PAR.2 – Elaboración del análisis de riesgos

Se siguen los pasos del método descrito en el capítulo X anterior.

La mayor parte de las tareas requerirán dos o tres entrevistas con los interlocutores apropiados:

— una primera entrevista para exponer las necesidades y recabar los datos

— una segunda entrevista para validar que los datos son completos y se han entendido correctamente

— según las circunstancias puede ser necesaria alguna entrevista adicional si la validación levanta muchas inexactitudes o dudas

El todas estas tareas debe procurarse manejar documentación escrita sometida a un proceso formal de gestión; es decir, aprobada y con unos procedimientos de revisión continua. La información de carácter verbal o informal debe limitarse a facilitar la comprensión, no a transmitir elementos sustanciales que no están documentados en parte alguna.

5.4. PAR.3 – Comunicación de resultados

La salida de la fase de análisis es la entrada de la fase de tratamiento. Para la tomar decisiones de tratamiento es necesario conocer tanto los indicadores residuales como los indicadores potenciales de impacto y riesgo. Y para cada escenario de riesgo es necesario disponer de información suficiente para poder entender en qué consiste el riesgo, así como su dinámica y los razonamientos o la base de las estimaciones empleadas para derivar resultados. No basta conocer el valor final del indicador, sino que hay que poder analizar el por qué de ese valor.

Por otra parte, las decisiones de tratamiento pueden requerir la realización de modificaciones del análisis de riesgo. Frecuentemente es necesario analizar situaciones hipotéticas (¿qué ocurriría si …?) para poder optar por una decisión u otra. Es por ello que es fundamental el soporte de herramientas que automaticen el cálculo.

Para el informe ejecutivo final basta destacar gráficamente los escenarios de mayor impacto, de mayor nivel de riesgo y combinaciones peligrosas de ambos indicadores (ver los cuadrantes o zonas más arriba).

5.5. Control del proyecto

5.5.1. Hitos de control

Hito de control H1.1:

La Dirección procederá a la aprobación o no de la realización del proyecto de análisis de riesgos, basándose en el estudio de oportunidad realizado por el promotor.

Hito de control H1.2:

El comité de seguimiento del proyecto validará el informe de "Planificación del Proyecto de Análisis de Riesgos" que contendrá una síntesis de los productos obtenidos en las actividades realizadas en el proceso P1.

5.5.2. Documentación resultante

Documentación intermedia

- Resultados de las entrevistas.
- Documentación de otras fuentes: estadísticas, observaciones de expertos y observaciones de los analistas.
- Documentación auxiliar: planos, organigramas, requisitos, especificaciones, análisis funcionales, cuadernos de carga, manuales de usuario, manuales de explotación, diagramas de flujo de información y de procesos, modelos de datos, etc.
- Análisis de los resultados, con la detección de las áreas críticas claves.
- Información existente utilizable por el proyecto (por ejemplo inventario de activos)
- Resultados de posibles aplicaciones de métodos de análisis y gestión de riesgos realizadas anteriormente (por ejemplo catalogación, agrupación y valoración de activos, amenazas, vulnerabilidades, impactos, riesgo, mecanismos de salvaguarda, etc.).

Documentación final

- Modelo de valor: identificación de activos junto con sus dependencias y valoración propia y acumulada
- Mapa de amenazas junto con sus consecuencias y probabilidad de ocurrencia.
- Documento de aplicabilidad de las salvaguardas.
- Informe de valoración de la efectividad de las salvaguardas presentes.
- Informe de insuficiencias o debilidades del sistema de salvaguardas.
- Indicadores de impacto y riesgo, potenciales y residuales.

6. Plan de seguridad

Esta sección trata de cómo llevar a cabo planes de seguridad, entendiendo por tales proyectos para materializar las decisiones adoptadas para el tratamiento de los riesgos.

Estos planes reciben diferentes nombres en diferentes contextos y circunstancias:

- plan de mejora de la seguridad
- plan director de seguridad
- plan estratégico de seguridad
- plan de adecuación (en concreto es el nombre que se usa en el ENS)

Se identifican 3 tareas:

PS – Plan de Seguridad
PS.1 – Identificación de proyectos de seguridad PS.2 – Plan de ejecución PS.3 – Ejecución

6.1. Tarea PS.1: Identificación de proyectos de seguridad

Se traducen las decisiones de tratamiento de los riesgos en acciones concretas.

PS: Plan de seguridad ***PS.1: Identificación de proyectos de seguridad***
Objetivos • Elaborar un conjunto armónico de programas de seguridad
Productos de entrada • Resultados de las actividades de análisis y tratamiento de riesgos • Conocimientos de técnicas y productos de seguridad • Catálogos de productos y servicios de seguridad
Productos de salida • Relación de programas de seguridad
Técnicas, prácticas y pautas • Planificación de proyectos
Participantes • El equipo de proyecto • Especialistas en seguridad • Especialistas en áreas específicas de seguridad

En última instancia se trata de implantar o mejorar la implantación de una serie de salvaguardas que lleven impacto y riesgo a los niveles residuales determinados por la Dirección. Este tratamiento de las salvaguardas se materializa en una serie de tareas a llevar a cabo.

Un programa de seguridad es una agrupación de tareas. La agrupación se realiza por conveniencia, bien porque se trata de tareas que en singular carecerían de eficacia, bien porque se trata de

tareas con un objetivo común, bien porque se trata de tareas que competen a una única unidad de acción.

Cada programa de seguridad debe detallar:

- Su objetivo genérico.
- Las salvaguardas concretas a implantar o mejorar, detallando sus objetivos de calidad, eficacia y eficiencia
- La relación de escenarios de impacto y/o riesgo que afronta: activos afectados, tipos de activos, amenazas afrontadas, valoración de activos y amenazas y niveles de impacto y riesgo
- La unidad responsable de su ejecución.
- Una estimación de costes, tanto económicos como de esfuerzo de realización, teniendo en cuenta:
  - costes de adquisición (de productos), o de contratación (de servicios), o de desarrollo (de soluciones llave en mano), pudiendo ser necesario evaluar diferentes alternativas
  - costes de implantación inicial y mantenimiento en el tiempo
  - costes de formación, tanto de los operadores como de los usuarios, según convenga al caso
  - costes de explotación
  - impacto en la productividad de la Organización
- Una relación de subtareas a afrontar, teniendo en cuenta
  - cambios en la normativa y desarrollo de procedimientos
  - solución técnica: programas, equipos, comunicaciones e instalaciones,
  - plan de despliegue
  - plan de formación
- Una estimación del tiempo de ejecución desde su arranque hasta su puesta en operación.
- Una estimación del estado de riesgo (impacto y riesgo residual a su compleción).
- Un sistema de indicadores de eficacia y eficiencia que permitan conocer en cada momento la calidad del desempeño de la función de seguridad que se desea y su evolución temporal.

Las estimaciones anteriores pueden ser muy precisas en los programas sencillos; pero pueden ser simplemente orientativas en los programas complejos que conlleven la realización de un proyecto específico de seguridad. En este último caso, cada proyecto desarrollará los detalles últimos por medio de una serie de tareas propias de cada proyecto que, en líneas generales responderán a los siguientes puntos:

- Estudio de la oferta del mercado: productos y servicios.
- Coste de un desarrollo específico, propio o subcontratado.
- Si se estima adecuado un desarrollo específico hay que determinar:
  - la especificación funcional y no-funcional del desarrollo
  - el método de desarrollo que garantice la seguridad del nuevo componente
  - los mecanismos de medida (controles) que debe llevar empotrados
  - los criterios de aceptación
  - el plan de mantenimiento: incidencias y evolución

6.2. Tarea PS.2: Planificación de los proyectos de seguridad

PS: Plan de seguridad ***PS.2: Plan de ejecución***
Objetivos • Ordenar temporalmente los programas de seguridad
Productos de entrada • Resultados de las actividades de análisis y tratamiento de riesgos • Resultados de la tarea PS.1 Programas de seguridad
Productos de salida • Cronograma de ejecución del plan • **Plan de Seguridad**
Técnicas, prácticas y pautas • Análisis de riesgos (ver “Método de Análisis de Riesgos”) • Planificación de proyectos
Participantes • Departamento de desarrollo • Departamento de compras

Hay que ordenar en el tiempo los proyectos de seguridad teniendo en cuenta los siguientes factores:

- la criticidad, gravedad o conveniencia de los impactos y/o riesgos que se afrontan, teniendo máxima prioridad los programas que afronten situaciones críticas
- el coste del programa
- la disponibilidad del personal propio para responsabilizarse de la dirección (y, en su caso, ejecución) de las tareas programadas
- otros factores como puede ser la elaboración del presupuesto anual de la Organización, las relaciones con otras organizaciones, la evolución del marco legal, reglamentario o contractual, etc.

Típicamente un plan de seguridad se planifica en tres niveles de detalle:

Plan director (uno).

A menudo denominado “plan de actuación”, trabaja sobre un periodo largo (típicamente entre 3 y 5 años), estableciendo las directrices de actuación.

Plan anual (una serie de planes anuales).

Trabaja sobre un periodo corto (típicamente entre 1 y 2 años), estableciendo la planificación de los programas de seguridad.

Plan de proyecto (un conjunto de proyectos con su planificación).

Trabaja en el corto plazo (típicamente menos de 1 año), estableciendo el plan detallado de ejecución de cada programa de seguridad.

Se debe desarrollar un (1) plan director único, que es el que da perspectiva y unidad de objetivos a las actuaciones puntuales. Este plan director permite ir desarrollando planes anuales que, dentro del marco estratégico, van estructurando la asignación de recursos para la ejecución de las tareas, en particular partidas presupuestarias. Y, por último, habrá una serie de proyectos que materializan los programas de seguridad.

6.3. Tarea PS.3: Ejecución del plan

PS: Plan de seguridad ***PS.3: Ejecución***
Objetivos • Alcanzar los objetivos previstos en el plan de seguridad para cada proyecto planificado
Productos de entrada • Resultados de las actividades PS.1 (proyectos de seguridad) y PS.2 (planificación) • Proyecto de seguridad que nos ocupa
Productos de salida • Salvaguardas implantadas • Normas de uso y procedimientos de operación • Sistema de indicadores de eficacia y eficiencia del desempeño de los objetivos de seguridad perseguidos • Modelo de valor actualizado • Mapa de riesgos actualizado • Estado de riesgo actualizado (impacto y riesgo residuales).
Técnicas, prácticas y pautas • Análisis de riesgos (ver “Método de Análisis de Riesgos”) • Planificación de proyectos
Participantes • El equipo de proyecto: evolución del análisis de riesgos • Personal especializado en la salvaguarda en cuestión

6.4. Lista de control de los planes de seguridad

√	**actividad**	**tarea**
	Se han definido los proyectos constituyentes	PS.1
	Se han definido las interdependencias entre proyectos (necesidades de que uno avance para que progrese otro)	PS.1
	Se han asignado recursos — disponibles para los proyectos en curso — previstos para los proyectos que seguirán en el futuro	PS.2
	Se han definido roles y responsabilidades	PS.1
	Se ha establecido un calendario de ejecución	PS.2
	Se han definido indicadores de progreso	PS.3
	Se han previsto necesidades de concienciación y formación	PS.1
	Se han previsto necesidades de documentación: — normativa de seguridad y — procedimientos operativos de seguridad	PS.1

7. Desarrollo de sistemas de información

Las aplicaciones *(software)* constituyen un tipo de activos frecuente y nuclear para el tratamiento de la información en general y para la prestación de servicios basados en aquella información. La presencia de aplicaciones en un sistema de información es siempre una fuente de riesgo en el sentido de que constituyen un punto donde se pueden materializar amenazas. A veces, además, las aplicaciones son parte de la solución en el sentido de que constituyen una salvaguarda frente a riesgos potenciales. En cualquier caso es necesario que el riesgo derivado de la presencia de aplicaciones esté bajo control.

El análisis de los riesgos constituye una pieza fundamental en el diseño y desarrollo de sistemas de información seguros. Es posible, e imperativo, incorporar durante la fase de desarrollo las funciones y mecanismos que refuerzan la seguridad del nuevo sistema y del propio proceso de desarrollo, asegurando su consistencia y seguridad, completando el plan de seguridad vigente en la Organización. Es un hecho reconocido que tomar en consideración la seguridad del sistema antes y durante su desarrollo es más efectivo y económico que tomarla en consideración a posteriori. La seguridad debe estar embebida en el sistema desde su primera concepción.

El Esquema Nacional de Seguridad recoge el riesgo como pieza fundamental de la seguridad de los sistemas en varios de sus principios básicos:

Artículo 5. La seguridad como un proceso integral.

1. La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.
2. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

Artículo 6. Gestión de la seguridad basada en los riesgos.

1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

Artículo 9. Reevaluación periódica.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

Durante el desarrollo de un sistema de información, se pueden identificar dos tipos de actividades diferenciadas:

- **SSI**: actividades relacionadas con la propia seguridad del sistema de información que se está desarrollando.
- **SPD**: actividades que velan por la seguridad del proceso de desarrollo del sistema de información.

7.1. Inicialización de los procesos

Hay varias razones que pueden llevar a plantear el desarrollo de un nuevo sistema de información o la modificación de uno ya existente:

Nuevos servicios y/o datos.

- Requiere el desarrollo de un nuevo sistema o la modificación de un sistema ya operativo. Puede implicar la desaparición de partes actualmente operativas.
- La iniciativa la lleva el responsable de desarrollo, actuando el responsable de seguridad como subsidiario.

Evolución tecnológica. Las tecnologías TIC se encuentran en evolución continua, pudiendo presentarse cambios en las técnicas de desarrollo de sistemas, en los lenguajes o las plataformas de desarrollo, en las plataformas de explotación, en los servicios de explotación, en los servicios de comunicaciones, etc.

- Requiere el desarrollo de un nuevo sistema o la modificación de un sistema ya operativo. Puede implicar la desaparición de partes actualmente operativas.
- La iniciativa la lleva el responsable de desarrollo, actuando el responsable de seguridad como subsidiario.

Modificación de la calificación de seguridad de servicios o datos.

- Típicamente requiere la modificación de un sistema ya operativo. Raramente implica el desarrollo de un nuevo sistema o la desaparición de partes actualmente operativas.
- La iniciativa la lleva el responsable de seguridad, actuando el responsable de sistemas como subsidiario.

Consideración de nuevas amenazas. La evolución de las tecnologías y los servicios de comunicaciones pueden habilitar nuevas amenazas o convertir amenazas que eran despreciables en el pasado en amenazas relevantes en el futuro.

- Típicamente requiere la modificación del sistema, bien en sus componentes o, más frecuentemente, en sus condiciones de explotación. Raramente implica el desarrollo de un nuevo sistema o la desaparición de partes actualmente operativas.
- La iniciativa la lleva el responsable de seguridad, actuando el responsable de sistemas como subsidiario.

Modificación de los cri terios de calificación de riesgos. Puede venir inducido por criterios de calidad operativa, por novedades en la legislación aplicable, en la reglamentación sectorial o por acuerdos o contratos con terceros.

- Típicamente requiere la modificación del sistema. Raramente implica el desarrollo de un nuevo sistema o la desaparición de partes actualmente operativas.
- La iniciativa la lleva el responsable de seguridad, actuando el responsable de sistemas como subsidiario.

7.2. SSI – Seguridad del sistema de información

Toda la existencia de un sistema de información puede verse como etapas de concreción creciente, desde una perspectiva muy global durante los procesos de planificación hasta una visión en detalle durante el desarrollo y explotación. No obstante, este ciclo de vida no es lineal, sino que frecuentemente habrá que tantear opciones alternativas y revisar decisiones tomadas.

El análisis de riesgos debe basar sus estimaciones de impacto y riesgo en la realidad de los sistemas, concretada en sus activos. En consecuencia, se puede entender el modelo de valor como evolutivo, recogiendo en cada momento el nivel de detalle de que se dispone. Magerit, como metodología, permite un tratamiento sistemático y homogéneo que es esencial para poder comparar opciones alternativas y para gestionar la evolución de los sistemas.

Como principio básico debe considerarse que el análisis de los riesgos debe seguir fielmente la realidad del sistema de información y su contexto, facilitando el mejor análisis de riesgos posible para poder tomar decisiones de tratamiento adecuadas a cada momento.

