MINISTERIO DE
ADMINISTRACIONES
PÚBLICAS

MAGERIT – versión 2

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

I - Método

Madrid, 16 de junio de 2005
NIPO 326-05-047-X

EQUIPO RESPONSABLE DEL PROYECTO MAGERIT versión 2

Director:
Francisco López Crespo
Ministerio de Administraciones Públicas

Miguel Angel Amutio Gómez
Ministerio de Administraciones Públicas

Javier Candau
Centro Criptológico Nacional

Consultor externo:
José Antonio Mañas
Catedrático
Universidad Politécnica de Madrid

Índice

1. Introducción a Magerit

El CSAE[1] ha elaborado y promueve Magerit[2] como respuesta a la percepción de que la Administración (y en general toda la sociedad) depende de forma creciente de las tecnologías de la información para la consecución de sus objetivos de servicio. La razón de ser de Magerit está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios.

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 Guías de la OCDE[3] que, en su principio 6 dice:

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

Esta metodología interesa a todos aquellos que trabajan con información mecanizada y los sistemas informáticos que la tratan. Si dicha información o los servicios que se prestan gracias a ella son valiosos, esta metodología les permitirá saber cuánto de este valor está en juego y les ayudará a protegerlo.

Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos y por ello han aparecido multitud de guías informales, aproximaciones metódicas y herramientas de soporte todas las cuales buscan objetivar el análisis para saber cuán seguros (o inseguros) están 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 se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Pese a que se ha puesto en manos de los sistemas de información graves responsabilidades para cumplir los objetivos de las organizaciones, 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 en defensa de los medios de trabajo no se traduce 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.

1.1. Objetivos de Magerit

Magerit persigue los siguientes objetivos:

Directos:

1. concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo
2. ofrecer un método sistemático para analizar tales riesgos
3. ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control

Indirectos:

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

1 CSAE: Consejo Superior de Administración Electrónica.
2 MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
3 Guías de la OCDE para la seguridad de los sistemas de información y redes. Hacia una cultura de seguridad. 2002.

También se ha buscado la uniformidad de los informes que recogen los hallazgos y las conclusiones de un proyecto 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.

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.

Plan de seguridad

Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos

1.2. 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 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.

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.

Autenticidad (de quién hace uso de los datos o servicios):

o que no haya duda de quién se hace responsable de una información o prestación de un servicio, tanto a fin de confiar en él como de poder perseguir posteriormente los incumplimientos o errores. Contra la autenticidad se dan suplantaciones y engaños que buscan realizar un fraude. La autenticidad es la base para poder luchar contra el repudio y, como tal, fundamenta el comercio electrónico o la administración electrónica, permitiendo confiar sin papeles ni presencia física.

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 es-

fuerzo 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:

Gestión de riesgos:

selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

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.

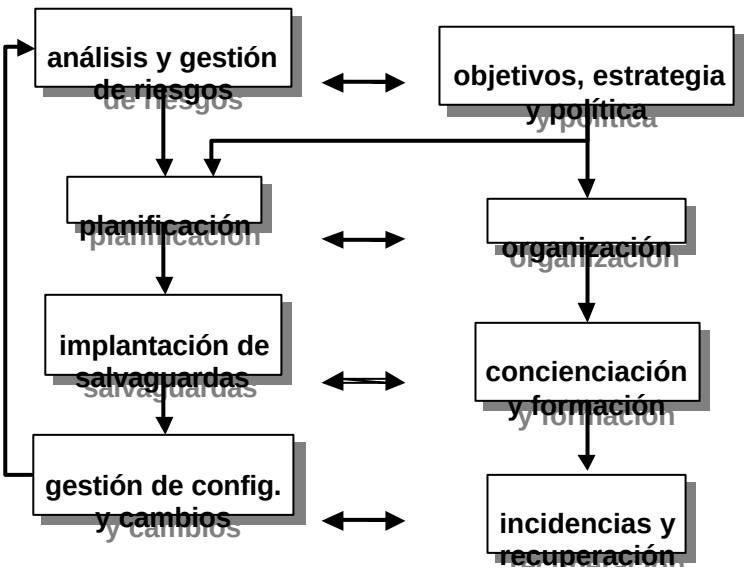
Como todo esto es muy delicado, no es meramente técnico, e incluye la decisión de aceptar un cierto nivel de riesgo, deviene imprescindible saber en qué condiciones se trabaja y así poder ajustar la confianza que merece el sistema. Para ello qué mejor que una aproximación metódica que permita tomar decisiones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

1.3. El análisis y gestión de riesgos en su contexto

Las tareas de análisis y gestión de 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 protegidos se encuentran los activos. En coordinación con los objetivos, estrategia y política de la Organización, las actividades de gestión de riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que se acepta la Dirección.

La implantación de los controles 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 gestión de riesgos es la estructuración de las acciones de seguridad para satisfacer las necesidades de-

tectadas por el análisis.

1.3.1. 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 o de “luchar contra las 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 dos 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 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, que facilite el cumplimiento de las buenas prácticas propuestas y
- practicada por la Dirección que de ejemplo en la actividad diaria y reaccione con presteza a los cambios e incidencias.

1.3.2. Incidencias y recuperación

Simétricamente, las personas involucradas 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 salvaguardas responderá a la realidad.

Cuando se produce una incidencia, el tiempo empieza a correr en contra del sistema: su supervivencia depende de la presteza 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.

Tanto de los éxitos como de los fracasos conviene aprender continuamente e incorporarlos al proceso de análisis y 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.

1.4. Organización de las guías

Esta versión 2 de Magerit se ha estructurado en tres libros: éste, que describe “El Método”, un "Catálogo de Elementos" y una "Guía de Técnicas".

Esta guía describe la metodología desde tres ángulos:

- El capítulo 2 describe los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación. Es una presentación netamente conceptual.
- El capítulo 3 describe las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, entendiendo que no basta con tener los conceptos claros, sino que es conveniente pautar roles, actividades, hitos y documentación para que la realización del proyecto de análisis y gestión de riesgos esté bajo control en todo momento.
- El capítulo 4 aplica la metodología al caso del desarrollo de sistemas de información, en el entendimiento que los proyectos de desarrollo de sistemas deben tener en cuenta los riesgos desde el primer momento, tanto los riesgos a que están expuestos, como los riesgos que las propias aplicaciones introducen en el sistema.

Como complemento, el capítulo 5 desgrana una serie de aspectos prácticos, derivados de la experiencia acumulada en el tiempo para la realización de un análisis y una gestión realmente efectivos.

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,
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 en esta versión 2.

Por ultimo, se desarrolla un caso práctico como ejemplo.

1.4.1. Modo de empleo

Los lectores nuevos en la materia, deben empezar por el capítulo 2.

Si ya hay un conocimiento de los conceptos, el ejemplo ayuda a centrar ideas y terminología.

Si se va a lanzar un proyecto de análisis y gestión de riesgos, el capítulo 3 ayuda a estructurarlo y planificarlo. Si el sistema de información es simple y reducido o bien si sólo se requiere una primera aproximación, puede bastar un planteamiento informal; pero cuando el proyecto toma envergadura conviene ser metódico.

Si se está realizando un proyecto de análisis y gestión de riesgos, el capítulo 5 ayuda a centrar la actividad sin distracciones.

Si se va a colaborar en un proyecto de desarrollo de un nuevo sistema de información, o en un ciclo de mantenimiento, conviene recurrir al capítulo 4.

Si se va a trabajar con sistemas homologados, bien porque interesa como mecanismo para especificar lo que se necesita, bien porque interesa como mecanismo para especificar lo que se tiene, conviene recurrir al apéndice 4.

En el planteamiento de estas guías se ha seguido un criterio “de máximos”, reflejando todo tipo de activos, todo tipo de aspectos de seguridad, todo tipo de situaciones, en definitiva. 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 disponibilidad de los servicios (típicamente porque se busca el desarrollo de un plan de contingencia)
- etc.