7.2.1. Ciclo de vida de las aplicaciones

Típicamente, una aplicación sigue un ciclo de vida a través de varias fases:

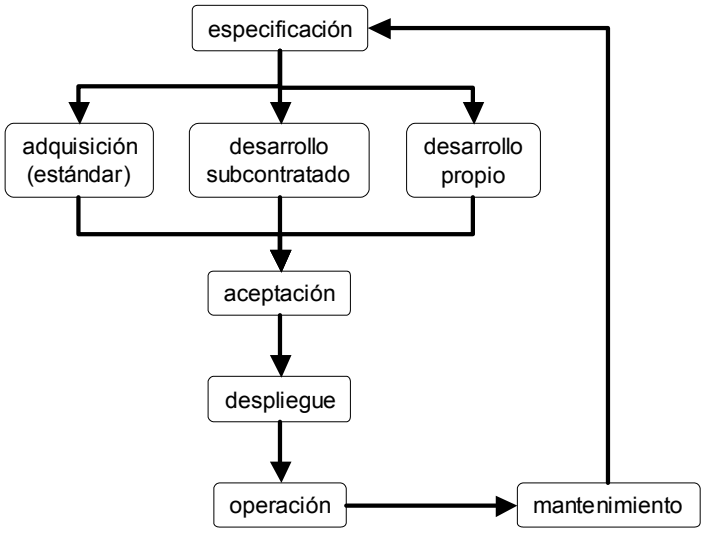

Ilustración 16. Ciclo de vida de las aplicaciones

Especificación. En esta fase se determinan los requisitos que debe satisfacer la aplicación y se elabora un plan para las siguientes fases.

Adquisición o desarrollo. Para traducir una especificación en una realidad, se puede adquirir un producto, o se puede desarrollar, bien en casa, bien por subcontratación externa.

Aceptación. Tanto si es una aplicación nueva como si es modificación de una aplicación anterior, nunca una aplicación debe entrar en operación sin haber sido formalmente aceptada.

Despliegue. Consistente en instalar el código en el sistema y configurarlo para que entre en operación.

Operación. La aplicación se usa por parte de los usuarios, siendo atendidos los incidentes por parte de usuarios y/o los operadores.

Mantenimiento. Bien porque aparecen nuevos requisitos, bien porque se ha detectado un fallo, la aplicación puede requerir un mantenimiento que obligue a regresar a cualquiera de las etapas anteriores, en última instancia a la especificación básica.

MÉTRICA versión 3

La metodología MÉTRICA Versión 3 ofrece a las Organizaciones un instrumento para la sistematización de las actividades que dan soporte al ciclo de vida del *software*. MÉTRICA versión 3 identifica los siguientes elementos:

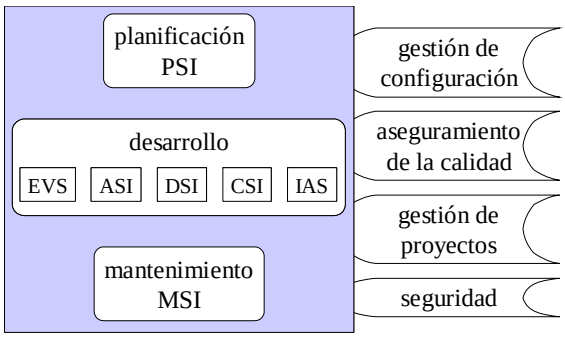

Ilustración 17. Métrica 3 - Actividades

Métrica 3

especificación	PSI – Planificación del sistema de información EVS – Estudio de viabilidad del sistema ASI – Análisis del sistema de información
adquisición o desarrollo	DSI – Diseño del sistema de información. CSI – Construcción del sistema de información
aceptación	IAS – Implantación y aceptación del sistema
despliegue	
operación	
mantenimiento	MSI – Mantenimiento del sistema de información

Tabla 7. Ciclo de vida y actividades en Métrica 3

7.2.2. Contexto

Se debe determinar el contexto general:

- política de seguridad y normas
- requisitos de cumplimiento normativo
- obligaciones contractuales
- roles y funciones
- criterios de valoración de información y servicios
- criterios de valoración de riesgos
- criterios de aceptación de riesgos

En particular, hay que establecer unos procedimientos operativos que instrumenten la comunicación entre las tareas de desarrollo y las tareas de análisis y tratamiento de riesgos.

- La Dirección aporta los servicios necesarios y la calidad de la seguridad deseada.
- El equipo de desarrollo aporta los elementos técnicos que materializan la aplicación.
- El equipo de análisis de riesgos aporta un juicio crítico sobre la seguridad del sistema.
- La misma Dirección aprueba el riesgo residual.

7.2.3. Fase de especificación: adquisición de datos

Se debe recopilar información sobre

- la información esencial y sus requisitos de seguridad

— los servicios esenciales y sus requisitos de seguridad

— el contexto en el que se va a desarrollar y explotar el sistema

En particular se debe establecer un perfil de amenazas, sean naturales, del entorno o de origen humano, sean accidentales o deliberadas. La caracterización del potencial del atacante debe formar parte de las especificaciones del diseño y su modificación más adelante en el ciclo de vida del sistema será objeto de un nuevo análisis y decisión de tratamiento.

7.2.4. Fase de diseño: estudio de opciones

La toma de decisiones de tratamiento de los riesgos puede recomendar salvaguardas evaluando su efecto en los indicadores de impacto y riesgo. Las decisiones que se adopten dependerán de los criterios establecidos en la política de seguridad de la Organización y de otras consideraciones específicas de cada caso. Si bien la política de seguridad establece un marco de referencia que no puede violentarse, es habitual que no prevea todos los detalles técnicos y coyunturales del servicio para tomar decisiones precisas.

Debido a la interrelación entre los elementos que constituyen un sistema, no es suficiente proteger un cierto tipo de activos para proteger el conjunto. Por ello, la toma de decisiones de tratamiento es local sobre una parte del sistema, pero siempre con un análisis global sobre la seguridad del conjunto.

Análisis y tratamiento de los riesgos

La seguridad requerida para la información que se maneja y los servicios que se prestan quedó fijada en la fase de especificación y no se puede modificar ahora.

El equipo de desarrollo y el equipo de análisis de riesgos trabajan de forma iterativa hasta encontrar una solución que satisfaga a ambas partes. Normalmente la iniciativa la toma el equipo de desarrollo proponiendo una solución técnica que responda a los requisitos funcionales del sistema. El equipo de seguridad analiza la propuesta informando de los riesgos asociados y, en su caso, proponiendo salvaguardas que pudieran dejar el riesgo en niveles aceptables. En la medida en que las salvaguardas propuestas afecten al diseño, el equipo rehará su propuesta para un nuevo análisis.

La especificación de salvaguardas debe incorporar tanto los mecanismos de actuación como los mecanismos de configuración, monitorización y control de su eficacia y eficiencia. Es frecuente que aparezcan algunos desarrollos específicamente destinados a configurar el conjunto de salvaguardas y a monitorizar su operación.

Es posible que el equipo de desarrollo pueda presentar dos o más opciones, en cuyo todas ellas serán evaluadas en lo que respecta a riesgo y salvaguardas requeridas. El informe de riesgos será un elemento más de decisión entre las diferentes opciones.

Cuando ambos equipos lleguen a una situación estable, con un diseño técnicamente viable, con un riesgo aceptable y unos requisitos aceptables de recursos, la propuesta se eleva para su aprobación.

Como resultado de esta fase, dispondremos de especificaciones técnicas de desarrollo acompañadas de un análisis de los riesgos y sus decisiones de tratamiento.

7.2.5. Soporte al desarrollo: puntos críticos

Durante el desarrollo hay que incorporar las salvaguardas aprobadas en la fase de diseño, así como controles que permitan monitorizar su eficacia. Estos requisitos de monitorización se suelen concretar en los siguientes aspectos:

— registros de actividad

— mecanismos para procesar estos registros e informar de la efectividad del sistema de protección

— disparo de alarmas cuando los hecho evidencian un problema de seguridad

El despliegue de estos elementos viene modulado por el nivel de riesgo potencial que se soporta en cada componente del sistema de información.

Durante el desarrollo conviene gestionar los riesgos según se indica en la sección relativa a “Seguridad del Proceso de Desarrollo” más adelante.

7.2.6. Aceptación y puesta en marcha: puntos críticos

Cuando el sistema se prueba antes de ponerlo en funcionamiento, debe revisarse que todos los registros de actividad funcionan correctamente, así como los sistemas de procesamiento y de alarma incorporados al sistema.

También debe comprobarse que el sistema responde al diseño previsto, concretamente que las salvaguardas están desplegadas, que su despliegue es efectivo y que no existen formas de circunvalarlas u obviarlas: es decir que el sistema no permite puertas traseras fuera de control.

Sistema(s) de identificación y autenticación:

— todo acceso al sistema requiere que el usuario se identifique y se autentique según lo previsto, bloqueando cualquier otra forma de acceso

— los mecanismos de identificación y autenticación están protegidos para evitar que un atacante pueda acceder a información o mecanismos que pongan en peligro su efectividad

Sistema(s) de control de acceso:

— todo acceso a la información y a los servicios verifica previamente que el usuario tiene las autorizaciones pertinentes

Servicios externalizados: cuando parte de la operación del sistema está delegada en un tercero:

— hay que revisar los contratos de prestación del servicio

— hay que revisar la completitud de los procedimientos de reporte y gestión de incidencias

Si el sistema no refleja el modelo cuyos riesgos han sido analizados, será rechazado sin pasar a producción.

Hay que verificar que la documentación de seguridad es clara y precisa. Esto incluye normativa, procedimientos operacionales, material de concienciación y de formación.

Sin poder ser exhaustivos, las siguientes líneas muestran pruebas de aceptación que conviene realizar:

— datos de prueba
  - si no son reales, deben ser realistas
  - si no se puede evitar que sean reales, hay que controlar copias y acceso

— pruebas funcionales (de los servicios de seguridad)
  - simulación de ataques: verificando que se detectan y reportan
  - pruebas en carga: verificando que no se obvian las medidas de protección
  - intrusión controlada (*hacking* ético)

— inspección de servicios / inspección de código
  - fugas de información: canales encubiertos, a través de los registros, etc.
  - puertas traseras de acceso
  - escalado de privilegios
  - problemas de desbordamiento de registros *(buffer overflow)*

7.2.7. Operación: análisis y gestión dinámicos

Durante la vida operativa del sistema podemos encontrarnos con cambios en el escenario que invalidan el análisis de riesgos realizado anteriormente. En entornos formales, el sistema requiere una re-acreditación para seguir operando bajo las nuevas condiciones.

Nuevas amenazas

Bien porque se descubren nuevas formas de ataque, bien porque la valoración de la capacidad del atacante se modifica. En estos casos hay que rehacer el análisis y decidir cómo tratar los nuevos resultados.

Vulnerabilidades sobrevenidas

Por ejemplo, defectos reportados por los fabricantes. En estos casos hay que analizar la nueva situación de riesgo y determinar cual es su tratamiento adecuado para seguir operando. Lo ideal es parchear el sistema; pero bien porque el parche no existe o porque su aplicación requiere unos recursos de los que no disponemos, podemos encontrarnos en una situación nueva ante la cual hay que decidir cómo tratar el riesgo.

Incidentes de seguridad

Los incidentes de seguridad pueden indicarnos un fallo en nuestra identificación de amenazas o en su valoración, obligando a revisar el análisis.

Un incidente de seguridad también puede suponer un cambio en el sistema. Por ejemplo, una intrusión significa que no podemos contar con la defensa perimetral: tenemos un nuevo sistema, con el atacante en un nuevo lugar y con unas opciones nuevas.

Cambios en la utilización del sistema

A veces un sistema ya operacional no se utiliza como estaba previsto:

- nueva información con diferentes requisitos de seguridad
- nuevos servicios con diferentes requisitos de seguridad
- nuevos procedimientos operativos

En términos del análisis de riesgos, esto significa una diferente valoración de los activos o de las salvaguardas desplegadas.

Es posible que la alteración del sistema en alguna de las facetas contempladas en los puntos anteriores lleve a unos niveles de riesgo que no sean aceptables, obligando a un ciclo de mantenimiento que rediseñe el sistema o parte de él.

7.2.8. Ciclos de mantenimiento: análisis marginal

Cuando se propone una modificación del sistema, los nuevos elementos deben llevar a un nuevo análisis de riesgos, regresando a los ciclos iterativos de propuestas y soluciones de la fase de diseño.

7.2.9 Terminación

Cuando un sistema de información se retira del servicio, hay que realizar una serie de tareas de seguridad proporcionadas al riesgo al que están sometidos los componentes del sistema a retirar. En concreto:

- proteger el valor de la información manejada: retención y control de acceso
- proteger las claves criptográficas de cifra y de autenticación: retención y control de acceso

Todo lo que no sea necesario retener se destruirá de forma segura:

- datos operacionales

— copias de seguridad

— configuración de los sistemas

7.2.10 Documentación de seguridad

La documentación de seguridad evoluciona con el ciclo de vida del sistema:

fase	documentación de seguridad
contexto	se revisa la política de seguridad se revisa la normativa de seguridad
especificación	se amplia la normativa de seguridad
diseño	se prepara el índice de procedimientos operacionales de seguridad
desarrollo	se elaboran los procedimientos operacionales de seguridad
aceptación y puesta en operación	se validan los procedimientos operacionales de seguridad
operación	se actualizan los procedimientos operacionales de seguridad
mantenimiento	se actualizan los procedimientos operacionales de seguridad

Tabla 8. Documentación de seguridad a lo largo del ciclo de vida de las aplicaciones

7.3. SPD – Seguridad del proceso de desarrollo

Lo que se comenta en esta sección afecta a todas y cada uno de los procesos y subprocesos de Métrica: PSI, EVS, ASI, DSI, CSI, IAS y MSI.

La interfaz de seguridad de Métrica identifica hasta 4 tareas que se repiten en cada proceso. Aquí se tratan de forma compacta:

Activos a considerar

En cada proceso se requiere un análisis de riesgos específico que contemple:

- los datos que se manejan:
  - especificaciones y documentación de los sistemas
  - código fuente
  - manuales del operador y del usuario
  - datos de prueba
- el entorno *software* de desarrollo:
  - herramientas de tratamiento de la documentación: generación, publicación, control de documentación, etc.
  - herramientas de tratamiento del código: generación, compilación, control de versiones, etc.
- el entorno *hardware* de desarrollo: equipos centrales, puestos de trabajo, equipos de archivo, etc.
- el entorno de comunicaciones de desarrollo
- las instalaciones
- el personal involucrado: desarrolladores, personal de mantenimiento y usuarios (de pruebas)

Actividades

Se siguen los siguientes pasos

1. el equipo de desarrollo expone a través del jefe de proyecto los elementos involucrados
2. el equipo de análisis de riesgos recibe a través del director de seguridad la información de los activos involucrados
3. el equipo de análisis de riesgos realiza el análisis
4. el equipo de análisis de riesgos expone a través de su director el estado de riesgo, proponiendo una serie de medidas a tomar
5. el equipo de desarrollo elabora un informe del coste que supondrían las medidas recomendadas, incluyendo costes de desarrollo y desviaciones en los plazos de entrega
6. la dirección califica el riesgo y decide las salvaguardas a implantar oyendo el informe conjunto de análisis de riesgos y coste de las soluciones propuestas
7. el equipo de análisis de riesgos elabora los informes correspondientes a las soluciones adoptadas
8. el equipo de seguridad elabora la normativa de seguridad pertinente
9. la dirección aprueba el plan para ejecutar el proceso con la seguridad requerida

Resultados del análisis y gestión de riesgos

En todos los casos

- salvaguardas recomendadas
- normas y procedimientos de tratamiento de la información

Otras consideraciones

Aunque cada proceso requiere su análisis de riesgos específico, es cierto que se trata de modelos tremendamente similares por lo que el mayor esfuerzo lo llevará el primero que se haga, siendo los demás adaptaciones de aquel primero.

En los primeros procesos, notablemente en PSI, pueden aparecer contribuciones de alto nivel que afecten a la normativa de seguridad de la Organización e incluso a la propia política de seguridad corporativa.

Entre las normas y procedimientos generados es de destacar la necesidad de una normativa de clasificación de la documentación y procedimientos para su tratamiento.

En todos los procesos hay que prestar una especial atención al personal involucrado. Como reglas básicas conviene:

- identificar los roles y las personas
- determinar los requisitos de seguridad de cada puesto e incorporarlos a los criterios de selección y condiciones de contratación
- limitar el acceso a la información: sólo por necesidad
- segregar tareas; en particular evitar la concentración en una sola persona de aquellas aplicaciones o partes de una aplicación que soporten un alto riesgo

7.4. Referencias

- “Seguridad de las Tecnologías de la Información. La construcción de la confianza para una sociedad conectada”, E. Fernández-Medina y R. Moya (editores). AENOR, 2003.
- Metodología de Planificación, Desarrollo y Mantenimiento de sistemas de información. Métrica v3. Consejo Superior de Informática y para el Impulso de la Administración Electrónica, 2000.

8. Consejos prácticos

Todo el planteamiento anterior puede quedar un poco abstracto y no permitir al analista progresar con solvencia a través de los pasos indicados si confundiera lo importante con lo esencial. Por ello se ha considerado conveniente incluir algunos comentarios que puedan servir de guía para avanzar.

Se recomienda también la consulta del "Catálogo de Elementos" que recopila tipos de activos, dimensiones de valoración, guías de valoración, catálogos de amenazas y de salvaguardas.

8.1. Alcance y profundidad

Magerit cubre un espectro muy amplio de intereses de sus usuarios. En el planteamiento de estas guías se ha seguido un criterio “de máximos”, reflejando todo tipo de activos, todo tipo de aspectos de seguridad; en definitiva, todo tipo de situaciones. En la práctica, el usuario puede encontrarse ante situaciones donde el análisis es más restringido. Siguen algunos casos prácticos frecuentes:

- sólo se requiere un estudio de los ficheros afectos a la legislación de datos de carácter personal
- sólo se requiere un estudio de las garantías de confidencialidad de la información
- sólo se requiere un estudio de la seguridad de las comunicaciones
- sólo se requiere un estudio de la seguridad perimetral
- sólo se requiere un estudio de la disponibilidad de los servicios (típicamente porque se busca el desarrollo de un plan de contingencia)
- se busca una homologación o acreditación del sistema o de un producto
- se busca lanzar un proyecto de métricas de seguridad, debiendo identificar qué puntos interesa controlar y con qué grado de periodicidad y detalle
- etc.

Estas situaciones, frecuentes, se traducen en un ajuste del alcance del análisis. Una estrategia frecuente es identificar como servicio a proporcionar el ámbito que deseamos analizar en detalle y usarlo como perímetro exterior de los activos, incorporando directamente valoraciones inferidas de la información que se maneja y la calidad que se espera del servicio.

Además de cubrir un dominio más o menos extenso, pueden darse situaciones en las que se requieren análisis de diferente calado:

- un análisis urgente para determinar los activos críticos
- un análisis global para determinar las medidas generales
- un análisis de detalle para determinar salvaguardas específicas para ciertos elementos del sistema de información
- un análisis de detalle cuantitativo para determinar la oportunidad de un gasto elevado
- ...

En resumen, las tareas que a continuación se detallan hay que adaptarlas

1. horizontalmente al alcance que se requiere (tarea MAR.1)
2. verticalmente a la profundidad oportuna

8.2. Para identificar activos

Conviene repetir que sólo interesan los recursos de los sistemas de información que tienen un valor para la Organización, bien en sí mismos, bien porque sobre sus hombros descansan activos de valor.

A título de ejemplo, un servidor de presentación web es un activo de escaso valor propio. Esto puede asegurarse porque no es normal que una Organización despliegue un servidor de presentación web salvo que lo necesite para prestar un servicio. Todo su valor es imputado:

- la indisponibilidad del servidor supone la interrupción del servicio; el coste que suponga la interrupción del servicio es el valor de disponibilidad que se le imputará al servidor
- el acceso no controlado al servidor pone en riesgo el secreto de los datos que presenta; el coste que suponga la pérdida de confidencialidad de los datos es el valor de confidencialidad que se le imputará al servidor
- ... y así con las diferentes dimensiones en consideración

Los intangibles

Ciertos elementos de valor de las organizaciones son de naturaleza intangible:

- credibilidad o buena imagen
- conocimiento acumulado
- independencia de criterio o actuación
- intimidad de las personas
- integridad física de las personas

Estos elementos pueden incorporarse al análisis de riesgos como activos[26] o como elementos de valoración[27]. La cuantificación de estos conceptos es a menudo difícil; pero de una u otra forma nunca puede olvidarse que lo que hay que proteger en última instancia es la misión de la Organización y el valor de ésta reside en estos intangibles como ya se reconocía en Magerit versión 1.0[28].

Identificación de activos

Quizás la mejor aproximación para identificar los activos sea preguntar directamente:

- ¿Qué activos son esenciales para que usted consiga sus objetivos?
- ¿Hay más activos que tenga que proteger por obligación legal?
- ¿Hay activos relacionados con los anteriores?

Lo esencial es siempre la información que se maneja y los servicios que se prestan. A veces nos interesa singularizar la diferente información y los diferentes servicios, mientras que otras veces podemos agrupar varias informaciones o varios servicios que son equivalentes a efectos de requisitos de seguridad. Incluso es frecuente hacer paquetes de { información + servicios } que la Dirección entiende como un uno.

No siempre es evidente qué es un activo en singular.

---

26 No todos los autores son unánimes en que sea una buena idea identificar activos intangibles. Es cierto que son activos en el sentido financiero; pero es discutible que sean recursos propiamente dichos del sistema de información. Ocurre que si a los interlocutores se les pregunta durante las entrevistas en términos de valores intangibles de la Organización, se pierde la perspectiva del día a día, pues la mayor parte de los miembros de la Organización tienen objetivos más concretos y cercanos sobre los que sí pueden emitir una opinión fundada.

27 Ver “Catálogo de Elementos”, capítulo “4. Criterios de valoración”.

28 Ver Magerit versión 1.0, “Guía de Procedimientos” / “3. Submodelo de Elementos” / “3.4. Impactos” / ”3.4.3. Tipos”.

Es habitual y práctico identificar lo que podríamos llamar subsistemas. Un subsistema típico es un equipo informático, que bajo ese nombre contiene el *hardware*, los soportes de información (discos), periféricos, sistema operativo y aplicaciones (*software*) de base tales como ofimática, antivirus, etc. Si es posible, trate ese conglomerado como un activo único.

Si por ejemplo en su unidad tiene 300 puestos de trabajo PC, todos idénticos a efectos de configuración y datos que manejan, no es conveniente analizar 300 activos idénticos. Baste analizar un PC genérico que cuya problemática representa la de todos. Agrupar simplifica el modelo. Una buena idea es tener tantos activos como perfiles de configuración de equipos personales.

Otras veces se presenta el caso contrario, un servidor central que se encarga de mil funciones: servidor de ficheros, de mensajería, de la intranet, del sistema de gestión documental y ... En este caso conviene segregar los servicios prestados como servicios (internos) independientes. Sólo cuando se llegue al nivel de equipamiento físico habrá que hacer confluir en un único equipo todos los servicios. Si en el futuro se consigue segregar servicios entre varios servidores, entonces es fácil revisar el modelo de valor y dependencias.

Durante la fase de identificación de activos es frecuente que haya ciclos de expansión en los que los activos complejos se desagregan en activos más sencillos, y fases de compresión, en las que muchos activos se agrupan bajo un activo único (es frecuente hablar de subsistemas). Estos ciclos se repiten recurrentemente hasta que

- el conjunto de activos sea lo bastante detallado como para no olvidarnos de nada
- el número de activos no sea tan grande que nos perdamos
- la denominación de los activos no sea ambigua y recoja la terminología habitual en la Organización

en pocas palabras, el modelo debe ser manejable y **fácil de explicar** a los que van a tomar decisiones a partir de nuestras conclusiones.

8.3. Para descubrir y modelar las dependencias entre activos

Siempre hay que empezar poniendo en lo más alto la información y los servicios. Depende de cada circunstancia el que sea antes la información o los servicios; pero lo más frecuente es que el valor esté en la información y deba ser respetado por los servicios que la manejan.

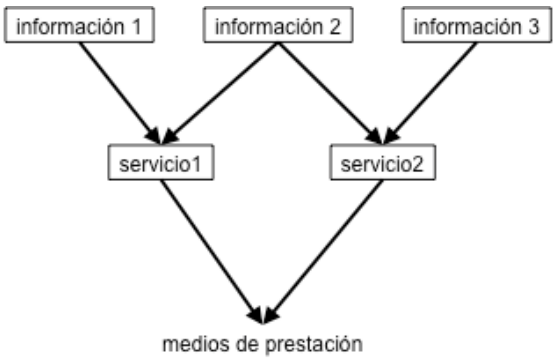

Ilustración 18. Dependencias al nivel superior

A veces es más difícil de lo esperado porque los responsables de los activos suelen estar más preocupados por el encadenamiento funcional entre activos que por la dependencia en el sentido de propagación de valor (requisitos de seguridad).

Es necesario transmitir al interlocutor que no se busca qué es necesario para que el sistema funciones, sino al revés, se busca dónde puede fallar el sistema o, más precisamente, dónde puede verse comprometida la seguridad de los activos.

- Si unos datos son importantes por su confidencialidad, se necesita saber en qué sitios van a residir dichos datos y por qué lugares van a circular: en esos puntos pueden ser revelados.
- Si unos datos son importantes por su integridad, se necesita saber en qué sitios van a residir dichos datos y por qué lugares van a circular: en esos puntos pueden ser alterados.
- Si un servicio es importante por su disponibilidad, se necesita saber qué elementos se usan para prestar dicho servicio: el fallo de esos elementos detendría el servicio.

Estas consideraciones pueden plantearse con argumentos del tipo:

- si usted quisiera acceder a estos datos, ¿dónde atacaría para robarlos?
- si usted quisiera detener este servicio, ¿dónde atacaría para estropearlo?

Este planteamiento de "póngase en el lugar del atacante" es el que da pie a las técnicas denominadas "árboles de ataque"[29] que van parejas a lo que en esta metodología se denominan dependencias. En efecto, un activo puede ser atacado directamente o indirectamente a través de otro activo del que dependa.

Las anteriores consideraciones pueden desembocar en un diagrama "plano" de dependencias que se puede (y conviene a efectos prácticos) convertir en un árbol más compacto. Así, es normal decir que los servicios dependen del equipamiento, que depende a su vez de los locales donde se ubican los equipos, sin necesidad de explicitar que los servicios dependen de los locales[30]. Es frecuente identificar "servicios internos" o "servicios horizontales" que son agrupaciones de activos para una cierta función. Estos servicios intermedios son eficaces para compactar el grafo de dependencias, pues las dependencias de dichos servicios se interpretan sin ambigüedad como dependencia de todos los elementos que prestan el servicio.

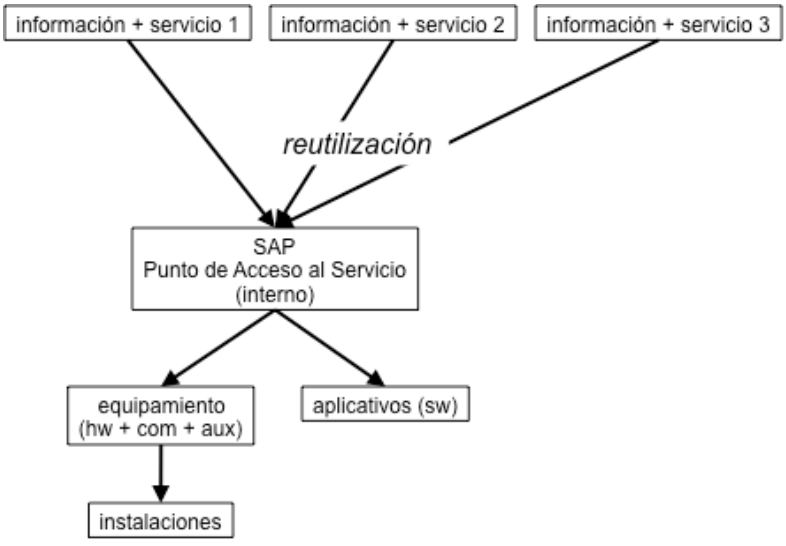

Ilustración 19. Servicios internos

Cuando se usen diagramas de flujo de datos o diagramas de procesos, no debe preocupar tanto la ruta que siguen los datos como el conjunto (desordenado) de elementos que intervienen. Un proceso depende de todos los activos que aparecen en su diagrama. Unos datos dependen de todos los sitios por donde pasen. Tanto en unos como en otros diagramas es frecuente encontrar descripciones jerarquizadas donde un proceso se subdivide en niveles de mayor detalle. Estas jerarquías de diagramas pueden ayudar a elaborar el grafo de dependencias.

Hay organizaciones donde está muy clara la información que hay que tratar y a partir de ella podemos identificar los servicios que la tratan y el equipamiento desplegado.

29 Ver "Guía de Técnicas".

30 En la "Guía de Técnicas" encontrará el modelo algorítmico para calcular las dependencias totales entre activos a partir de las dependencias directas.

Hay organizaciones más centradas en los servicios que prestan, pudiendo partir de una enumeración de servicios para asociarles la información que manejan y el equipamiento desplegado.

Hay veces que el análisis empieza por el inventariado de equipamiento y luego se va buscando qué servicios se prestan y qué información se trata en el sistema.

Errores típicos

No es correcto decir que una aplicación depende de la información que maneja. El razonamiento de quien tal afirma es que “la aplicación no funcionaría sin datos”, lo que es correcto; pero no es lo que interesa reflejar.

Más bien es todo lo contrario: la [seguridad de la] información depende de la aplicación que la maneja. En términos de servicio, se puede decir que la aplicación no vale para nada sin datos. Pero como el valor es una propiedad de la información, y la información es alcanzable por medio de la aplicación, son los requisitos de seguridad de la información los que hereda la aplicación. Luego la información depende de la aplicación. En otras palabras: a través de la aplicación puede accederse a la información, convirtiéndose la aplicación en la vía de ataque.

Dado que datos y aplicaciones suelen aunar esfuerzos para la prestación de un servicio, el valor del servicio se transmite tanto a los datos como a las aplicaciones intervinientes.

mal	***bien***
aplicación → información	información → aplicación

Tabla 9. Dependencias de la información y las aplicaciones

En este contexto, a veces conviene distinguir entre los datos y la información. La información es un bien esencial, siendo los datos una concreción TIC de la información. La información es valiosa, lo demás es valioso en la medida en que contiene información.

La información que maneja un sistema o bien se pone por encima de los servicios, o bien se agrupa

1. información → servicios → equipamiento (incluyendo datos, aplicaciones, equipos, …)
2. { información + servicios } → equipamiento (incluyendo datos, aplicaciones, equipos, …)

No es correcto decir que una aplicación dependa del equipo donde se ejecuta. El razonamiento de quien tal afirma es que “la aplicación no funcionaría sin equipo”, lo que es correcto; pero no es lo que interesa reflejar. Si tanto la aplicación como el equipo son necesarios para prestar un servicio, se debe decir explícitamente, sin buscar caminos retorcidos.

mal	***bien***
• servicio → aplicación • aplicación → equipo	• servicio → aplicación • servicio → equipo

Tabla 10. Dependencias de los servicios

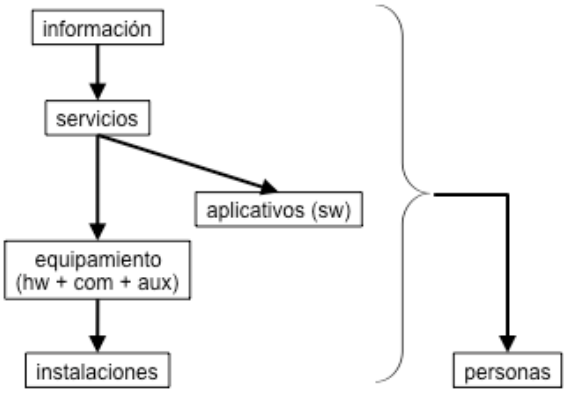

Ilustración 20. Jerarquía de dependencias

Los errores comentados a veces pasan desapercibidos mientras el sistema es muy reducido (sólo hay un servicio, una aplicación y un equipo); pero aparecen en cuanto el sistema crece. Por ejemplo, una aplicación X puede ejecutarse en diferentes equipos con diferentes datos para prestar diferentes servicios. Resulta entonces imposible relacionar la aplicación con uno o más equipos, salvo considerando cada caso

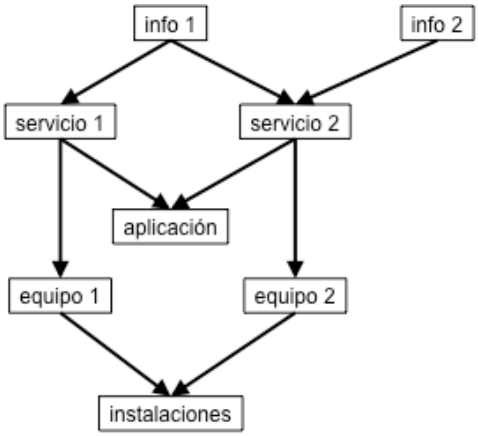

Ilustración 21. Dependencias entre activos para la prestación de unos servicios

¿Están bien modeladas las dependencias?