Estas situaciones, frecuentes, se recogen formalmente en las tareas de la actividad A1.2 e informalmente comentando que es constructivo centrarse en un dominio reducido e ir ampliando en la medida de las necesidades, antes que afrontar la totalidad.

1.4.2. 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.

1.4.3. La guía de técnicas

En libro aparte, aporta luz adicional y guías 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
  - análisis coste-beneficio
  - diagramas de flujo de datos
  - diagramas de procesos
  - técnicas gráficas
  - planificación de proyectos
  - 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.

1.5. Para los que han trabajado con Magerit v1.0

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”[4] 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”.

4 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.”*

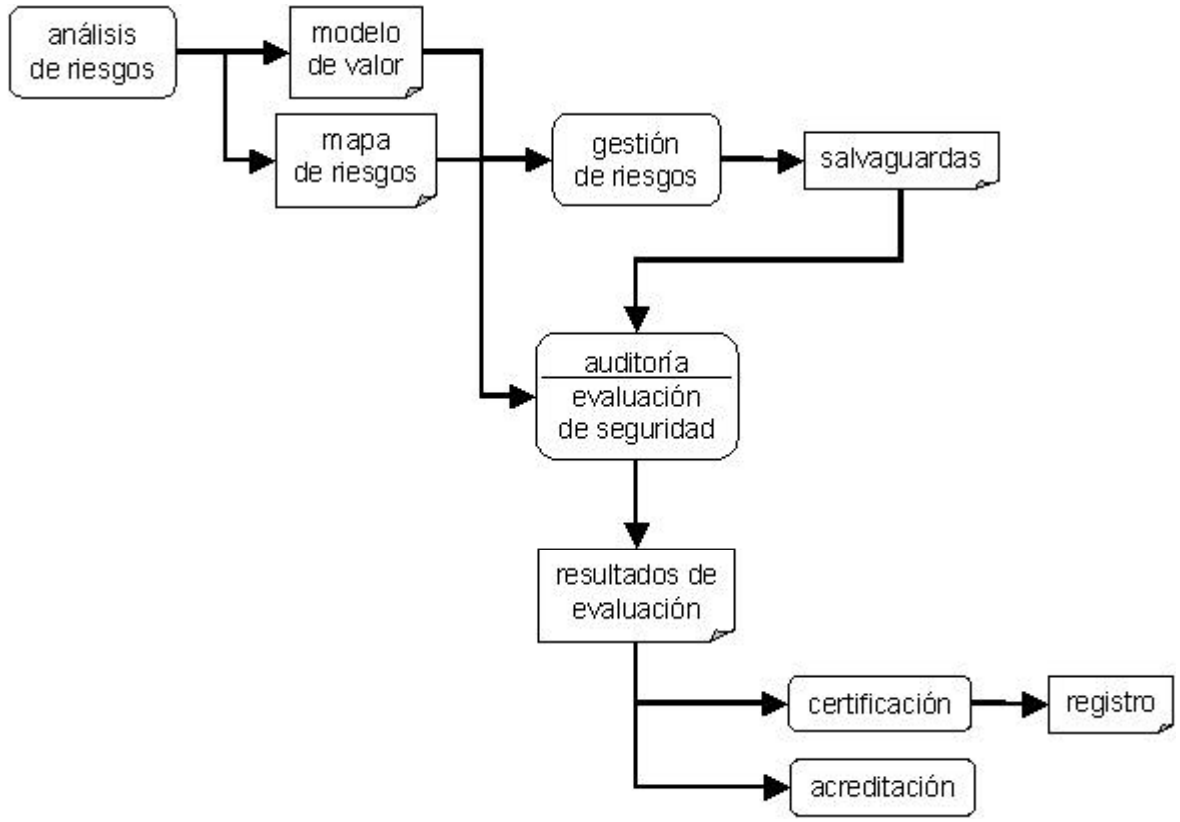
Si bien Magerit v1.0 ha resistido bien el paso del tiempo en lo conceptual, no se puede decir lo mismo de los detalles técnicos de los sistemas de información con los que se trabaja. Se intenta una puesta al día; pero ante todo se intenta diferenciar lo que es esencial (y permanente) de lo que es coyuntural 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, tanto por progreso tecnológico como por progreso de los sujetos, pues tan cierto es que los sistemas cambian como que lo hacen los sujetos a su alrededor, buenos y malos. Y, cuanto más éxito tengan los sistemas, más usuarios tendrán y simultáneamente, más sujetos habrá interesados en abusar de ellos o, simplemente, destruirlos. Así pues, quede el método, abierto de forma que estando claro qué se hace y cómo, se puedan adaptar los detalles a cada momento.

A efectos prácticos, el párrafo anterior se traduce en que se ha segregado en un libro anejo, “Catálogo de Elementos”, los tipos de activos, las dimensiones y criterios de valoración, el catálogo de amenazas y el catálogo de salvaguardas, de tal forma que puedan evolucionar.

El apéndice 6 es más preciso estableciendo las correspondencias entre la versión 1.0 y esta.

1.6. 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. En 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 riesgo paso obligado para poder llevar a cabo todas las tareas mencionadas, que se relacionan según el siguiente esquema:



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[5].

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?[6]. 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.

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,
- 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 al

5 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.

6 Y así tenemos sistemas aptos para "consumo humano" o "utilización en condiciones térmicas extremas".

> presente Reglamento, 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 994/1999, artículo 17.2]

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

- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
- "Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades", MAP, 2004

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.

1.7. ¿Cuándo procede analizar y gestionar los riesgos?

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 datos 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.

Un análisis de riesgos 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 inversión en tecnología, desde la adquisición de equipos de producción hasta el despliegue de un centro alternativo para asegurar la continuidad de la actividad, pasando por las decisiones de adquisición de salvaguardas técnicas y de selección y capacitación del personal.

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 de las aplicaciones 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.

Por precepto legal

El análisis de riesgos puede venir requerido por precepto legal. Tal es el caso del Real Decreto 263/1996, de 16 de Febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado. En su artículo 4 (Garantías generales de la utilización de soportes, medios y aplicaciones electrónicas, informáticas y telemáticas) dice así:

> 2. Cuando se utilicen los soportes, medios y aplicaciones referidos en el apartado anterior, se adoptarán las medidas técnicas y de organización necesarias que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información. Dichas medidas de seguridad deberán tener en cuenta el estado de la tecnología y ser proporcionadas a

la naturaleza de los datos y de los tratamientos y a *los riesgos a los que estén expuestos*[7].

De forma similar, en 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.

Texto que se recoge de nuevo en el preámbulo al REAL DECRETO 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. En este decreto se recoge la obligación de elaborar un documento de seguridad

1. El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.

Difícilmente se puede desarrollar dicho documento sin un análisis previo de los riesgos sobre los datos, análisis que nos lleve a determinar las medidas de seguridad pertinentes.

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[8] 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 último, cabe mencionar el empleo de perfiles de protección como mecanismo de contratación. Los perfiles de protección (ISO/IEC-15408) nacen con la doble misión de poder especificar a priori los requisitos de seguridad de un sistema (para su adquisición o desarrollo) y poder servir de referencia internacional del significado de una certificación. En uno u otro caso, establece la “vara de medir” respecto de la que se calificará la idoneidad de la seguridad del sistema. Véase el apéndice 4.2 sobre criterios comunes de evaluación (CC).

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.

7 El análisis de riesgos permite determinar los riesgos a los que están expuestos y la gestión de riesgos permite adecuar las medidas a dichos riesgos.

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

2. Realización del análisis y de la gestión

Este capítulo expone de forma conceptual en qué consiste esto del análisis de riesgos y aquello de su gestión, qué se busca en cada momento y qué conclusiones se derivan.

Hay dos grandes tareas a realizar:

análisis de riesgos,

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

Elementos:

1. activos, que no son sino los elementos del sistema de información (o estrechamente relacionados con este) que aportan valor a la Organización
2. amenazas, que no son sino cosas que les pueden pasar a los activos causando un perjuicio a la Organización
3. salvaguardas (o contra medidas), que no son sino elementos de defensa desplegados 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.

gestión de 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.