Establecer dependencias es una tarea delicada que puede acabar mal. Antes de dar por bueno un modelo de dependencias hay que trazar para cada activo todos los activos de los que depende directa o indirectamente. Y se debe responder positivamente a las preguntas de si

- ¿Están todos los que son? Es decir, si se han identificado todos los activos en los que puede ser atacado indirectamente el activo valorado.
- ¿Son todos los que están? Es decir, si realmente el activo valorado puede ser atacado en todos esos activos de los que depende

Como la relación de dependencia propaga el valor acumulado, encontrar un activo sin valor acumulado es síntoma de que las dependencias están mal modeladas o, simplemente, que el activo es irrelevante.

En otras palabras: para saber si las dependencias están bien establecidas, estudie el valor acumulado.

8.4. Para valorar activos

Siempre conviene valorar la información que constituye la razón de ser del sistema de información.

Si se han modelado servicios esenciales (prestados a usuarios externos al dominio de análisis), conviene valorarlos igualmente.

Es fácil identificar activos de tipo información y valorarlos siguiendo clasificaciones pautadas como su carácter personal o su clasificación de seguridad. Pero pasa a ser mucho más delicado valorar datos de tipo comercial u operacional porque hay que ir a las consecuencias del daño sufrido. Por ello en las metodologías de gestión de riesgos se requiere que la Organización establezca unos criterios para valorar, criterios que trascienden a los analistas y que deben proceder de los órganos superiores que son los encargados de valorar el sistema y de recibir los resultados del análisis.

El resto de los activos puede frecuentemente pasar sin valorar, pues su valor más importante es soportar la información y/o los servicios y de ese cálculo se encargan las relaciones de dependencias.

No obstante, si considera oportuno valorar otro tipo de activos ...

Los activos más sencillos de valorar son aquellos que se adquieren en un comercio. Si se avería, hay que poner otro. Esto cuesta dinero y tiempo (o sea, más dinero). Se habla de un coste de reposición. Salvo notorias excepciones, frecuentemente ocurre que el coste de los activos físicos es despreciable frente a otros costes, pudiendo obviarse.

Es difícil valorar las personas, en general; pero si un puesto supone una formación lenta y trabajosa, hay que tener en cuenta que la persona que desempeña ese puesto se convierte en muy valiosa, pues su “coste de reposición” es notable.

En cualquier caso, para valorar un activo se debe identificar al responsable, que será la persona adecuada para valorar el activo. A este responsable hay que ayudarle con tablas de valoración como las del capítulo 4 del "Catálogo de Elementos" que, adaptadas al caso concreto, permitan traducir la percepción de valor en una medida cualitativa o cuantitativa del mismo.

A menudo no existe el responsable único y singular de un activo y/o servicio, sino que varias personas dentro de la Organización tienen opinión cualificada al respecto. Hay que oírlas todas. Y llegar a un consenso. Si el consenso no es obvio, puede requerir

un careo: junte a los que opinan e intente que lleguen a una opinión común

un Delphi[31]**:** mande cuestionarios a los que opinan e intente que converjan a una opinión común

En los procesos de valoración de activos es frecuente recurrir a personas diferentes para valorar activos diferentes. Y es frecuente que cada entrevistado considere sus activos como de la máxima importancia; tanto más frecuente cuanto más especializado esté el entrevistado. Como muchas valoraciones son estimaciones de valor, hay que cuidar que todo el mundo use la misma escala de estimar. Por ello es importante usar una tabla como la del capítulo 4 del "Catálogo de Elementos", directamente o adaptada al caso concreto. Y es importante que tras haber preguntado a los que entienden de cada activo, todos reciban una copia de la valoración global del sistema para que aprecien el valor relativo de “sus activos” y opinen en contexto.

Datos de carácter personal

Los datos de carácter personal están tipificados por leyes y reglamentos, requiriendo de la Organización que adopte una serie de medidas de protección independientes del valor del activo[32].

La forma más realista de enfrentarse a los activos de carácter personal es caracterizarlos como tales en el nivel que corresponda y, además, determinar su valor: el daño que supondría su revelación o alteración indebida. Con esta aproximación, el análisis de impactos y riesgos permitirá proteger los datos tanto por obligación legal como por su propio valor.

31 Ver "Guía de Técnicas".

32 Es posible aproximarse a la valoración de los activos que son de carácter personal cuantificando la multa que impondría la Agencia de Protección de Datos. Esta aproximación no vale en un análisis cualitativo. En un análisis cuantitativo, esta aproximación parte de la hipótesis de que lo peor que puede pasar con ese dato es ser motivo de multa.

8.5. Para identificar amenazas

La tarea aparece como imposible: para cada activo, en cada dimensión, identificar amenazas.

Se puede partir de la experiencia pasada, propia o de organizaciones similares. Lo que ha ocurrido puede repetirse y, en cualquier caso, sería impresentable no tenerlo en cuenta.

Complementariamente, un catálogo de amenazas como el incluido en el "Catálogo de Elementos" ayuda a localizar lo que conviene considerar en función del tipo de activo y de las dimensiones en las que tiene un valor propio o acumulado.

A menudo se recurre a idear escenarios de ataque que no son sino dramatizaciones de cómo un atacante se enfrentaría a nuestros sistemas. Esta técnica es la que a veces se denomina “árboles de ataque”. Póngase en la piel del atacante e imagine qué haría con sus conocimientos y su capacidad económica. Puede que tenga que plantearse diferentes situaciones dependiendo del perfil técnico del atacante o de sus recursos técnicos y humanos. Estas dramatizaciones son interesantes para poder calcular impactos y riesgos; pero además serán muy útiles a la hora de convencer a la alta dirección y a los usuarios de por qué una amenaza no es teórica sino muy real. Es más, cuando evalúe las salvaguardas puede ser conveniente revisar estos escenarios de ataque.

Es habitual que las herramientas de soporte al análisis de riesgos aporten perfiles típicos para apoyar en esta tarea.

8.6. Para valorar amenazas

La tarea es desmoralizadora: para cada activo en cada dimensión, determinar la degradación que causarían y la probabilidad de ocurrencia.

Siempre que sea posible conviene partir de datos estándar. En el caso de desastres naturales o accidentes industriales, se puede disponer de series históricas, genéricas o del lugar en el que se ubican los equipos de nuestro sistema de información bajo estudio. Probablemente también se disponga de un historial que informe de lo que es frecuente y de lo que “no pasa nunca”.

Más complicado es calificar los errores humanos; pero la experiencia permite ir aquilatando valores realistas.

Y lo más complejo es calificar los ataques deliberados pues dependen de la suerte, buena o mala. Hay muchos motivos que agudizan el peligro de una amenaza:

- que no requiera grandes conocimientos técnicos por parte del atacante[33]
- que no requiera gran inversión en equipo por parte del atacante[34]
- que haya un enorme beneficio económico en juego (que el atacante puede enriquecerse)
- que haya un enorme beneficio en juego (que el atacante pueda salir fuertemente beneficiado, en su estima, en su conocimiento por todo el mundo, ...); por lo que más quiera, evite los retos y jamás alardee de que su sistema de información es invulnerable: no lo es y no tiene gracia que se lo demuestren
- que haya un mal ambiente de trabajo, semilla de empleados descontentos que se vengan a través de los sistemas, simplemente para causar daño
- que haya una mala relación con los usuarios externos, que se vengan a través de nuestros sistemas

33 Hay que estar atentos a la “comercialización” de las herramientas de ataque pues un ataque puede requerir un gran experto para realizarlo manualmente (es decir, es poco frecuente); pero si el experto empaqueta su ataque en una herramienta con una simple interfaz gráfica, usar la herramienta se convierte en un deporte que no requiere del atacante sino ausencia de escrúpulos (es decir, la amenaza ha pasado a ser muy frecuente).

34 Hay que tener muy en cuenta que Internet es una red inmensa de poder de cómputo. Si alguien sabe cómo organizarse, no es difícil poner a la red a “trabajar para mí” lo que supone que el atacante disponga de muchísimos más medios efectivos que el atacado.

Partiendo de un valor estándar, hay que ir aumentando o disminuyendo sus calificaciones de frecuencia y degradación hasta reflejar lo más posible el caso concreto. A menudo no es evidente determinar el valor correcto y es necesario recurrir a simulaciones que orienten. El uso de algún tipo de herramienta es muy útil para estudiar las consecuencias de un cierto valor, lo que algunos autores denominan la sensibilidad del modelo a cierto dato. Si se aprecia que los resultados cambian radicalmente ante pequeñas alteraciones de una estimación de frecuencia o degradación, hay que (1) ser realistas y (2) prestar extrema atención a por qué el sistema es tan sensible a algo tan concreto y tomar medidas orientadas a independizar el sistema; es decir, a no hacer crítica una cierta amenaza.

Recuerde que la frecuencia no afecta al impacto, por lo que estudiando el impacto se puede ajustar la degradación y, posteriormente, estudiando el riesgo se puede ajustar la frecuencia. Nunca se debe aceptar un valor injustificado de degradación en la esperanza de compensarlo con la frecuencia, pues la estimación del impacto es importante en sí misma, además de la de riesgo.

Sea cual sea la decisión final que se tome para estimar un valor, hay que documentarla pues antes o después se pedirán explicaciones, sobre todo si como consecuencia se van a recomendar salvaguardas costosas.

Es habitual que las herramientas de soporte al análisis de riesgos aporten perfiles típicos para apoyar en esta tarea.

8.7. Para seleccionar salvaguardas

Probablemente la única forma es tirar de catálogo. Use un (sistema) experto que le ayude a ver qué solución es adecuada para cada combinación de

- tipo de activo
- amenaza a la que está expuesto
- dimensión de valor que es motivo de preocupación
- nivel de riesgo

A menudo encontrará muchas soluciones para un problema, con diferentes calidades. En estos casos debe elegir una solución proporcionada a los niveles de impacto y riesgo calculados.

Muchas salvaguardas son de bajo coste, bastando configurar adecuadamente los sistemas u organizar normativa para que el personal haga las cosas de forma adecuada. Pero algunas contra medidas son realmente costosas (en su adquisición, en su despliegue, en su mantenimiento periódico, en la formación del personal a su cargo, ...). En estos casos conviene ponderar si el coste de la salvaguarda no supera el riesgo potencial; es decir, tomar siempre decisiones de gasto que supongan un ahorro neto.

Por último, y no menos importante, a la hora de desplegar salvaguardas hay que considerar su facilidad de uso. Lo ideal es que la salvaguarda sea transparente de forma que el usuario no tenga que hacer nada o, en su defecto, cuanto menos haya que hacer, mejor. Simplemente porque una salvaguarda de complejo manejo requiere personal especializado y añade a las amenazas que ya tenía el sistema la amenaza que supone su defectuosa utilización.

8.8. Aproximaciones sucesivas

El lector ya se habrá percibido de que el análisis de riesgos puede ser muy laborioso, requiriendo tiempo y esfuerzo. Además, hay que introducir muchos elementos que no son objetivos, sino estimaciones del analista, lo que implica que haya que explicar y consensuar lo que significa cada cosa para no estar expuestos a impactos o riesgos que se ignoran o se infravaloran, ni convertir la paranoia en un dispendio de recursos injustificados.

Si hay que ser prácticos y efectivos, conviene realizar aproximaciones sucesivas. Se empieza por un análisis somero, de alto nivel, identificando rápidamente lo más crítico: activos de gran valor, vulnerabilidades manifiestas o, simplemente, recomendaciones de libro de texto porque no hay nada más prudente que aprender en cabeza ajena, aprovechando la experiencia de los demás. Este análisis de riesgos es imperfecto, evidentemente; pero cabe confiar en que lleve en la direc-

ción correcta. Los párrafos siguientes dan indicaciones de cómo orientarse rápidamente hacia el objetivo final: tener impactos y riesgos bajo control.

Nótese que estas aproximaciones imperfectas permiten desplegar rápidamente sistemas razonablemente protegidos cuando no hay tiempo para un análisis de riesgos en toda su plenitud. Cuando, con tiempo, se llegue a la fase de gestión de riesgos tras un análisis exhaustivo, muy probablemente ocurra que muchas salvaguardas están ya dispuestas, necesitándose sólo la introducción de algunas nuevas y/o la mejora de la eficacia de las existentes. No es pues trabajo perdido seguir estas aproximaciones informales.

8.8.1. Protección básica

Es frecuente oír hablar de medidas básicas de protección *(baseline)* que deberían implantarse en todos los sistemas, salvo que se demuestre que no son pertinentes a algún caso particular.

Por favor, no discuta; ni lo dude: a sus sistemas de información no debe poder acceder cualquiera en cualquier momento. Puede protegerlos física o lógicamente, poniéndolos en una sala donde no entra cualquiera, o imponiendo una identificación de acceso lógico. Pero ¡protéjalos!

Este tipo de razonamientos se pueden aplicar con frecuencia y llevan a desplegar un mínimo de salvaguardas “de puro sentido común”. Una vez avanzado lo que es obvio y no se debería nunca discutir, se puede avanzar a niveles más elaborados, específicos de cada sistema.

Para aplicar un tratamiento básico se requiere un catálogo de salvaguardas. Existen numerosas fuentes, entre las que cabe destacar:

- normas internacionales, por ejemplo [ISO 27002]
- normas sectoriales
- normas corporativas, especialmente frecuentes en pequeñas delegaciones de grandes organizaciones

Las ventajas de protegerse por catálogo son:

- es muy rápido
- cuesta menos esfuerzo que ponerse a analizar y decidir
- se logra un nivel homogéneo con otras organizaciones parecidas

Los inconvenientes de protegerse por catálogo son:

- el sistema puede protegerse frente a amenazas que no padece, lo que supone un gasto injustificado
- el sistema puede estar inadecuadamente protegido frente a amenazas reales

En general, con la protección básica no se sabe lo que se hace y, aún estando probablemente en la senda correcta, no hay medida de si falta o si sobra. No obstante, puede ser un punto de partida útil para refinar posteriormente.

La protección por catálogo puede refinarse un poco considerando el valor y la naturaleza de los activos o cuantificando las amenazas.

En base a la tipificación de los activos

Si usted tiene datos de carácter personal calificados de nivel alto, tiene que cifrarlos.

Si usted tiene datos clasificados como confidenciales, tiene que etiquetarlos y cifrarlos.

Aparte de cumplir con la legislación y normativa específica, habrá llevado a cabo una especie de “vacunación preventiva” de activos que seguro que son importantes.

Si usted tiene una red local conectada al exterior, tiene que poner un cortafuegos en el punto de conexión.

etc.

En base al valor de los activos

Si usted tiene todos los datos operacionales en soporte informático, tiene que hacer copias de seguridad.

Si usted tiene equipos informáticos, manténgalos al día con las actualizaciones del fabricante.

Lo que vale hay que cuidarlo, por si le pasara algo, sin entrar en muchas precisiones de qué les puede pasar exactamente.

En base a las amenazas

Si se trata de un sistema de la llamada administración electrónica (tramitación administrativa no presencial) o si los sistemas se usan para comerciar electrónicamente (compras y ventas no presenciales), registre cuidadosamente quién hace qué en cada momento pues se enfrentará a incidencias con los usuarios, teniendo que determinar quién tiene razón y quien paga los perjuicios. También habrá quien quiera usar sus servicios sin tener derecho a ello (fraude).

Lo que se puede necesitar, es necesario, y parte de las responsabilidades del responsable de seguridad es disponer de la información correcta cuando haga falta.

En base a la exposición

Si usted tiene una red de equipos antiguos y se conecta a Internet, debe instalar un cortafuegos.

Si tiene usted una aplicación en producción, debe mantenerla al día aplicando mejoras y corrigiendo los defectos anunciados por el fabricante.

Cuando se sabe que los sistemas de información son vulnerables, hay que protegerlos.

Apéndice 1. Glosario

Diferentes autores u organizaciones definen los mismos términos de diferentes formas y maneras. Las siguientes tablas recopilan definiciones acordes al sentido en el cual se emplean los términos en esta guía metodológica, tanto en español como en inglés. De las múltiples definiciones se ha seleccionado la preferida en Magerit v2, resaltándola en negrita. Cuando la definición procede de alguna fuente, se cita esta. La ausencia de fuente indica que es definición propia de esta guía. Salvo razones en contra, siempre se ha preferido mantener la definición propuesta en Magerit v1 (1997).

A1.1. Términos en español

Aceptación del riesgo	Decisión informada a favor de tomar un riesgo. [UNE-ISO Guía 73:2010]
Acreditación	Acción de facultar a un sistema o red de información para que procese datos sensibles, determinando el grado en el que el diseño y la materialización de dicho sistema cumple los requerimientos de seguridad técnica preestablecidos. [CESID:1997] Accreditation: Formal declaration by the responsible management approving the operation of an automated system in a particular security mode using a particular set of safeguards. Accreditation is the official authorization by management for the operation of the system, and acceptance by that management of the associated residual risks. Accreditation is based on the certification process as well as other management considerations. [15443-1:2005]
Activo	Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008] Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección. [Magerit: 2006] Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección. [Magerit:1997] Bienes: En la teoría de los valores, la realidad que posee un valor positivo y por ello es estimable. [DRAE] Asset: A component or part of the total system. Assets may be of four types: physical, application software, data, or end user services. [CRAMM:2003] Asset: Something of value to the enterprise. [Octave:2003] Asset: Any information resource with value that is worth protecting or preserving. [TDIR:2003] Assets: Information or resources to be protected by the countermeasures of a Target of Evaluation. [CC:1999]
Amenaza	Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008] Potential cause of an unwanted incident, which may result in harm to a system or organization. [ISO/IEC 27000:2009]

Aceptación del riesgo	Decisión informada a favor de tomar un riesgo. [UNE-ISO Guía 73:2010]
	Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos. [Magerit:2006] Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos. [Magerit:1997] Condición del entorno del sistema de información que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad. [CESID:1997] Threat: Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [800-53:2009] Threat: Any circumstance or event with the potential to adversely impact an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. [CNSS:2003] Threat: An activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity. [TDIR:2003] Threat: Any circumstance or event that could harm a critical asset through unauthorized access, compromise of data integrity, denial or disruption of service, or physical destruction or impairment. [CIAO:2000] A threat is an indication of a potential undesirable event. [NSTISSI:1998] Threat: A potential violation of security. [7498-2:1989]
Análisis de impacto	Estudio de las consecuencias que tendría una parada de X tiempo sobre la Organización.
Análisis de riesgos	Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. Análisis del riesgo – Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo. [UNE-ISO Guía 73:2010] Identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como 'activos'); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre. [Magerit:1997] Risk assessment: Process of evaluating the risks of information loss based on an analysis of threats to, and vulnerabilities of, a system, operation or activity. [OPSEC] Risk Analysis: Examination of information to identify the risk to an information system. [CNSS:2003] Risk Assessment:: Process of analyzing threats to and vulnerabilities of an information system, and the potential impact resulting from the loss of information or capabilities of a system. This analysis is used as a basis for identifying appropriate and cost-effective security countermeasures. [CNSS:2003] Risk Analysis: An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence. [TDIR:2003]

Aceptación del riesgo	Decisión informada a favor de tomar un riesgo. [UNE-ISO Guía 73:2010]
	Risk Assessment: A study of vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures. The process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations. [TDIR:2003]
Ataque	Intento de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja, o violar alguna política de seguridad de alguna otra manera. [ISO/IEC 18043:2006] Cualquier acción deliberada encaminada a violar los mecanismos de seguridad de un sistema de información. [CESID:1997]
Auditoría de seguridad	Estudio y examen independiente del historial y actividades de un sistema de información, con la finalidad de comprobar la idoneidad de los controles del sistema, asegurar su conformidad con la estructura de seguridad y procedimientos operativos establecidos, a fin de detectar brechas en la seguridad y recomendar cambios en los procedimientos, controles y estructuras de seguridad.
Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008] Aseguramiento de la identidad u origen. [Magerit:2006] Autenticación: Característica de dar y reconocer la autenticidad de los activos del dominio (de tipo información) y/o la identidad de los actores y/o la autorización por parte de los autorizadores, así como la verificación de dichas tres cuestiones. [Magerit:1997] Authenticity: Having an undisputed identity or origin. [OPSEC] Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. [800-53:2009]
Certificación	Confirmación del resultado de una evaluación, y que los criterios de evaluación utilizados fueron correctamente aplicados.
Confidencialidad	Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. [UNE 71504:2008] Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso. [Magerit:2006] Característica que previene contra la divulgación no autorizada de activos del dominio. [Magerit:1997] Confidentiality: An assurance that information is not disclosed to unauthorized entities or processes (DOD JP 1994; JCS 1997) [OPSEC] Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [800-53:2009] Confidentiality: The requirement of keeping proprietary, sensitive, or personal information private and inaccessible to anyone that is not authorized to see it. [Octave:2003] Confidentiality: Assurance that information is not disclosed to unauthorized persons, processes, or devices. [CNSS:2003] [TDIR:2003]

Aceptación del riesgo	Decisión informada a favor de tomar un riesgo. [UNE-ISO Guía 73:2010]
	Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [ISO 7498-2:1989]
Contra medida	Véase salvaguarda.
Control	Véase salvaguarda.
Declaración de aplicabilidad	Documento formal en el que, para un conjunto de salvaguardas, se indica sin son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.
Degradación	Pérdida de valor de un activo como consecuencia de la materialización de una amenaza.
Dimensión de seguridad	Un aspecto, diferenciado de otros posibles aspectos, respecto del que se puede medir el valor de un activo en el sentido del perjuicio que causaría su pérdida de valor.
Disponibilidad	Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados. [UNE 71504:2008] Característica que previene contra la denegación no autorizada de acceso a activos del dominio. [Magerit:1997] Availability: The assurance that data transmissions, computer processing systems, and/or communications are not denied to those who are authorized to use them (JCS 1997) [OPSEC] Availability: Ensuring timely and reliable access to and use of information. [800-53:2009] Availability: The extend to which, or frequency with which, an asset must be present or ready for use. [Octave:2003] Availability: Timely, reliable access to data and information services for authorized users. [CNSS:2003] [TDIR:2003] [CIAO:2000] Availability: The property of being accessible and usable upon demand by an authorized entity. [ISO 7498-2:1989]
Estado de riesgo	Informe: Caracterización de los activos por su riesgo residual; es decir lo que puede pasar tomando en consideración las salvaguardas desplegadas.
Evaluación de salvaguardas	Informe: Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.
Frecuencia	Tasa de ocurrencia de una amenaza. Número de sucesos o de efectos en una unidad de tiempo definida. [UNE-ISO Guía 73:2010]
Gestión de riesgos	Actividades coordinadas para dirigir y controlar una organización el lo relativo al riesgo. [UNE-ISO Guía 73:2010] Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados. [Magerit:2006] Selección e implantación de las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. La gestión de riesgos se basa en los resultados obtenidos en el análisis de los riesgos. [Magerit:1997]

Aceptación del riesgo	Decisión informada a favor de tomar un riesgo. [UNE-ISO Guía 73:2010]
	Risk management: A security philosophy which considers actual threats, inherent vulnerabilities, and the availability and costs of countermeasures as the underlying basis for making security decisions (JSCR 1994). [OPSEC] Risk management: Process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment. [CNSS:2003] The identification, assessment, and mitigation of probabilistic security events (risks) in information systems to a level commensurate with the value of the assets protected. [CIAO:2000]
Impacto	Consecuencia que sobre un activo tiene la materialización de una amenaza. Consecuencia – Resultado de un suceso que afecta a los objetivos. [UNE-ISO Guía 73:2010] Consecuencia que sobre un activo tiene la materialización de una amenaza. [Magerit:1997] Impact: The effect of a threat on an organization's mission and business objectives. [Octave:2003] Impact: The effect on the organisation of a breach in security. [CRAMM:2003]
Impacto residual	Impacto remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información.
Incidente de seguridad	Suceso (inesperado o no deseado) con consecuencias en detrimento de la seguridad del sistema de información. [UNE 71504:2008] Evento con consecuencias en detrimento de la seguridad del sistema de información. [Magerit:2006] Information security event: identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant. [ISO/IEC 27000:2009] Information security incident: single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. [ISO/IEC 27000:2009] Incident: A successful or unsuccessful action attempting to circumvent technical controls, organizational policy, or law. This is often called an attack. [TDIR:2003]
Informe de insuficiencias	Informe: Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir el riesgo sobre el sistema.
Integridad	Propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada. [UNE 71504:2008] Característica que previene contra la modificación o destrucción no autorizadas de activos del dominio. [Magerit:1997] Information integrity: The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed (NSC EO 1995; JCS 1997). [OPSEC]

Aceptación del riesgo	Decisión informada a favor de tomar un riesgo. [UNE-ISO Guía 73:2010]
	Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [800-53:2009] Integrity: the authenticity, accuracy, and completeness of an asset. [Octave:2003] Data integrity: A condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. [CNSS:2003] [TDIR:2003] [CIAO:2000] Data integrity: The data quality that exists as long as accidental or malicious destruction, alteration, or loss of data does not occur. [CRAMM:2003] Integrity: Condition existing when an information system operates without unauthorized modification, alteration, impairment, or destruction of any of its components. [CIAO:2000]
Mapa de riesgos	Informe: Relación de las amenazas a que están expuestos los activos. Threat Analysis: The examination of all actions and events that might adversely affect a system or operation. [TDIR:2003] Threat Assessment: An evaluation of the nature, likelihood, and consequence of acts or events that could place sensitive information and assets as risk. [TDIR:2003]
Medida de seguridad	Véase salvaguarda.
Modelo de valor	Informe: Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.
Plan de seguridad	Conjunto de proyectos de seguridad que permiten materializar las decisiones de gestión de riesgos.
Probabilidad	Probabilidad *(likelihood)* – Posibilidad de que un hecho se produzca. [UNE-ISO Guía 73:2010] NOTA 1 – En la terminología de la gestión del riesgo, la palabra “probabilidad” se utiliza para indicar la posibilidad de que algún hecho se produzca, que esta posibilidad está definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o de forma matemática [tales como una probabilidad o una frecuencia sobre un periodo de tiempo dado].
Proyecto de seguridad	Agrupación de tareas orientadas a tratar el riesgo del sistema. La agrupación se realiza por conveniencia, bien porque se trata de tareas que en singular carecerían de eficacia, bien porque se trata de tareas con un objetivo común, bien porque se trata de tareas que competen a una única unidad de acción.
Riesgo	Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. Efecto de la incertidumbre sobre la consecución de los objetivos. [UNE-ISO Guía 73:2010] Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la Organización. [Magerit:1997]

Aceptación del riesgo	Decisión informada a favor de tomar un riesgo. [UNE-ISO Guía 73:2010]
	Probabilidad de que una vulnerabilidad propia de un sistema de información sea explotada por las amenazas a dicho sistema, con el objetivo de penetrarlo. [CESID:1997] Risk: A measure of the potential degree to which protected information is subject to loss through adversary exploitation. [OPSEC] Risk: Possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability. [CNSS:2003] Risk: A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting adverse impact. Reducing either the threat or the vulnerability reduces the risk. [TDIR:2003] Total risk: The potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability). [TDIR:2003] Risk: A measure of the exposure to which a system or potential system may be subjected. [CRAMM:2003]
Riesgo acumulado	Dícese del calculado tomando en consideración el valor propio de un activo y el valor de los activos que depende de él. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma.
Riesgo potencial	Riesgos potenciales. Los riesgos del sistema de información en la hipótesis de que no hubieran salvaguardas presentes. [UNE 71504:2008] Inherent risk – The risk level or exposure without taking into account the actions that management has taken or might take (e.g. implementing controls) [RiskIT-PG:2009]
Riesgo repercutido	Dícese del calculado tomando en consideración únicamente el valor propio de un activo. Este valor se combina con la degradación causada por una amenaza y la frecuencia estimada de la misma, medidas ambas sobre activos de los que depende.
Riesgo residual	Riesgo remanente en el sistema después del tratamiento del riesgo. [UNE-ISO Guía 73:2010] Riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información. [Magerit:2006] Riesgo que se da tras la aplicación de salvaguardas dispuestas en un escenario de simulación o en el mundo real. [Magerit:1997] Residual risk: Portion of risk remaining after security measures have been applied. [CNSS:2003] [CRAMM:2003] Residual Risk: The potential for the occurrence of an adverse event after adjusting for the impact of all in-place safeguards. [TDIR:2003]
Salvaguarda	Procedimiento o mecanismo tecnológico que reduce el riesgo. Control: Medida que modifica un riesgo. [UNE-ISO Guía 73:2010] Control: Means of managing risks, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management or legal nature. [ISO/IEC 27000:2009] Countermeasure: Anything which effectively negates or mitigates an adversary's ability to exploit vulnerabilities. [OPSEC]

Aceptación del riesgo	Decisión informada a favor de tomar un riesgo. [UNE-ISO Guía 73:2010]
	Safeguard: Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. [800-53:2009] Countermeasure: Action, device, procedure, technique, or other measure that reduces the vulnerability of an information system. [CNSS:2003] Security safeguard: Protective measures and controls prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. [CNSS:2003] Countermeasure: Any action, device, procedure, technique, or other measure that mitigates risk by reducing the vulnerability of, threat to, or impact on a system. [TDIR:2003]
Seguridad	La capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles. [Reglamento (CE) n 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información]. Information System Security: Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. [CNSS:2003]
Seguridad de la información	Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables. [UNE 71504:2008]
Sistema de información	Los ordenadores y redes de comunicaciones electrónicas, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento. Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar (tratar), mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. [UNE 71504:2008] Conjunto de elementos físicos, lógicos, elementos de comunicación, datos y personal que permiten el almacenamiento, transmisión y proceso de la información. [Magerit:1997] Cualquier sistema o producto destinado a almacenar, procesar o transmitir información. [CESID:1997] Information System: Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. [CNSS:2003] Information System: Any procedure or process, with or without IT support, that provides a way of acquiring, storing, processing or disseminating information. Information systems include applications and their supporting infrastructure. [CRAMM:2003]
Tratamiento de riesgos	Proceso destinado a modificar el riesgo. [UNE-ISO Guía 73:2010] El proceso de selección e implantación de las medidas o salvaguardas pa-