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.

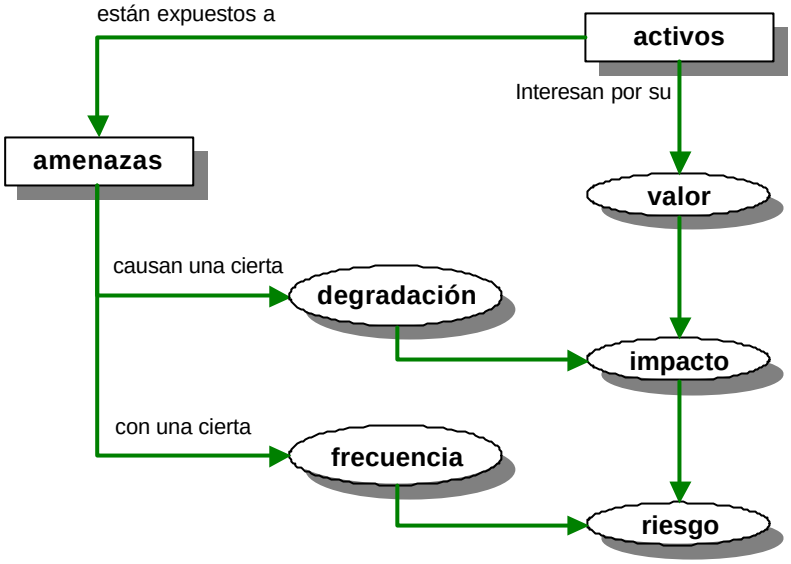
2.1. Análisis de Riesgos

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 expectación de materialización) de la amenaza

Con el objeto de organizar la presentación, se tratan primero los pasos 1, 2, 4 y 5, obviando el paso 3, de forma que las estimaciones de impacto y riesgo sean “potenciales”: 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[9]:



2.1.1. Paso 1: Activos

Se denominan activos los **recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección.**

El activo esencial es la información que maneja el sistema; o sea los datos. Y alrededor de estos datos se pueden identificar otros activos relevantes:

Los servicios que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.

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

Los equipos informáticos *(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.

Tipos de activos

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.

Si el sistema maneja datos de carácter personal, estos suelen ser importantes por sí mismos y requerir una serie de salvaguardas frecuentemente reguladas por ley. En estos activos interesa

9 Los lectores familiarizados con Magerit v1.0, detectarán la ausencia de la voz “vulnerabilidad”. El concepto de vulnerabilidad (potencialidad o posibilidad de ocurrencia de una amenaza sobre un activo) se incorpora por medio de las métricas de degradación del activo y frecuencia de ocurrencia de la amenaza.

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

determinar qué tratamiento hay que imponerles[11]. El hecho de que un dato sea de carácter personal impacta sobre todos los activos involucrados en su tratamiento y custodia.

Algo similar ocurre con los datos sometidos a una clasificación de confidencialidad. Cuando se dice que un cierto informe está clasificado como *"reservado",* de forma que las copias están numeradas, sólo pueden llegar a ciertas personas, no deben salir del recinto y deben ser destruidas concienzudamente, etc. se están imponiendo una serie de salvaguardas porque lo ordena el reglamento, sectorial o específico de la Organización.

Dependencias

Los activos más llamativos suelen ser los datos y los servicios; pero estos activos dependen de otros activos más prosaicos como pueden ser los equipos, las comunicaciones o las frecuentemente olvidadas personas que trabajan con aquellos. 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*[12].

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:

- capa 1: **el entorno**: activos que se precisan para garantizar las siguientes capas
    - equipamiento y suministros: energía, climatización, comunicaciones
    - personal: de dirección, de operación, de desarrollo, etc.
    - otros: edificios, mobiliario, etc.
- capa 2: **el sistema de información** propiamente dicho
    - equipos informáticos *(hardware)*
    - aplicaciones *(software)*
    - comunicaciones
    - soportes de información: discos, cintas, etc.
- capa 3: **la información**
    - datos
    - meta-datos: estructuras, índices, claves de cifra, etc.
- capa 4: **las funciones de la Organización**, que justifican la existencia del sistema de información y le dan finalidad
    - objetivos y misión
    - bienes y servicios producidos
- capa 5: **otros** activos
    - credibilidad o buena imagen

11 Es como si el legislador hubiera realizado el análisis de riesgos por nosotros y hubiera determinado las salvaguardas pertinentes. En todo caso, leyes y regulaciones existen y ayudan a que estos datos, ciertamente importantes, estén protegidos.

12 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 empresa, 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.

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

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.

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 (o datos) que el sistema maneja, quedando los demás activos subordinados a las necesidades de explotación y protección de la información. 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 datos y servicios finales 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 **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)
- 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[13].

En sistemas dedicados a la administración electrónica o al 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. En estos activos, además de la autenticidad, interesa calibrar la:

- 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 las dimensiones básicas: autenticidad, confidencialidad, integridad y disponibilidad. En esta metodología se ha refinado la autenticidad para distinguir entre el uso de un servicio y el acceso a unos datos. Además se ha introducido el concepto de trazabilidad (del inglés, *accountability*) tomado de las guías ISO/IEC 13335, igualmente segmentada entra la traza-

13 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.

bilidad del servicio y la de los datos. Los aspectos de autenticidad y trazabilidad de los datos son críticos para satisfacer medidas reglamentarias sobre ficheros que contengan datos de carácter personal.

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 salir 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

Todos estos 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.

El capítulo 8.1 de la "Guía de Técnicas" presenta un modelo de análisis basado en valoraciones cualitativas.

Valoración cuantitativa

Las valoraciones numéricas absolutas cuestan mucho esfuerzo; pero no adolecen de los problemas de las valoraciones cualitativas. Sumar valores numéricos es absolutamente "natural" y la in-

terpretación 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?

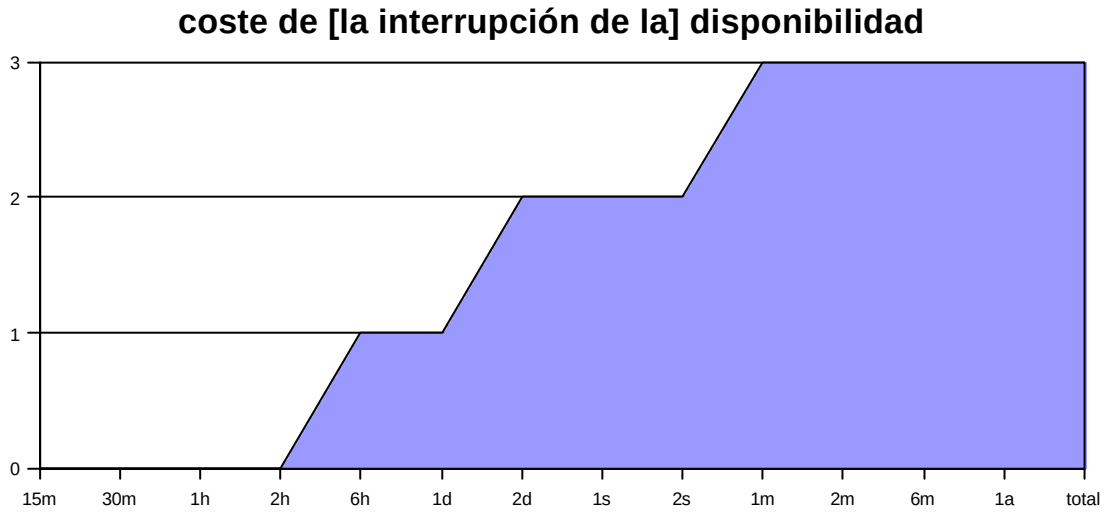
El capítulo 8.2 de la "Guía de Técnicas" presenta un modelo de análisis basado en valoraciones cuantitativas.

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:



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.

2.1.2. 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.