Aceptación del riesgo	Decisión informada a favor de tomar un riesgo. [UNE-ISO Guía 73:2010]
	ra prevenir, impedir, reducir o controlar los riesgos identificados. [UNE 71504:2008]
Trazabilidad	Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. [UNE 71504:2008] Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [ISO/IEC 7498-2:1989] Responsabilidad: Cualidad que permite que todas las acciones realizadas sobre un sistema de tecnología de la información sean asociadas de modo inequívoco a un individuo o entidad. [CESID:1997] Accountability: Process of tracing information system activities to a responsible source. [CNSS:2003]
Valor	De un activo. Es una estimación del coste inducido por la materialización de una amenaza. Cualidad que poseen algunas realidades, consideradas bienes, por lo cual son estimables. [DRAE]
Valor acumulado	Considera tanto el valor propio de un activo como el valor de los activos que dependen de él. Bienes de abolengo: Los heredados de los abuelos. [DRAE]
Vulnerabilidad	Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza. Propiedades intrínsecas de que algo se produzca como resultado de una sensibilidad a una fuente de riesgo que puede conducir a un suceso con una consecuencia. [UNE-ISO Guía 73:2010] A weakness in design, implementation, operation or internal control. [RiskIT-PG:2009] A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy. [RFC4949:2007] Estimación de la exposición efectiva de un activo a una amenaza. Se determina por dos medidas: frecuencia de ocurrencia y degradación causada. [Magerit:2006] Vulnerabilidad de un activo es la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo. [Magerit:1997] Debilidad en la seguridad de un sistema de información. [CESID:1997] Vulnerability: The susceptibility of information to exploitation by an adversary. [OPSEC] Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited. [CNSS:2003] Vulnerability: A weakness or lack of controls that would allow or facilitate a threat actuation against a specific asset or target. [CRAMM:2003]

A1.2. Términos anglosajones

Breve diccionario inglés-español de términos habituales en análisis y gestión de riesgos:

Acrónimos	
ALE	Annual Loss Expectancy
ARO	Annual Rate of Occurrence
BIA	Business Impact Analysis
GRC	Governance, Risk Management, and Compliance

Accountability	Trazabilidad
Authenticity	Autenticidad
Availability	Disponibilidad
Asset	Activo
Business Impact Analysis	Análisis de impacto
Compliance	Cumplimiento
Confidentiality	Confidencialidad
Countermeasure	Contra medida
Frequency	Frecuencia
Impact	Impacto
Information security	Seguridad de la información
Information security incident	Incidente de seguridad
Information system	Sistema de información
Integrity	Integridad
Residual risk	Riesgo residual
Risk	Riesgo
Risk acceptance	Aceptación de riesgos
Risk analysis	Análisis de riesgos
Risk assessment	Análisis de riesgos
Risk management	Gestión de riesgos
Risk map	Mapa de riesgo
Risk treatment	Tratamiento del riesgo
Safeguard	Salvaguarda
Security	Seguridad
Statement of applicability	Documento de selección de controles
Traceability	Trazabilidad
Threat	Amenaza
Value	Valor
Vulnerability	Vulnerabilidad

A1.3. ISO – Gestión del riesgo

La definiciones de ISO en lo que respecta a riesgos se recogen en la guía [ISO 73]

Definiciones

Riesgo

Efecto de la incertidumbre sobre la consecución de los objetivos.

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.

Proceso de gestión del riesgo

Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo.

Dueño del riesgo

Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo.

Tratamiento del riesgo

Proceso destinado a modificar el riesgo.

NOTA 1 – El tratamiento del riesgo puede implicar:

— evitar el riesgo, decidiendo no iniciar o continuar con la actividad que motiva el riesgo;

— aceptar o aumentar el riesgo con objeto de buscar una oportunidad;

— eliminar la fuente de riesgo;

— cambiar la probabilidad;

— cambiar las consecuencias;

— compartir el riesgo con otra u otras partes [incluyendo los contratos y la financiación del riesgo]; y

— mantener el riesgo en base a una decisión informada.

NOTA 2 – Los tratamientos del riesgo que conducen a consecuencias negativas, en ocasiones se citan como “mitigación del riesgo”, “eliminación del riesgo”, “prevención del riesgo” y “reducción del riesgo”.

NOTA 3 – El tratamiento del riesgo puede originar nuevos riesgos o modificar los riesgos existentes.

Apéndice 2. Referencias

Arreglo 2000
“Arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes en el campo de la Seguridad de las Tecnologías de la Información”, Mayo, 2000.

BSI
Federal Office for Information Security (BSI). “IT Baseline Protection Manual”, October 2003. Germany.
http://www.bsi.de/gshb/english/etc/index.htm

CC
Comon Criteria. Ver [ISO 15408].

CEM
Common Evaluation Methodology. Ver [ISO 18045].

CESID
Centro Superior de Información de la Defensa, “Glosario de Términos de Criptología”, Ministerio de Defensa, 3ª edición, 1997.

CIAO
Critical Infrastructure Assurance Office, “Practices for Securing Critical Information Assets”, January 2000.

CNSS
Committee on National Security Systems, Instruction No. 4009, “National Information Assurance (IA) Glossary“, May 2003.

CRAMM
“CCTA Risk Analysis and Management Method (CRAMM)”, Version 5.0, 2003.

DARPA 1601
“The Vulnerability Assessment and Mitigation Methodology”, P.S. Antón et al., RAND National Defense Research Institute, MR-1601-DARPA, 2003.

DRAE
Real Academia Española. Diccionario de la Lengua Española. 22.ª edición, 2001.
http://buscon.rae.es/diccionario/drae.htm

EA-7
European Co-Operation for Accreditation, “Guidelines for the Accreditation of Bodies Operating Certification / Registration of Information Security Management Systems”, EA-7/03, February 2000.

EBIOS
“Méthode pour l’Expression des Besoins et l’Identification des Objectifs de Sécurité”. Service Central de la Sécurité des Systèmes d'Information. France.

GAO
United States General Accounting Office, Accounting and Information Management Division, “Information Security Risk Assessment — GAO Practices of Leading Organizations.

ISO 73
ISO Guide 73:2009, “Risk management — Vocabulary”.
UNE-ISO Guía 73:2010, “Gestión del riesgo. Vocabulario”.

ISO 7498-2
ISO 7498-2:1989, “Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture”.

ISO 15408
ISO/IEC 15408:2009, “Information technology — Security techniques — Evaluation criteria for IT security”.

ISO 15443-1
ISO/IEC TR 15443-1:2005, “Information technology — Security techniques — A framework for IT security assurance -- Part 1: Overview and framework”.

ISO 18043
ISO/IEC 18043:2006, “Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems”.

ISO 18045
ISO/IEC 18045:2008, “Information technology — Security techniques — Methodology for IT security evaluation”.

ISO 27000
ISO/IEC 27000:2009, “Information technology — Security techniques — Information security management systems — Overview and vocabulary”.

ISO 27001
ISO/IEC 27001:2005, “Information technology — Security techniques — Information security management systems — Requirements”
UNE-ISO/IEC 27001:2007, “Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos”

ISO 27002
ISO/IEC 27002:2005, “Information technology — Security techniques — Code of practice for information security management”.
UNE-ISO/IEC 27002:2009, “Tecnología de la Información. Código de Buenas Prácticas de la Gestión de la Seguridad de la Información”.

ISO 27005
ISO/IEC 27005:2011, “Information technology — Security techniques — Information security risk management”.

ISO 31000
ISO 31000:2009, “Risk management — Principles and guidelines”.
UNE-ISO 31000:2010, “Gestión del riesgo. Principios y directrices”.

ISO 31010
ISO/IEC 31010:2009, “Risk management — Risk assessment techniques”.
UNE-ISO/IEC 31010:2010, “Gestión del riesgo. Técnicas de apreciación del riesgo”.

ISO 38500
ISO/IEC 38500:2008. “Corporate governance of information technology”.

ITSEC
European Commission, “Information Technology Security Evaluation Criteria”, version 1.2, 1991.

Magerit:1997
Ministerio de Hacienda y Administraciones Públicas, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Versión 1”, 1997.

Magerit:2006
Ministerio de Hacienda y Administraciones Públicas, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – Versión 2”, 2006.

NIST 800-27
NIST, “Engineering Principles for Information Technology Security (A Baseline for Achieving Security)”, SP 800-27 Rev. A, June 2004.

NIST 800-30
NIST, “Risk Management Guide for Information Technology Systems”, SP 800-30, 2Jul. 002.
NISR, “DRAFT Guide for Conducting Risk Assessments”, SP 800-30 Rev.1, Sept. 2011.

NIST 800-37
NIST, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach”, SP 800-37 Rev.1, Feb. 2010

NIST 800-39
NIST, “Managing Information Security Risk: Organization, Mission, and Information System View”, SP 800-39, Mar. 2011

NIST 800-53
NIST, “Recommended Security Controls for Federal Information Systems”, National Institute of Standards and Technology, special publication SP 800-53 Rev.3, Aug. 2009.

NIST 800-64
NIST, “Security Considerations in the Information System Development Life Cycle”, SP 800-64 Rev.2, Oct. 2008.

NSTISS
National Security Telecommunications and Information Systems Security Committee, “Index of National Security Telecommunications Information Systems Security Issuances”, NSTISSI no. 4014, NSTISSC Secretariat, 1998.

OCDE
Directrices de la ocde para la seguridad de sistemas y redes de información : hacia una cultura de seguridad. 2004

Octave
C. Alberts and A. Dorofee, “Managing information Security Risks. The OCTAVE Approach”, Addison Wesley, 2003.

OPSEC
OPSEC Glossary of Terms,
http://www.ioss.gov/docs/definitions.html

Peltier 2001
T.R. Peltier, “Information Security Risk Analysis”, Auerbach Pub; 1st edition (January 23, 2001)

PILAR
“Procedimiento Informático-Lógico para el Análisis de Riesgos”. Centro Criptológico Nacional. Centro Nacional de Inteligencia. Ministerio de Presidencia. España.

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

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

Ribagorda
A. Ribagorda, “Glosario de Términos de Seguridad de las T.I.”, Ediciones CODA, 1997.

RIS2K
Soporte de Magerit v1.0. Ministerio de Hacienda y Administraciones Públicas. España.

RiskIt-F
ISACA, “The Risk IT Framework”, 2009.

RiskIt-PG
ISACA, “The Risk IT Practitioner Guide”. 2009.

TCSEC
Department of Defense, “Trusted Computer System Evaluation Criteria”, DOD 5200.28-STD, Dec. 1985.

TDIR:2003
Texas Department of Information Resources, “Practices for Protecting Information Resources Assets“, Revised September 2003.

UNE 71504
UNE 71504:2008, “Metodología de análisis y gestión de riesgos para los sistemas de información”.

Apéndice 3. Marco legal

En este apéndice se apunta cierta normativa legal, nacional e internacional, relevante al caso del análisis y gestión de riesgos, bien por exigirlo, bien por sustentarlo, bien por ser de utilidad en el Proceso de Gestión de Riesgos. La relación no pretende ser exhaustiva, amén de estar sujeta a un proceso legislativo activo, por lo que es obligación del responsable prestar atención a las novedades que vayan apareciendo..

Se han incluido algunas referencias a acuerdos de carácter político o de otra naturaleza a los cuales conviene también prestar atención. Por ejemplo, las Guías de la OCDE.

A3.1. Seguridad en el ámbito de la Administración electrónica

- Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, LRJ-PAC.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. BOE de 29 de enero de 2010.
- Corrección de errores del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. BOE de 11 de marzo de 2010.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. BOE de 29 de enero 2010.

A3.2. Protección de datos de carácter personal

- LOPD, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

A3.3. Firma electrónica

- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social; art. 81.
- Real Decreto 1317/2001, de 30 de noviembre, por el que se desarrolla el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, en materia de prestación de servicios de seguridad por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos, con las Administraciones Públicas.

A3.4. Información clasificada

- Ley 9/1968, de 5 de abril, sobre Secretos Oficiales.
- Decreto 242/1969, de 20 de Febrero. por el que se desarrollan las disposiciones de la Ley 9/1968. de 5 de abril sobre Secretos Oficiales.
- Ley 48/1978, de 7 de octubre, que modifica la Ley 9/1968, de 5 de abril, sobre secretos oficiales.

- Orden Ministerial número 76/2002, de 18 de abril, por la que se establece la política de seguridad para la protección de la información del Ministerio de Defensa almacenada, procesada o transmitida por sistemas de información y telecomunicaciones.
- LEY 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.
- Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional.
- Decisión del Consejo de 19 de marzo de 2001, por la que se adoptan las normas de seguridad del Consejo (2001/264/EC)
- Decisión de la Comisión de 29 de noviembre de 2001, por la que se modifica su Reglamento interno (2001/844/CE, CECA, Euratom)

A3.5. Seguridad de las redes y de la información

- COM(2001)298 final -- Seguridad de las redes y de la información: Propuesta para un enfoque político europeo
- OCDE: Directrices para la seguridad de los sistemas y redes de información - Hacia una cultura de seguridad

Apéndice 4. Marco de evaluación y certificación

La complejidad de los sistemas de información conlleva un gran esfuerzo para determinar la calidad de las medidas de seguridad de que se ha dotado y la confianza que merecen. Es frecuente la aparición de terceras partes que de forma independiente emiten juicios sobre dichos aspectos, juicios que se emiten tras una evaluación rigurosa y que se plasman en un documento reconocido.

En este capítulo se repasan someramente dos marcos en los que se ha formalizado el proceso de evaluación y certificación (o registro):

- en los sistemas de gestión de la seguridad de la información
- en los productos de seguridad

Para cada uno de estos marcos se indica su oportunidad, la forma de organizarse para alcanzar la certificación y el marco administrativo y normativo en el que se desarrolla la actividad.

A4.1. Sistemas de gestión de la seguridad de la información (SGSI)

Se define “sistema de gestión” como lo que la Organización hace para gestionar sus procesos o actividades, de forma que los productos que fabrica o los servicios que presta satisfagan los objetivos que la propia organización de ha marcado, típicamente

- satisfacer la calidad demandada por los clientes
- cumplir con las obligaciones legales, regulatorias y contractuales

Dentro del sistema de gestión de una Organización, se entiende por “sistema de gestión de la seguridad de la información” (SGSI) la parte relacionada con la seguridad de la información. Es habitual entender que los sistemas de gestión deben ajustarse al llamado ciclo de Denning (PDCA), habitual en sistemas de gestión de la calidad:

P – Plan – Se establecen objetivos y se preparan planes para alcanzarlos. Esto incluye analizar la situación de la Organización: dónde estamos y dónde queremos estar.

D – Do – Se ejecutan los planes.

C – Check – Se evalúan los resultados obtenidos para determinar en qué medida se han alcanzado los objetivos propuestos.

A – Act – A fin de estar cada día mejor (mejora continua), se actualizan los planes y su implantación.

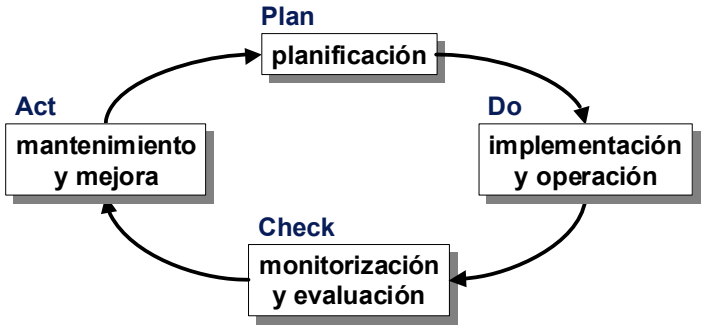

Ilustración 22. Ciclo PDCA

La planificación (P de *Plan*) debe incluir una política de seguridad que marque objetivos y un análisis de riesgos que modele el valor del sistema, su exposición a amenazas, y lo que se tiene (o se necesita) para mantener el riesgo bajo control. Es natural que con estas bases se genere un plan de seguridad razonado para la gestión de riesgos.

La acción (D de *Do*) es la ejecución del plan, en sus aspectos técnicos y de organización, involucrando a las personas que se hacen cargo del sistema o están relacionadas con éste. Un plan tiene éxito cuando lleva a una operación diaria sin sorpresas.

La monitorización (C de *Check*) de la operación del sistema parte del hecho de que no se puede confiar ciegamente en la eficacia de las medidas, sino que continuamente hay que evaluar si responden a lo esperado con la eficacia deseada. Hay que medir tanto lo que ocurre como lo que ocurriría si no se hubieran tomado medidas. A veces se habla del "coste de la inseguridad" como justificación de que el gasto de dinero y esfuerzo tiene fundamento. Y hay que atender a las novedades que se produzcan, tanto en cuanto a modificaciones del propio sistema de información, como a nuevas amenazas.

La reacción (A de *Act*) es saber derivar consecuencias de la experiencia, propia y de sistemas similares, repitiendo el ciclo PDCA.

La evaluación de un sistema de gestión de la seguridad parte del supuesto de que el esquema anterior vertebra las actuaciones de la Organización en materia de seguridad, y juzga la eficacia de los controles implantados para ~~alcanzar~~ asegurarnos de que se alcanzan los objetivos propuestos.

Nótese que un sistema de gestión maduro debe estar documentado en todos sus aspectos. Es típico de organizaciones inmaduras que las actividades se realizan siguiendo normas y procedimientos que se sobreentienden o están en la cabeza de las personas. Sólo cuando todo figura por escrito podemos hablar de un sistema de gestión que puede ser objeto de una certificación.

A4.1.1. La certificación

Certificar un sistema de gestión de la seguridad consiste en que alguien, externo a la Organización y acreditado para la tarea, afirma que ha auditado el sistema y lo considera ajustado a la norma correspondiente. En el caso que nos ocupa, la norma es la UNE-ISO/IEC 27001:2007.

El que certifica compromete en ello su palabra (por escrito). Con todas las cautelas de alcance y tiempo que se consideren oportunas (y se recojan explícitamente). Y sabiendo que lo que se asegura hoy, hay que revisarlo a medio plazo pues todo evoluciona.

Para obtener un certificado hay que seguir una serie de formalismos. Sin entrar en excesivo detalle nos centraremos en qué evalúa el equipo que envía el organismo de certificación a juzgar a la Organización.

Lo primero que hay que hacer es delimitar el alcance de lo que se va a evaluar como "Sistema de Gestión de la Seguridad de la Información". Esta es una delimitación propia de cada Organización, que refleja su misión y su organización interna. Es importante delimitar con claridad. Si el perímetro es difuso no quedará claro qué hay que hacer en los pasos siguientes; en particular, no se sabrá muy bien a qué personas y departamentos hay que dirigirse para reclamar la información pertinente. Nótese que esto puede no ser evidente. Actualmente es raro encontrar una organización cerrada desde el punto de vista de sus sistemas de información: la externalización de servicios, la administración electrónica y el comercio electrónico han diluido las fronteras. Por otra parte, el organigrama interno rara vez responde a las responsabilidades en seguridad.

Lo siguiente que hay que tener claro, escrito y mantenido es la política de seguridad ~~corporativa~~. A menudo la política de seguridad incluye la relación de la legislación que afecta. Es absolutamente necesario delimitar el marco legislativo y regulatorio al que hay que atenerse.

Todo debe estar escrito. Y bien escrito: se entiende, es coherente, se divulga, es conocido por los involucrados y se mantiene al día. Un proceso de certificación siempre tiene un fuerte componente de revisión de documentación.

Antes de que venga el equipo evaluador, hay que tener una foto del estado de riesgo de la Organización. Es decir, que hay que hacer un análisis de riesgos identificando activos, valorándolos, identificando y valorando las amenazas significativas. En este proceso se determina qué salvaguardas requiere el sistema y con qué calidad. Cada caso es un mundo aparte: ni todo el mundo tiene los mismos activos, ni valen lo mismo, ni están igualmente interconectados, ni todo el mundo está sujeto a las mismas amenazas, ni todo el mundo adopta la misma estrategia para protegerse.

El análisis de riesgos es una herramienta (imprescindible) de gestión. Por hacer o dejar de hacer un análisis de riesgos no se está ni más ni menos seguro: simplemente, se sabe dónde se está. A partir de este conocimiento podemos tomar decisiones de tratamiento y ejecutarlas.

Los resultados del análisis de riesgos permiten justificar las decisiones de tratamiento del riesgo. Todo esto deberá ser verificado por el equipo evaluador que, de quedar satisfecho, avalará la concesión del certificado.

El equipo evaluador inspecciona el sistema de información que se desea certificar contrastándolo con una referencia reconocida que permita objetivar la evaluación a fin de evitar cualquier tipo de arbitrariedad o subjetividad y permitir la utilización universal de las certificaciones emitidas. Se utiliza un "esquema de certificación" (en el caso que nos ocupa, la norma UNE-ISO/IEC 27001:2007).

La norma 27001 tiene por objeto la especificación de "los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información con independencia de su tipo, tamaño o área de actividad."

A4.1.2. La acreditación de la entidad certificadora

La credibilidad del certificado es la confianza que merezca el certificador. ¿Cómo se construye esta confianza?

Un componente esencial es la credibilidad del esquema de certificación. Un segundo componente es la credibilidad de la organización que emite los certificados. Esta organización es responsable de la competencia del equipo evaluador y de la ejecución del proceso de evaluación. Para certificar que estas responsabilidades se cumplen se procede al llamado "proceso de acreditación" donde una nueva organización evalúa al evaluador. En España, la organización encargada de acreditar organismos certificadores es ENAC, que se acoge a la normativa internacional de reconocimiento mutuo de certificados emitidos por diferentes certificadores en diferentes países.

A4.1.3. Terminología

Se recogen a continuación los términos usados en las actividades de certificación de sistemas de información, tal y como se entienden en este contexto.

Acreditación

Procedimiento mediante el cual un Organismo autorizado reconoce formalmente que una organización es competente para la realización de una determinada actividad de evaluación de la conformidad.

Auditoría

Ver "evaluación".

Certificación

El objetivo de la certificación es "declarar públicamente que un producto, proceso o servicio es conforme con requisitos establecidos" .

Certification: A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. [NIST 800-37]

Documento de certificación (o registro)

Documento que afirma que el sistema de gestión de la seguridad de la información (SGSI) de una organización es conforme a la normativa de referencia adaptada a la singularidad de la organización certificada.

Documento de selección de controles

Documento que describe los objetivos de control y los controles relevantes y aplicables al Sistema de Gestión de la Seguridad de la Información de la organización. Éste documento debe estar basado en los resultados y conclusiones del proceso de análisis y gestión de riesgos.

Esquema de certificación

Marco técnico y administrativo que establece la referencia de trabajo frente a la que se contrasta el cumplimiento de la organización sometida a evaluación, se emite el certificado o registro y se mantiene actualizado y válido.

Evaluación

Conjunto de actividades que permiten determinar si la organización satisface los criterios aplicables dentro del esquema de certificación. Incluye actividades preparatorias, revisión de la documentación, inspección del sistema de información y la preparación de la documentación pertinente para la emisión del certificado de conformidad, si procede.

Organismo de certificación (o registro)

Entidad que, a la vista del informe de evaluación, certifica (o registra) la satisfacción por la organización de los requisitos establecidos en el esquema de certificación.

Organismos de evaluación de la conformidad

Son los encargados de evaluar y realizar una declaración objetiva de que los servicios y productos cumplen unos requisitos específicos, ya sean del sector reglamentario o del voluntario.

Sistema de gestión

Conjunto de recursos que utiliza una organización para alcanzar sus. El sistema de gestión incluye aspectos tan diversos como

- la estructura organizativa,
- la definición y asignación de responsabilidades,
- la documentación: política(s), normativa, procedimientos, guías, instrucciones, etc.
- la planificación de actividades.

Sistema de gestión de la seguridad de la información

Parte del sistema de gestión que, basado en los riesgos para el negocio, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información.

Política de seguridad

Conjunto de normas reguladoras, reglas y prácticas que determinan el modo en que los activos, incluyendo la información considerada como sensible, son gestionados, protegidos y distribuidos dentro de una organización.

A4.2. Criterios comunes de evaluación (CC)

La necesidad de evaluar la seguridad de un sistema de información aparece muy temprano de la mano de los procesos de adquisición de equipos del Departamento de Defensa de los EEUU que, en 1983, publica el llamado “Libro Naranja” (TCSEC – *Trusted Computer System Evaluation Criteria*). El objetivo es especificar sin ambigüedad qué se necesita por parte del comprador y qué se ofrece por parte del vendedor, de forma que no haya malentendidos sino un esquema transparente de evaluación, garantizando la objetividad de las adquisiciones.

La misma necesidad lleva a la aparición de iniciativas europeas como ITSEC *(Information Technology Security Evaluation Criteria).* A mediados de los años 90, existe en el mundo una proliferación de criterios de evaluación que dificulta enormemente el comercio internacional, llegándose a un acuerdo de convergencia que recibe el nombre de *“Common Criteria for Information Technology Security Evaluation”,* normalmente conocidos como “Criterios Comunes” o por sus siglas, CC.

Los CC, además de la necesidad de un entendimiento universal, capturan la naturaleza cambiante de las tecnologías de la información que, en el periodo desde 1980, han pasado de estar centradas en los equipos de computación, a englobar sistemas de información mucho más complejos.

Los CC permiten

1. definir las funciones de seguridad[35] de los productos y sistemas (en tecnologías de la información) y
2. determinar los criterios para evaluar [la calidad] de dichas funciones.

Es esencial la posibilidad que los CC abren para que la evaluación sea objetiva y pueda realizarse por una tercera parte (ni por el proveedor, ni por el usuario) de forma que la elección de salvaguardas adecuadas se vea notablemente simplificada para las organizaciones que necesitan mitigar sus riesgos.

La administración española, y otras muchas, reconocen las certificaciones de seguridad emitidas en otros países en base al "Arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes en el Campo de la Tecnología de la Información"[36].

La evaluación de un sistema es la base para su certificación. Para certificar es necesario disponer de

1. unos criterios, que definen el significado de los elementos que se van a evaluar
2. una metodología, que marque cómo se lleva a cabo la evaluación
3. un esquema de certificación[37] que fije el marco administrativo y regulatorio bajo el que se realiza la certificación

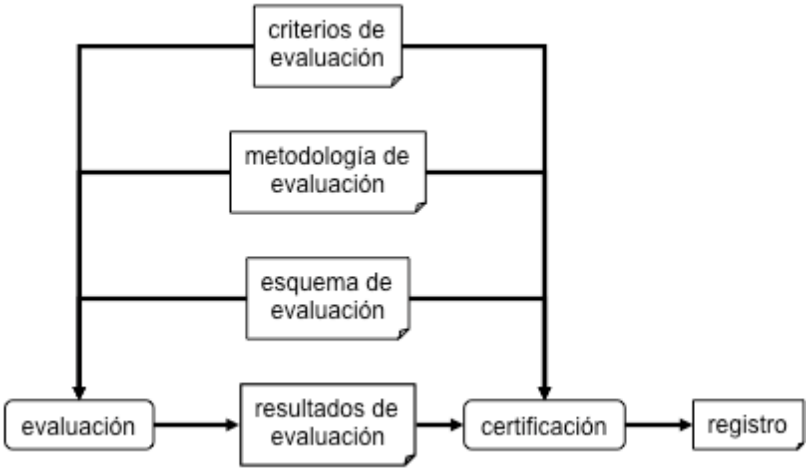

Ilustración 23. Proceso de certificación

De esta forma se puede garantizar la objetividad del proceso; es decir, construir la confianza en que los resultados de un proceso de certificación son válidos universalmente, independientemente de dónde se realice la certificación.

Dado que [la calidad de] la seguridad requerida de un sistema no es siempre la misma, sino que depende de para qué se quiera emplear, CC establece una escala de niveles de aseguramiento[38]:

EAL0: sin garantías

EAL1: probado funcionalmente

35 En CC se emplea una terminología propia, rigurosa pero no siempre intuitiva. Más adelante se recoge la definición precisa de cada término en el contexto de los CC.

36 El día 23 de mayo de 2000 tuvo lugar en Baltimore (Maryland, Estados Unidos) la ratificación de la adhesión de Alemania, Australia, Canadá, España, Estados Unidos, Finlandia, Francia, Grecia, Italia, Noruega, Nueva Zelanda, Países Bajos y Reino Unido, al Arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes en el campo de la Seguridad de la Tecnología de la Información (en lo sucesivo Arreglo). Posteriormente, se han incorporado Israel, Suecia, Austria, Turquía, Hungría, Japón, República Checa, Corea, Singapur e India. Véase http://www.csi.map.es/csi/pg3433.htm.

37 El Real Decreto 421/2004 de 12 de marzo, regula las funciones del Centro Criptológico Nacional, entre cuyas funciones aparece la de "constituir el organismo de certificación del esquema nacional de evaluación y certificación de la seguridad de las tecnologías de información, de aplicación a productos y sistemas en su ámbito." El esquema nacional puede encontrarse en http://www.oc.ccn.cni.es/ .

38 EAL: Evaluation Assurance Level

EAL2: probado estructuralmente

EAL3: probado y chequeado metódicamente

EAL4: diseñado, probado y revisado metódicamente

EAL5: diseñado y probado semi-formalmente

EAL6: diseñado, probado y verificado semi-formalmente

EAL7: diseñado, probado y verificado formalmente

Los niveles superiores requieren un mayor esfuerzo de desarrollo y de evaluación, ofreciendo a cambio unas grandes garantías a los usuarios. Por ejemplo, en el ámbito de la firma electrónica, los dispositivos seguros de firma suelen certificarse contra un perfil de nivel EAL4+[39].

A4.2.1. Beneficiarios

Los CC se dirigen a una amplia audiencia de potenciales beneficiarios de la formalización de los conceptos y elementos de evaluación: los consumidores (usuarios de productos de seguridad), los desarrolladores y los evaluadores. Un lenguaje común entre todos ellos se traduce en ventajas apreciables:

Para los consumidores

- que pueden expresar sus necesidades, antes de adquirir los servicios o productos que las satisfagan; esta caracterización puede resultar útil tanto en adquisiciones individuales, como en la identificación de necesidades de grupos de usuarios
- que pueden analizar las características de los servicios o productos que ofrece el mercado
- que pueden comparar diferentes ofertas

Para los desarrolladores

- que saben qué se les va a exigir y cómo se van a evaluar sus desarrollos
- que saben, objetivamente, qué requieren los usuarios
- que pueden expresar sin ambigüedad lo que hacen sus desarrollos

Para los evaluadores

- que disponen de un marco formalizado para saber qué tienen que evaluar y cómo tienen que calificarlo

Para todo el mundo

- que dispone de unos criterios objetivos que permiten aceptar las certificaciones realizadas en cualquier parte

Todos estos participantes convergen sobre un objeto a evaluar denominado **TOE** *(Target Of Evaluation*)**,** que es el servicio o producto (de seguridad) cuyas características (de seguridad) se quieren evaluar.

Cuando un análisis de riesgos expone la relación de salvaguardas adecuadas, estas pueden venir expresadas en terminología CC, lo que permite engarzar con las ventajas citadas, convirtiéndose en una especificación normalizada.

A4.2.2. Requisitos de seguridad

Dado un sistema se pueden determinar, a través de un análisis de riesgos, qué salvaguardas se requieren y con qué calidad. Este análisis puede hacerse sobre un sistema genérico o sobre un sistema concreto. En CC, el conjunto de requisitos que se le exigen a un sistema genérico se de-

39 Cuando un producto está entre dos niveles, se indica su nivel inferior seguido de un signo "+" que se lee como "aumentado". Así, un producto evaluado EAL4+ significa que cumple todos los niveles de calidad del nivel 4 y algunos de niveles superiores.

nomina **perfil de protección** (**PP** – *Protection Profile*). Si no se está hablando de un sistema genérico, sino de un sistema concreto, el conjunto de requisitos se conoce como **declaración de seguridad** (**ST** – *Security Target*).

Los PP, dado su carácter genérico, cubren diferentes productos concretos. Suelen ser preparados por grupos de usuarios u organismos internacionales que quieren modelar el mercado[40].

Los ST, dado su carácter específico, cubren un producto concreto. Suelen ser preparados por los propios fabricantes que de esta manera formalizan su oferta[41].

CC determina los apartados en que debe estructurarse un PP o un ST. El índice de estos documentos es un buen indicador de su alcance:

PP- perfil de protección	*ST – declaración de seguridad*
— Introduction — TOE description — Security environment • assumptions • threats • organizational security policies — Security objectives • for the TOE • for the environment — Security requirements • for the environment • TOE functional requirements • TOE assurance requirements — Application notes — Rationale	— Introduction — TOE description — Security environment • assumptions • threats • organizational security policies — Security objectives • for the TOE • for the environment — Security requirements • for the environment • TOE functional requirements • TOE assurance requirements — TOE summary specification — PP claims • PP reference • PP tailoring • PP additions — Rationale

Tabla 11. Perfiles de protección y Declaraciones de seguridad

Los PP y los ST pueden ser a su vez sometidos a una evaluación formal que verifique su completitud e integridad. Los PP así evaluados pueden pasar a registros públicos para ser compartidos por diferentes usuarios.