Hay accidentes naturales (terremotos, inundaciones, ...) y desastres industriales (contaminación, fallos eléctricos, ...) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos. Hay amenazas causadas por las personas, bien errores,

bien ataques intencionados.

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

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.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable[15] es el activo, en dos sentidos:

degradación: cuán perjudicado resultaría el activo

frecuencia: cada cuánto se materializa 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 frecuencia[16] pone en perspectiva aquella degradación, pues una amenaza puede ser de terribles consecuencias pero de muy improbable materialización; mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulando un daño considerable.

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

100	muy frecuente	a diario
10	frecuente	mensualmente
1	normal	una vez al año
1/10	poco frecuente	cada varios años

2.1.3. Paso 4: Determinación del impacto

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 de información se centre en los servicios que presta y los datos que maneja, al tiempo que las amenazas suelen materializarse en los medios.

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)

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.

15 Los lectores familiarizados con Magerit v1.0, detectarán la ausencia de la voz “vulnerabilidad”. El concepto de vulnerabilidad (potencialidad o posibilidad de ocurrencia de una amenaza sobre un activo) se incorpora por medio de las métricas de degradación del activo y frecuencia de ocurrencia de la amenaza.

16 Se mide como el número medio de ocurrencias de la amenaza en un intervalo determinado de tiempo. Típicamente estima sobre periodos anuales. Por ejemplo, si en un cierto sistema se produce una avería del aire acondicionado un promedio de cinco veces en un año, esa es la frecuencia: 5.

- las amenazas a que está expuesto

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, ni dependan de ningún 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.

2.1.4. Paso 5: Determinación del riesgo

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 frecuencia de ocurrencia.

El riesgo crece con el impacto y con la frecuencia.

Riesgo acumulado

Es el calculado sobre un activo teniendo en cuenta

- el impacto acumulado sobre un activo debido a una amenaza y
- la frecuencia 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 frecuencia 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 frecuencia 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 frecuencia 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 riesgo acumulado sobre activos que no sean dependientes entre sí, ni dependan de ningún 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.

2.1.5. 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.

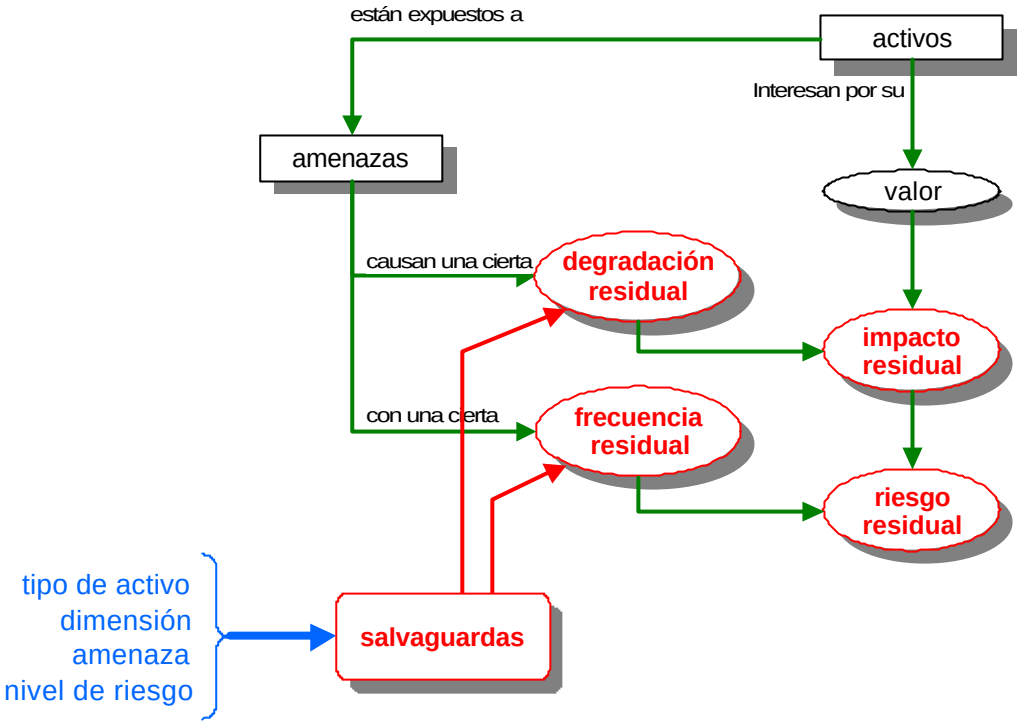
Las salvaguardas entran en el cálculo del riesgo de dos formas:

Reduciendo la frecuencia 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.



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

- es teóricamente idónea
- está perfectamente desplegada, configurada y mantenida
- se emplea siempre
- 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 están de adorno y el 100% para aquellas que son perfectas, se estimará un grado de eficacia real en cada caso concreto.

2.1.6. Revisión del paso 4: impacto residual

Si se han hecho todos los deberes a la perfección, el impacto residual debe ser despreciable.

Si hay deberes a medio hacer (normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no controlan) entonces se dice que el sistema permanece sometido a un impacto 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.

2.1.7. Revisión del paso 5: riesgo residual

Si se han hecho todos los deberes a la perfección, el riesgo residual debe ser despreciable.

Si hay deberes a medio hacer (normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no controlan) entonces se dice que el sistema permanece sometido a un riesgo 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 frecuencia de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la nueva tasa de ocurrencia.

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

La magnitud de la frecuencia 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.

2.2. Gestión de Riesgos

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, mientras que el riesgo refleja el daño probable.

Si el impacto y el riesgo residuales son despreciables, se ha terminado. Si no, hay que hacer algo.

2.2.1. La 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 despreciables. Son pues una métrica de carencias.

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.

Si el valor residual es despreciable, ya está. Esto no quiere decir descuidar la guardia; pero si afrontar el día con cierta confianza[17].

Mientras el valor residual sea más que despreciable, hay una cierta exposición.

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. Los responsables de la toma de decisiones deberán prestar cuidadosa atención a esta relación de tareas pendientes, que se denomina **Informe de Insuficiencias**.

2.2.2. Selección de salvaguardas

Las amenazas hay que conjurarlas, por principio y mientras no se justifique lo contrario.

Hay que planificar el conjunto de salvaguardas pertinentes para atajar tanto el impacto como el riesgo, reduciendo bien la degradación del activo (minimizando el daño), bien reduciendo la frecuencia de la amenaza (minimizando sus oportunidades).

Toda amenaza debe ser conjurada profesionalmente, lo que quiere decir que hay que:

1. establecer una política de la Organización al respecto; o sea, unas directrices generales de quién es responsable de cada cosa

17 Don Quijote (Capítulo X) llamaba la atención sobre el *"bálsamo de Fierabrás"* que *"es un bálsamo ... con el cual no hay que tener temor a la muerte, ni hay pensar morir de ferida alguna. "* No puede el responsable de seguridad caer en la confianza ciega pues los sistemas evolucionan, los atacantes inventan, los usuarios son impredecibles en sus errores y en definitiva siempre hay que estar atento y pronto a reaccionar ante nuevas realidades.

2. establecer una norma; o sea, unos objetivos a satisfacer para poder decir con propiedad que la amenaza ha sido conjurada
3. establecer unos procedimientos; o sea, instrucciones paso a paso de qué hay que hacer
4. desplegar salvaguardas técnicas que efectivamente se enfrenten a las amenazas con capacidad para conjurarlas
5. desplegar controles que permitan saber que todo lo anterior está funcionando según lo previsto

A este conjunto de elementos se le encasilla habitualmente bajo el nombre de Sistema de Gestión de la Seguridad de la Información (SGSI), aunque se está gestionando tanto como actuando.

El párrafo anterior puede llamar a engaño si el lector interpreta que hay que llevar a cabo todos y cada uno de los puntos para cada amenaza. No. En la práctica lo dicho se traduce en desarrollar una política, unas normas y unos procedimientos junto con el despliegue de una serie de salvaguardas y controles y, ahora sí, verificar que todas y cada una de las amenazas tienen una respuesta adecuada.

De los puntos anteriores, el más “abierto” es el de determinación de las salvaguardas apropiadas. Es realmente un arte que requiere personal especializado aunque en la práctica las situaciones más habituales están perfectamente documentadas en la literatura y basta elegir de entre un catálogo en función de la magnitud del riesgo.

Tipos de salvaguardas

Un sistema debe considerar prioritariamente las salvaguardas de tipo preventivo que buscan que la amenaza no ocurra o su daño sea despreciable. Es decir, impedir incidentes o ataques.

En la práctica, no todo es previsible, ni todo lo previsible es económicamente razonable atajarlo en sus orígenes. Tanto para enfrentar lo desconocido como para protegerse de aquello a lo que se permanece expuesto, es necesario disponer de elementos que detecten el inicio de un incidente y permitan reaccionar con presteza impidiendo que se convierta en un desastre.

Tanto las medidas preventivas como las de emergencia admiten una cierta degradación de los activos por lo que habrá que disponer por último de medidas de recuperación que devuelvan el valor perdido por los activos.

Es de sentido común intentar actuar de forma preventiva para que las cosas no puedan ocurrir o no puedan causar mucho daño; pero no siempre es posible[18] y hay que estar preparados para que ocurran. Lo que no debe ser de ninguna manera es que un ataque pase inadvertido: hay que detectarlo, registrarlo y reaccionar primero con un plan de emergencia (que pare y limite el incidente) y después con un plan de continuidad y recuperación para regresar a donde se debe estar.

Por último, sin ánimo de saturar al lector, hay que recordar que conviene llegar a un cierto equilibrio entre

salvaguardas técnicas: en aplicaciones, equipos y comunicaciones

salvaguardas físicas: protegiendo el entorno de trabajo de las personas y los equipos

medidas de organización: de prevención y gestión de las incidencias

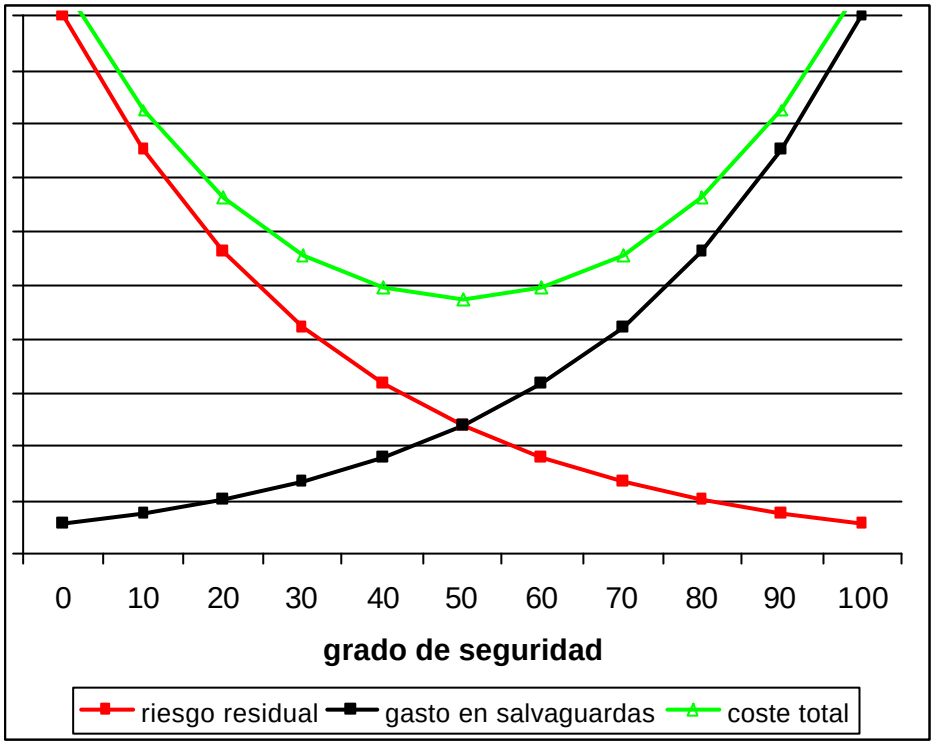
política de personal: que, a fin de cuentas, es el eslabón imprescindible y más delicado: política de contratación, formación permanente, Organización de reporte de incidencias, plan de reacción y medidas disciplinarias.

18 Hay mil razones que pueden impedir una protección absoluta: coste, dificultad técnica, límites legales, etc. No obstante, una de las razones más fuertes para no poder prevenir es el mero desconocimiento de lo que puede pasar. Podemos prever que se repita lo que ha ocurrido en el pasado; pero es difícil prever el próximo ataque intencionado pues hay un componente creativo de parte del atacante.

2.2.3. Pérdidas y ganancias

Es de sentido común que no se puede invertir en salvaguardas más allá del valor de los propios activos a 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.



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[19] y que el coste de las inversiones se dispare para alcanzar niveles de seguridad cercanos al 100%[20]. 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 inverte 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 (no hacer nada) 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 po-

19 Medidas básicas de seguridad suponen un importante descenso del riesgo. Por ello son inexcusables.
20 Reflejando una vez más que la seguridad absoluta (riesgo cero) no existe.

sitivos las entradas de dinero. Considerando los siguientes componentes:

(recurrente) riesgo residual[21]

(una vez) coste de las salvaguardas[22]

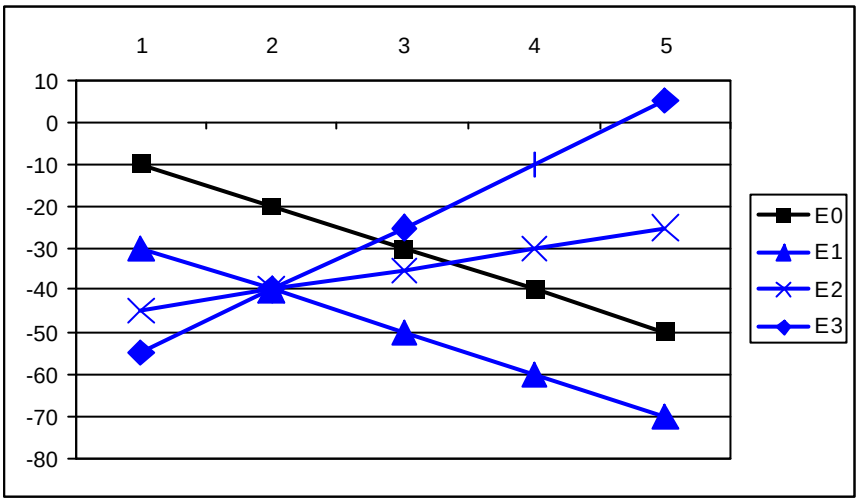
(recurrente) coste anual de mantenimiento de las salvaguardas

\+ (recurrente) mejora en la productividad[23]

\+ (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[24]:



- 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 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.

22 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.

23 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.

24 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.

2.2.4. La actitud de la Dirección

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[25].

Si el impacto y/o el riesgo están por encima de lo aceptable, se puede:

1. eliminar el activo; suena muy fuerte, pero a veces hay activos que, simplemente, no vale la pena mantener[26]
2. introducir nuevas salvaguardas o mejorar la eficacia de las presentes

2.2.5. Revisión del paso 1: activos

Algunas salvaguardas, notablemente las de tipo técnico, se traducen en el despliegue de más equipamiento[27] que se convierte a su vez en un activo del sistema. Estos activos soportan parte del valor del sistema y están a su vez sujetos a amenazas que pueden perjudicar a los activos de valor.

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.

25 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.

26 ¿Necesita realmente mantener este dato de carácter personal y nivel alto? ¿Es realmente necesaria la red inalámbrica en la oficina?

27 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.