En la elaboración de un ST se hace referencia a los PP a los que se acoge.

A4.2.3. Creación de perfiles de protección

La generación de un PP o un ST es básicamente un proceso de análisis de riesgos donde el analista, habiendo determinado el dominio del análisis (el TOE en terminología de CC), identifica amenazas y determina, a través de los indicadores de impacto y riesgo, las salvaguardas que se requieren. En la terminología de CC, las salvaguardas requeridas se denominan **requisitos de seguridad** y se subdividen en dos grandes grupos

40 Un ejemplo típico de PP podría ser aquel que fija las características de seguridad que se deben exigir a un cortafuegos.

41 Un ejemplo típico de ST podría ser aquel que fija las características de seguridad del modelo 3000 del fabricante XXL S.A., un modelo que permite cifrar las comunicaciones telefónicas.

requisitos funcionales de seguridad *(functional requirements)*

- ¿qué hay que hacer?
- definen el comportamiento funcional del TOE

requisitos de garantía de la funcionalidad de la seguridad *(assurance requirements)*

- ¿está el TOE bien construido?
- ¿es eficaz? ¿satisface el objetivo para el que se requiere?
- ¿es eficiente? ¿alcanza sus objetivos con un consumo razonable de recursos?

Es importante destacar que CC establece un lenguaje común para expresar los objetivos funcionales y de aseguramiento. Es necesario pues que el análisis de riesgos utilice esta terminología en la selección de salvaguardas. La norma CC nos proporciona en su parte 2 el catálogo estandarizado de objetivos funcionales, mientras que en su parte 3 nos proporciona el catálogo estandarizado de objetivos de aseguramiento.

Parte 2: Requisitos funcionales	*Parte 3: Requisitos de garantía*
FAU: Security audit	ACM: Configuration management
FCO: Communication	ADO: Delivery and operation
FCS: Cryptographic support	ADV: Development
FDP: User data protection	AGD: Guidance documents
FIA: Identification and authentication	ALC: Life cycle support
FMT: Security management	ATE: Tests
FPR: Privacy	AVA: Vulnerability assessment
FPT: Protection of the TOE security functions	APE: PP evaluation
FRU: Resource utilisation	ASE: ST evaluation
FTA: TOE access	
FTP: Trusted path / channels	

Tabla 12. Requisitos funcionales y de aseguramiento de la función

A4.2.4. Uso de productos certificados

Cuando un TOE ha sido certificado de acuerdo a un PP o un ST, según convenga en cada caso, se puede tener la certeza de que dicho TOE satisface las necesidades y además las satisface con la calidad requerida (por ejemplo, EAL4).

La certificación de un sistema o producto no es garantía ciega de idoneidad: es necesario cerciorarse de que el PP o ST respecto del que se han certificado satisface los requisitos de nuestro sistema. El análisis de riesgos nos ha permitido elaborar el PP o el ST o, en ocasiones, seleccionar un conjunto apropiado a nuestro mapa de riesgos. Pero lo esencial es que de análisis de riesgos se han obtenido unos requisitos de seguridad cuya satisfacción permitirá mantener impacto y riesgo residuales bajo control.

En la medida en que un producto certificado se ajusta a un PP o ST que satisface nuestras necesidades, la gestión de riesgos se reduce a adquirir el producto, instalarlo y operarlo en las condiciones adecuadas.

Es importante destacar que tanto los PP como los ST incluyen una sección denominada “hipótesis” *(assumptions)* en la que se establecen una serie de prerrequisitos que debe satisfacer el entorno operacional en el que se instala TOE. No se hace sino reconocer que el mejor producto, inadecuadamente instalado u operado, es incapaz de garantizar la satisfacción de los objetivos globales. Por ello, los productos certificados son componentes muy sólidos de un sistema; pero además hay que garantizar su entorno para asegurar el sistema completo.

A4.2.5. Terminología

Debido a que su objetivo es servir de referencia internacional y sustentar evaluaciones y certificaciones, los criterios comunes deben ser muy precisos en su terminología. En el texto previo se han venido introduciendo los términos según se necesitaban; estos términos se recogen formalmente a continuación:

Assurance (garantía)

Base de la confianza en que una entidad cumple sus objetivos de seguridad.

Evaluation (evaluación)

Valoración de un PP, ST o TOE frente a criterios definidos.

Evaluation Assurance Level (EAL) (nivel de garantía de evaluación)

Paquete que consiste en componentes de garantía de la Parte 3 y que representa un nivel en la escala de garantía predefinida de CC.

Evaluation authority (autoridad de evaluación)

Organismo que implementa los CC para una comunidad específica mediante un esquema de evaluación por el que se establecen las normas y se supervisa la calidad de las evaluaciones realizadas por organismos de dicha comunidad.

Evaluation scheme (esquema de evaluación)

Marco administrativo y regulador bajo el que una autoridad de evaluación aplica los CC en una comunidad específica.

Formal

Expresado en un lenguaje de sintaxis restringida con una semántica definida basada en conceptos matemáticos bien establecidos.

Informal

Expresado en lenguaje natural.

Organisational security policies (Políticas de seguridad organizativas)

Una o más reglas de seguridad, procedimientos, prácticas o directrices impuestas por una organización sobre sus operaciones.

Product (producto)

Paquete de *software*, *firmware* y/o *hardware* de TI que proporciona una funcionalidad diseñado para su uso o su incorporación en una gran variedad de sistemas.

Protection Profile (PP) (perfil de protección)

Conjunto de requisitos de seguridad, independiente de la implementación, para una categoría de TOEs que satisfacen unas necesidades específicas del consumidor.

Security objective (objetivo de seguridad)

Declaración de la intención de contrarrestar las amenazas identificadas y/o de cumplir las políticas e hipótesis de seguridad identificadas de la organización.

Security Target (ST) (declaración de seguridad)

Conjunto de requisitos de seguridad y especificaciones utilizados como base de la evaluación de un TOE identificado.

Semiformal

Expresado en un lenguaje de sintaxis restringida con semántica definida.

System (sistema)

Instalación específica de TI, con un propósito y en un entorno particulares.

Target of Evaluation (TOE) (objeto a evaluar)

Producto o sistema de TI y sus manuales de administrador y de usuario asociados que se somete a evaluación.

TOE Security Functions (TSF) (funciones de seguridad del TOE)

Conjunto compuesto de todo el *hardware*, *firmware* y *software* del TOE con el que hay que contar para la correcta aplicación de la TSP.

TOE Security Policy (TSP) (política de seguridad del TOE)

Conjunto de reglas que regulan cómo se gestionan, protegen y distribuyen los activos en el TOE.

Apéndice 5. Herramientas

La realización de un proyecto de análisis de riesgos supone trabajar con una cierta cantidad de activos que rara vez baja de las decenas y que habitualmente son algunos centenares. El número de amenazas típicamente está del orden de las decenas, mientras que el número de salvaguardas está en los millares. Todo ello nos indica que hay que manejar multitud de datos y combinaciones entre ellos, lo que lleva lógicamente a buscar apoyo de herramientas automáticas.

Como requisitos generales, una herramienta de apoyo al análisis de riesgos debe:

- permitir trabajar con un conjunto amplio de activos, amenazas y salvaguardas;
- permitir un tratamiento flexible del conjunto de activos para acomodar un modelo cercano a la realidad de la Organización;
- ser utilizada a lo largo de los tres procesos que constituyen el proyecto, especialmente como soporte al proceso P2, Análisis de Riesgos y
- no ocultar al analista el razonamiento que lleva a las conclusiones.

Las herramientas pueden hacer un tratamiento cualitativo o cuantitativo de la información. La opción entre uno y otro planteamiento ha sido motivo de largo debate. Los modelos cualitativos ofrecen resultados útiles antes que los modelos cuantitativos, simplemente porque la captura de datos cualitativa es más ágil que la cuantitativa[42]. Los modelos cualitativos son eficaces relativizando lo más importante de lo que no es tan importante; pero agrupan las conclusiones en grandes grupos. Los modelos cuantitativos, por el contrario, consiguen una ubicación precisa de cada aspecto.

Impacto y riesgo residual pueden ser cualitativos hasta que aparecen grandes inversiones y hay que determinar su racionalidad económica: ¿qué es lo que interesa más? En este punto se necesitan números.

Una opción mixta es útil: un modelo cualitativo para el sistema de información completo, con capacidad de entrar en un modelo cuantitativo para aquellos componentes cuya protección va a requerir fuertes desembolsos.

También es cierto que el modelo de valor de una Organización debe emplearse durante largo tiempo, al menos durante los años que dure el plan de seguridad para analizar el efecto de la ejecución del plan de seguridad. Es notablemente más dificultoso generar un modelo de valor desde cero que ir adaptando un modelo existente a la evolución de los activos del sistema y a la evolución de los servicios que presta la Organización. En esta evolución continua puede afrontarse la progresiva migración de un modelo cualitativo inicial hacia un modelo cada vez más cuantitativo.

Es de destacar que los datos de caracterización de las posibles amenazas son datos tentativos en los primeros modelos; pero la experiencia permite ir ajustando las valoraciones a la realidad.

Sean herramientas cualitativas o cuantitativas, estas deben:

- Manejar un catálogo razonablemente completo de tipos de activos. En esta línea se orienta el capítulo 2 del "Catálogo de Elementos".
- Manejar un catálogo razonablemente completo de dimensiones de valoración. En esta línea se orienta el capítulo 3 del "Catálogo de Elementos".
- Ayudar a valorar los activos ofreciendo criterios de valoración. En esta línea se orienta el capítulo 4 del "Catálogo de Elementos".
- Manejar un catálogo razonablemente completo de amenazas. En esta línea se encamina el capítulo 5 del "Catálogo de Elementos".

42 Hay que valorar activos y esta es una tarea de consenso. Tanto la valoración como la búsqueda del consenso son notablemente más rápidas si hay que determinar un orden de magnitud que si hay que determinar un número absoluto.

- Manejar un catálogo razonablemente completo de salvaguardas. En esta línea se orienta el capítulo 6 del "Catálogo de Elementos".
- Evaluar el impacto y el riesgo residuales.

Es interesante que las herramientas puedan importar y exportar los datos que manejan en formatos fácilmente procesables por otras herramientas, cabiendo citar

- XML – Extended Markup Language

  que es la opción tomada en esta guía, que establece formatos XML de intercambio
- CSV – Comma Separated Values

A5.1. PILAR

PILAR, acrónimo de “Procedimiento Informático-Lógico para el Análisis de Riesgos” es una herramienta desarrollada bajo especificación del Centro Nacional de Inteligencia para soportar el análisis de riesgos de sistemas de información siguiendo la metodología Magerit.

La herramienta soporta todas las fases del método Magerit:

- Caracterización de los activos: identificación, clasificación, dependencias y valoración
- Caracterización de las amenazas
- Evaluación de las salvaguardas

La herramienta incorpora los catálogos del "Catálogo de Elementos" permitiendo una homogeneidad en los resultados del análisis:

- tipos de activos
- dimensiones de valoración
- criterios de valoración
- catálogo de amenazas

Para incorporar este catálogo, PILAR diferencia entre el motor de cálculo de riesgos y la biblioteca de elementos, que puede ser reemplazada para seguir el paso de la evolución en el tiempo de los catálogos de elementos.

La herramienta evalúa el impacto y el riesgo, acumulado y repercutido, potencial y residual, presentándolo de forma que permita el análisis de por qué se da cierto impacto o cierto riesgo.

Las salvaguardas se califican por fases, permitiendo la incorporación a un mismo modelo de diferentes situaciones temporales. Típicamente se puede incorporar el resultado de los diferentes proyectos de seguridad a lo largo de la ejecución del plan de seguridad, monitorizando la mejora del sistema.

Los resultados se presentan en varios formatos: informes RTF, gráficas y tablas para incorporar a hojas de cálculo. De esta forma es posible elaborar diferentes tipos de informes y presentaciones de los resultados.

Por último, la herramienta calcula calificaciones de seguridad siguiendo los epígrafes de normas *de iure* o *de facto* de uso habitual. Caben citarse:

- UNE-ISO/IEC 27002:2009: sistemas de gestión de la seguridad
- RD 1720/2007: datos de carácter personal
- RD 3/2010: Esquema Nacional de Seguridad

Por último hay que destacar que PILAR incorpora tanto los modelos cualitativo como cuantitativo, pudiendo alternarse entre uno y otro para extraer el máximo beneficio de las posibilidades teóricas de cada uno de ellos.

Apéndice 6. Evolución de Magerit

La primera de Magerit, publicada en 1997 ha resistido en su mayor parte el paso del tiempo, ratificándose en lo fundamental. No obstante, el tiempo pasado permite mejorar notablemente aquella primera versión.

La segunda versión, publicada en 2005, se planteó como revisión constructiva, adaptándola al tiempo presente e incorporando la experiencia de estos años.

Esta tercera versión busca una nueva adaptación, teniendo en cuenta no solo la experiencia práctica sino también la evolución de las normas internacionales de ISO que constituyen un referente obligado.

A6.1. Para los que han trabajado con Magerit v1

Si usted ha trabajado con Magerit v1.0, todos los conceptos le resultarán familiares, aunque hay cierta evolución. En particular reconocerá lo que se denominaba submodelo de elementos: activos, amenazas, vulnerabilidades, impactos, riesgos y salvaguardas. Esta parte conceptual ha sido refrendada por el paso del tiempo y sigue siendo el eje alrededor del cual se vertebran las fases fundamentales de análisis y gestión. Se ha corregido y ampliado lo que se denominaba "subestados de seguridad" dándole el nuevo nombre de "dimensiones"[43] e introduciendo nuevas varas de medir lo que interesa de los activos. El submodelo de procesos aparece bajo el epígrafe de "estructuración del proyecto de análisis y gestión de riesgos".

Si bien Magerit v1.0 ha resistido bien el paso del tiempo en lo conceptual, no se puede decir lo mismo de los detalles técnicos de los sistemas de información con los que se trabaja. Se intenta una puesta al día; pero ante todo se intenta diferenciar lo que es esencial (y permanente) de lo que es coyuntural y cambiará con el tiempo. Esto se traduce en parametrizar el método de trabajo, referenciándolo a catálogos externos de amenazas y salvaguardas que se podrán actualizar, adaptándose al paso del tiempo. Así pues, quede el método, abierto de forma que estando claro qué se hace y cómo, se puedan adaptar los detalles a cada momento.

Los 7 libros segregados en Magerit versión 1, han evolucionado:

Magerit versión 1	Magerit versión 3
Libro I. Guía de aproximación a la seguridad de los sistemas de información	Libro I – Método
Libro II. Guía de procedimientos	Libro I – Método
Libro III. Guía de técnicas	Guía de Técnicas
Libro IV. Guía para desarrolladores de aplicaciones	Libro I – Método / Capítulo 7 Desarrollo de sistemas de información
Libro V. Guía para responsables del dominio protegible	Libro I – Método Libro II – Catálogo de Elementos
Libro VI. Arquitectura de la información y especificaciones de la interfaz para el intercambio de datos	Libro II – Catálogo de Elementos / formatos XML
Libro VII. Referencia de normas legales y técnicas	Libro I – Método / Apéndice 3. Marco legal

43 Dimensión, en una de las acepciones del Diccionario de la Lengua Española, dícese que es "Cada una de las magnitudes de un conjunto que sirven para definir un fenómeno. Por ejemplo, el espacio de cuatro dimensiones de la teoría de la relatividad."

A6.2. Para los que han trabajado con Magerit v2

Esta versión 3 mantiene en gran medida la estructura de la versión 2:

- Libro I – Método
- Libro II – Catálogo de Elementos
- Técnicas

Cambios en la versión 3:

- mejor alineamiento con la normativa ISO, buscando una integración de las tareas de análisis de riesgos dentro de un marco organizacional de gestión de riesgos dirigido desde los órganos de gobierno
- se aligera el texto
- se eliminan partes poco importantes o poco usadas
- se normalizan las diferentes actividades
    - MAR – Método de Análisis de Riesgos
    - PAR – Proyecto de Análisis de Riesgos
    - PS – Plan de Seguridad