3. Estructuración del proyecto

Si en el capítulo anterior se ha marcado de forma conceptual cómo llevar a cabo un análisis y una gestión de riesgos, en este capitulo se plasman aquellos conceptos en componentes de un proyecto de análisis y gestión de riesgos (AGR)[28]. Los pasos se organizan en tres grandes procesos (preparación, análisis y gestión). Cada proceso se organiza en actividades que, finalmente, se estructuran en tareas a realizar. En cada tarea se indica lo que hay que hacer así como las posibles dificultades para conseguirlo y la forma de afrontarla con éxito[29]. En cada proceso se indican los hitos que van marcando el progreso del proyecto hasta su terminación.

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, todo tipo de situaciones, en definitiva. 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 recogen formalmente en las tareas de la actividad A1.2 e informalmente comentando que es constructivo centrarse en un dominio reducido e ir ampliando en la medida de las necesidades, antes que afrontar la totalidad.

Además de cubrir un dominio más o menos extenso, pueden darse con 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 (actividad A1.2)
2. verticalmente a la profundidad oportuna

28 Corresponde al "Modelo de procesos" de Magerit versión 1.0.
29 En el capítulo 6 se incluyen consejos prácticos adicionales.

3.1. Participantes

Durante el desarrollo del proyecto AGR, desde su inicio a su terminación, se identifican los siguientes órganos colegiados[30]:

Comité de Dirección

El perfil requerido para este grupo de participantes incluye a personas con un nivel alto en la dirección de la Organización, conocimiento de los objetivos estratégicos y de negocio que se persiguen y autoridad para validar y aprobar cada uno de los procesos realizados durante el desarrollo del proyecto.

Las responsabilidades de este comité consisten en

- asignar los recursos necesarios para la ejecución del proyecto
- aprobar los resultados finales de cada proceso

El comité de dirección formaliza sus funciones en la tarea T1.3.2.

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

El comité de seguimiento de crea en la tarea T1.1.1 y sus funciones se formalizan en T1.3.2..

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 se determina en la tarea T1.3.2.

Grupos de Interlocutores

Está formado por usuarios representativos dentro de las unidades afectadas por el proyecto.

30 Es importante formalizar los roles de los participantes en el proyecto. En esta sección se identifican dichos roles y se les da un nombre estándar. Más adelante se detalla en qué momento (tarea) del proyecto se constituyen formalmente.

Lo constituyen varios posibles subgrupos:

- Responsables de servicio, consciente 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

Las unidades afectadas se determinan en las tareas T1.2.2 y T1.2.3. Los interlocutores de identifican en la tarea T1.3.1.

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 AGR 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.

El promotor tiene su papel en la tarea T1.1.1.

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.

El director del proyecto se designa en la tarea T1.2.2.

Enlace operacional

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

Es el interlocutor visible del comité de seguimiento.

El enlace operacional se designa en la tarea T1.3.2.

Conviene recordar que un proyecto AGR 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.

3.2. Desarrollo del proyecto

En esta sección se ordenan y formalizan las acciones a realizar a lo largo de un proyecto AGR, estableciendo un marco normalizado de desarrollo. Este marco de trabajo define:

1. una estructuración del proyecto que sirve de guía al equipo de trabajo y que permite involucrar en aquél a los responsables y a los usuarios.
2. un conjunto de productos a obtener
3. un conjunto de técnicas para obtener los productos
4. las funciones y responsabilidades de los distintos participantes

El proyecto se divide en tres grandes procesos, desglosándose cada uno en una serie de activi-

dades y estas, a su vez, en tareas con el grado de detalle oportuno.

Cada tarea especifica los siguientes conceptos:

- acciones a realizar
- datos de entrada
- datos de salida: productos y documentos a obtener como producto de las acciones
- técnicas recomendadas para llevar a buen término los objetivos de la tarea
- participantes que intervienen o están afectados por la cumplimentación de las acciones

Un proyecto AGR conlleva tres procesos:

Proceso P1: Planificación

- Se establecen las consideraciones necesarias para arrancar el proyecto AGR.
- Se investiga la oportunidad de realizarlo.
- Se definen los objetivos que ha de cumplir y el dominio (ámbito) que abarcará.
- Se planifican los medios materiales y humanos para su realización.
- Se procede al lanzamiento del proyecto.

Proceso P2: Análisis de riesgos

- Se identifican los activos a tratar, las relaciones entre ellos y la valoración que merecen.
- Se identifican las amenazas significativas sobre aquellos activos y se valoran en términos de frecuencia de ocurrencia y degradación que causan sobre el valor del activo afectado.
- Se identifican las salvaguardas existentes y se valora la eficacia de su implantación.
- Se estima el impacto y el riesgo al que están expuestos los activos del sistema.
- Se interpreta el significado del impacto y el riesgo.

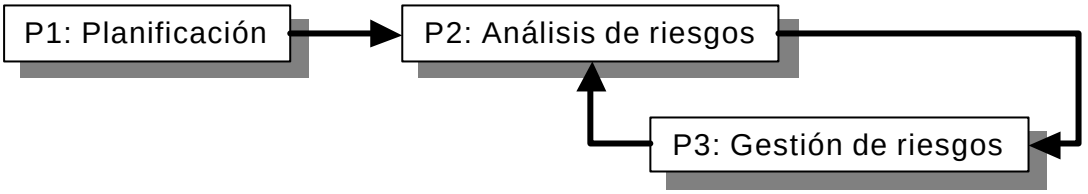
Proceso P3: Gestión de riesgos

- Se elige una estrategia para mitigar impacto y riesgo.
- Se determinan las salvaguardas oportunas para el objetivo anterior.
- Se determina la calidad necesaria para dichas salvaguardas.
- Se diseña un plan de seguridad (plan de acción o plan director) para llevar el impacto y el riesgo a niveles aceptables.
- Se lleva a cabo el plan de seguridad.

Estos tres procesos no son necesariamente secuenciales. El proceso P1 es claramente el iniciador del proyecto. El proceso P2 funciona como soporte del proceso P3 en el sentido de que la gestión de riesgos (P3) es una tarea continua soportada por los técnicas de análisis (P2). La gestión de riesgos supone siempre la alteración del conjunto de salvaguardas, bien porque aparecen nuevas salvaguardas, bien porque se reemplazan unas por otras, bien porque se mejoran las existentes. La gestión de riesgos puede suponer la alteración del conjunto de activos[31], bien porque

31 Formalmente se dice que la introducción de salvaguardas para mitigar ciertos riesgos puede introducir

aparecen nuevos activos (elementos de salvaguarda que pasan a formar parte del sistema) o porque se eliminan activos del sistema. En definitiva, a lo largo del proceso P3 se recurrirá a tareas del proceso P2.



A lo largo de estos procesos se generan una serie de documentos de interés general[32]:

P1: Planificación

- Tipología de activos
- Dimensiones de seguridad relevantes
- Criterios de evaluación

P2: Análisis de riesgos

- Modelo de valor
- Mapa de riesgos
- Evaluación de salvaguardas
- Estado de riesgo
- Informe de insuficiencias

P3: Gestión de riesgos

- Plan de seguridad

nuevos riesgos en el sistema.

32 Sin entrar en documentos de trabajo del propio proyecto AGR, que se detallan en las tareas.

3.2.1. Visión global

Sin perjuicio de una exposición detallada más adelante, se relaciona a continuación el árbol completo de procesos, actividades y tareas que vertebran un proyecto AGR.

Procesos, actividades y tareas
Proceso P1: Planificación Actividad A1.1: Estudio de oportunidad Tarea T1.1.1: Determinar la oportunidad Actividad A1.2: Determinación del alcance del proyecto Tarea T1.2.1: Objetivos y restricciones generales Tarea T1.2.2: Determinación del dominio y límites Tarea T1.2.3: Identificación del entorno Tarea T1.2.4: Estimación de dimensiones y coste Actividad A1.3: Planificación del proyecto Tarea T1.3.1: Evaluar cargas y planificar entrevistas Tarea T1.3.2: Organizar a los participantes Tarea T1.3.3: Planificar el trabajo Actividad A1.4: Lanzamiento del proyecto Tarea T1.4.1: Adaptar los cuestionarios Tarea T1.4.2: Criterios de evaluación Tarea T1.4.3: Recursos necesarios Tarea T1.4.4: Sensibilización
Proceso P2: Análisis de riesgos Actividad A2.1: Caracterización de los activos Tarea T2.1.1: Identificación de los activos Tarea T2.1.2: Dependencias entre activos Tarea T2.1.3: Valoración de los activos Actividad A2.2: Caracterización de las amenazas Tarea T2.2.1: Identificación de las amenazas Tarea T2.2.2: Valoración de las amenazas Actividad A2.3: Caracterización de las salvaguardas Tarea T2.3.1: Identificación de las salvaguardas existentes Tarea T2.3.2: Valoración de las salvaguardas existentes Actividad A2.4: Estimación del estado de riesgo Tarea T2.4.1: Estimación del impacto Tarea 2.4.2: Estimación del riesgo Tarea 2.4.3: Interpretación de los resultados
Proceso P3: Gestión de riesgos Actividad A3.1: Toma de decisiones Tarea A3.1.1: Calificación de los riesgos Actividad A3.2: Plan de seguridad Tarea T3.2.1: Programas de seguridad Tarea T3.2.2: Plan de ejecución Actividad A3.3: Ejecución del plan Tarea T3.3.*: Ejecución de cada programa de seguridad

3.3. Proceso P1: Planificación

El objetivo principal de este proceso es establecer el marco general de referencia para todo el proyecto.

Como objetivos complementarios se pueden identificar los siguientes:

- Motivar, concienciar e involucrar a la Dirección o Gerencia de la Organización.
- Razonar la oportunidad de realizar un proyecto AGR.
- Afirmar y dar a conocer la voluntad de su realización por parte de la Dirección.
- Crear las condiciones humanas y materiales para el buen desarrollo del proyecto.

Este proceso se desarrolla por medio de las siguientes actividades y tareas:

Actividad A1.1: Estudio de oportunidad

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

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

Tareas:

Tarea T1.1.1: Determinar la oportunidad

Actividad A1.2: Determinación del alcance del proyecto

Se definen los objetivos finales del proyecto, su dominio y sus límites. Se realiza una primera identificación del entorno y de las restricciones generales a considerar. Y por último se estima el coste que va a suponer.

El resultado de esta actividad es un perfil de proyecto AGR.

Tareas:

Tarea T1.2.1: Objetivos y restricciones generales

Tarea T1.2.2: Determinación del dominio y límites

Tarea T1.2.3: Identificación del entorno

Tarea T1.2.4: Estimación de dimensiones y coste

Actividad A1.3: Planificación del proyecto

Se determina las carga de trabajo que supone la realización del proyecto. 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 AGR
- procedimientos de gestión de la información generada

Tareas:

Tarea T1.3.1: Evaluar cargas y planificar entrevistas

Tarea T1.3.2: Organizar a los participantes

Tarea T1.3.3: Planificar el trabajo

Actividad A1.4: Lanzamiento del proyecto

Se adaptan los cuestionarios para la recogida de información adaptándolos al proyecto presente. Se eligen las técnicas principales de evaluación de riesgo a utilizar y se asignan los recursos necesarios para el comienzo del proyecto. 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 plan de entrevistas
- el catálogo de tipos de activos
- la relación de dimensiones de seguridad y
- los criterios de valoración

Tareas:

Tarea T1.4.1: Adaptar los cuestionarios

Tarea T1.4.2: Criterios de evaluación

Tarea T1.4.3: Recursos necesarios

Tarea T1.4.4: Sensibilización

3.3.1. Actividad A1.1: Estudio de oportunidad

Consta de una única tarea:

T1.1.1: Determinar la oportunidad

P1: Planificación ***A1.1: Estudio de oportunidad*** ***T1.1.1: Determinar la oportunidad***
Objetivos • Identificar o suscitar el interés de la Dirección de la Organización en la realización de un proyecto AGR
Productos de entrada
Productos de salida • **Informe preliminar** recomendando la elaboración del proyecto AGR • Sensibilización y apoyo de la Dirección a la realización del proyecto AGR • Creación del comité de seguimiento
Técnicas, prácticas y pautas • Entrevistas (ver "Guía de Técnicas" 3.6.1) • Reuniones (ver "Guía de Técnicas" 3.6.2)
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 AGR 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 sis-

temas 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 AGR[33]. 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.

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 AGR 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 AGR.

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.

33 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 un proyecto AGR.

3.3.2. Actividad A1.2: Determinación del alcance del proyecto

Una vez que se ha constatado la oportunidad de realizar el proyecto AGR y el apoyo por 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 AGR. 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.

Esta actividad consta de cuatro tareas:

T1.2.1: Objetivos y restricciones generales

T1.2.2: Determinación del dominio y límites

T1.2.3: Identificación del entorno

T1.2.4: Estimación de dimensiones y coste

P1: Planificación ***A1.2: Determinación del alcance del proyecto*** ***T1.2.1: Objetivos y restricciones generales***
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
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
Técnicas, prácticas y pautas • Entrevistas (ver "Guía de Técnicas" 3.6.1) • Reuniones (ver "Guía de Técnicas" 3.6.2)
Participantes • El comité de seguimiento

Un proyecto AGR 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

P1: Planificación ***A1.2: Determinación del alcance del proyecto*** ***T1.2.2: Determinación del dominio y límites***
Objetivos • Determinar el dominio, alcance o perímetro del proyecto AGR
Productos de entrada • Resultados de la tarea T1.2.1, Objetivos y restricciones generales • Perfil general de las unidades incluidas en el dominio del proyecto
Productos de salida • Relación de unidades de la Organización que se verán afectadas como parte del dominio del proyecto • Lista de roles relevantes en la unidades incluidas en el dominio • Designación del director del proyecto
Técnicas, prácticas y pautas • Diagramas de procesos (ver "Guía de Técnicas" 3.3)
Participantes • Responsables de las unidades de la Organización • El comité de seguimiento

Esta tarea identifica las unidades objeto del proyecto AGR 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.

P1: Planificación
A1.2: Determinación del alcance del proyecto
T1.2.3: Identificación del entorno

Objetivos

- Definir el perímetro del dominio
- Definir las relaciones entre el interior del dominio y el entorno

Productos de entrada

- Resultados de la tarea T1.2.1, Objetivos y restricciones generales
- Resultados de la tarea T1.2.2, Determinación del dominio y límites
- Esquema de las relaciones de las unidades del dominio con el entorno
- Diagramas de flujo de datos

Productos de salida

- Relación de unidades de la Organización que se verán afectadas como perímetro del dominio
- Lista de roles relevantes en otras unidades, a considerar para la caracterización del entorno

Técnicas, prácticas y pautas

- Diagramas de flujo de datos (ver "Guía de Técnicas" 3.2)
- Diagramas de procesos (ver "Guía de Técnicas" 3.3)
- Entrevistas (ver "Guía de Técnicas" 3.6.1)
- Reuniones (ver "Guía de Técnicas" 3.6.2)

Participantes

- Responsables de las unidades incluidas en el dominio
- El comité de seguimiento

Esta tarea realiza un estudio global de los sistemas de información de las unidades incluidas en el dominio del proyecto, con objeto de identificar sus funciones y finalidades principales y sus relaciones con el entorno, así como sus tendencias de evolución. El perfil general de las unidades, producto obtenido en la tarea anterior, se amplia en ésta con la información proporcionada por los responsables de las diversas áreas de dichas unidades.

P1: Planificación ***A1.2: Determinación del alcance del proyecto*** ***T1.2.4: Estimación de dimensiones y coste***
Objetivos • Determinar el volumen de recursos necesarios para la ejecución del proyecto AGR: humanos, temporales y financieros
Productos de entrada • Resultados de la tarea T1.2.1, Objetivos y restricciones generales • Resultados de la tarea T1.2.2, Determinación del dominio y límites • Resultados de la tarea T1.2.3, Identificación del entorno
Productos de salida • Dimensión del proyecto • Costes y beneficios del proyecto
Técnicas, prácticas y pautas • Análisis coste-beneficio (ver "Guía de Técnicas" 3.1) • Planificación de proyectos (ver "Guía de Técnicas" 3.5)
Participantes • El director de proyecto

La tarea posibilita el dimensionamiento (tamaño, complejidad, zonas de incertidumbre) del proyecto a partir del conocimiento de los objetivos del proyecto, del dominio y del perfil de las unidades incluidas en el estudio. En función de la dimensión estimada y de los objetivos del proyecto se escogen algunas de las técnicas a utilizar en el proyecto. Por ejemplo, si el proyecto tiene como objetivo la realización de un análisis inicial genérico, la técnica de cálculo del riesgo se orienta a una discriminación dicotómica (en dos bloques) de los riesgos, según que exijan o no otras aplicaciones más detalladas de análisis.

Por otra parte la tarea también dimensiona el proyecto en cuanto a su coste y los retornos o beneficios que puede aportar, para que la Dirección pueda tomar con fundamento la decisión de emprenderlo y asignar los recursos necesarios para su desarrollo.

- El estudio del coste del proyecto se realiza estimando los tiempos y perfiles de personal asignado a las etapas del proyecto dimensionado anteriormente.
- El estudio de los retornos sólo puede ser muy impreciso en este proceso inicial, pues no puede tener en cuenta aún el verdadero retorno de un proyecto de seguridad, que es precisamente el coste de no tener dicha seguridad en el dominio estudiado o sea el resultado del propio proyecto AGR.

3.3.3. Actividad A1.3: Planificación del proyecto

En esta actividad se determinan los participantes en el proyecto, determinando sus cargas de trabajo, su estructuración en grupos y su modo de actuación.

Esta actividad consta de tres tareas:

T1.3.1: Evaluar cargas y planificar entrevistas

T1.3.2: Organizar a los participantes

T1.3.3: Planificar el trabajo

P1: Planificación ***A1.3: Planificación del proyecto*** ***T1.3.1: Evaluar cargas y planificar entrevistas***
Objetivos • Definir los grupos de interlocutores: usuarios afectados en cada unidad • Planificar las entrevistas de recogida de información
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 cargas
Técnicas, prácticas y pautas • Planificación de proyectos (ver "Guía de Técnicas" 3.5)
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.

P1: Planificación
A1.3: Planificación del proyecto
T1.3.2: Organizar a los participantes

Objetivos

- Determinar los órganos participantes en la gestión, realización, seguimiento y mantenimiento del proyecto
- Definir las funciones y responsabilidades de los órganos participantes
- Establecer las reglas y los modos operativos
- Establecer la clasificación de la información generada

Productos de entrada

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

Productos de salida

- Formalización del comité de dirección
- Formalización del comité de seguimiento
- Criterios y procedimientos de clasificación y gestión de la información generada
- Designación del enlace operacional
- Creación del equipo de trabajo

Técnicas, prácticas y pautas

No aplica

Participantes

- Comité de seguimiento
- Director del proyecto

Aunque todos los proyectos AGR involucran básicamente a los mismos comités, en esta tarea se concreta la aproximación genérica al caso particular, pudiendo atenerse al caso general, o particularizar.

Es particularmente relevante determinar la clasificación de los documentos que se produzcan a lo largo del proyecto. Si existe una norma de clasificación, conviene atenerse a ella para aprovechar procedimientos ya establecidos de tratamiento de los documentos. Si no existiera, es necesario elaborar tanto los criterios de clasificación como los procedimientos de tratamiento. La calificación defecto será “confidencial”, siendo particularmente importante preservar la confidencialidad de los documentos de evaluación de salvaguardas y de insuficiencias.

P1: Planificación
A1.3: Planificación del proyecto
T1.3.3: Planificar el trabajo

Objetivos

- 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
- Resultados de la tarea T1.3.1, Evaluar cargas y planificar entrevistas
- Resultados de la tarea T1.3.2, Organizar a los participantes

Productos de salida

- Cronograma del proyecto
- Dedicaciones de los participantes
- Especificación de los recursos materiales necesarios
- Descripción de hitos

Técnicas, prácticas y pautas

- Planificación de proyectos (ver "Guía de Técnicas" 3.5)

Participantes

- El equipo de proyecto

3.3.4. Actividad A1.4: 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, así como especificar los criterios y las técnicas concretas a emplear; y terminando por asignar los recursos necesarios para la realización del proyecto y por realizar la campaña informativa de sensibilización a los implicados.

Esta actividad consta de cuatro tareas:

T1.4.1: Adaptar los cuestionarios

T1.4.2: Criterios de evaluación

T1.4.3: Recursos necesarios

T1.4.4: Sensibilización

P1: Planificación ***A1.4: Lanzamiento del proyecto*** ***T1.4.1: Adaptar los cuestionarios***
Objetivos • Identificar la información relevante a obtener, agrupada de acuerdo a la estructura de unidades y roles de los participantes
Productos de entrada • Resultados de la actividad A1.3, Planificación del proyecto
Productos de salida • Cuestionarios adaptados
Técnicas, prácticas y pautas • Cuestionarios (ver "Catálogo de Elementos" en general y el apéndice 2 en particular)
Participantes • 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.

P1: Planificación
A1.4: Lanzamiento del proyecto
T1.4.2: Criterios de evaluación

Objetivos

- 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

Productos de entrada

- Catálogo de elementos
- Resultados de la actividad A1.3, Planificación del proyecto

Productos de salida

- Catálogo de tipos de activos
- Relación de dimensiones de seguridad
- Criterios de valoración

Técnicas, prácticas y pautas

- Ver "Catálogo de Elementos" capítulos 2, 3 y 4

Participantes

- El equipo de proyecto

Esta tarea, preparatoria del proceso P2 (análisis de riesgos), establece la selección de los criterios y técnicas que se mantendrán a lo largo de todo el proceso. En efecto, la gestión de los riesgos del proceso P3 estará condicionada por el tipo de análisis realizado en el proceso P2: si se han elegido un tipo de criterios y técnicas para evaluar los riesgos, es recomendable aplicar las mismas técnicas para evaluar la reducción de riesgos al implantar las salvaguardas propuestas. La elección de estos criterios y técnicas en función de:

- los objetivos del proyecto (T1.2.1)
- el dominio del proyecto (T1.2.2)

Se recomienda atenerse a lo propuesto en el libro “Catálogo de Elementos” anejo a esta guía.

P1: Planificación
A1.4: Lanzamiento del proyecto
T1.4.3: Recursos necesarios

Objetivos

- Asignar los recursos necesarios (humanos, de organización, técnicos, etc.) para la realización del proyecto AGR

Productos de entrada

- Resultados de la actividad A1.3, Planificación del proyecto

Productos de salida

- Comunicaciones al personal participante de su asignación al proyecto
- Disponibilidad de los medios materiales necesarios

Técnicas, prácticas y pautas

- Planificación de proyectos (ver "Guía de Técnicas" 3.5)

Participantes

- El comité de seguimiento

P1: Planificación ***A1.4: Lanzamiento del proyecto*** ***T1.4.4: Sensibilización***
Objetivos • Informar a las unidades afectadas • Crear un ambiente de conocimiento general de los objetivos, responsables y plazos
Productos de entrada • Resultados de la actividad A1.3, Planificación del proyecto
Productos de salida • Nota informativa de la dirección • Material e informe de presentación del proyecto
Técnicas, prácticas y pautas • Presentaciones (ver "Guía de Técnicas" 3.6.3)
Participantes • El director del proyecto • El comité de seguimiento • El enlace operacional • El equipo de proyecto

Esta tarea informa a las unidades afectadas del lanzamiento del proyecto AGR, por diversos medios, y como mínimo:

- Una nota informativa de la Dirección, dirigida a las unidades implicadas y declarando su apoyo a la realización del proyecto.
- La presentación del proyecto, sus objetivos y la metodología a emplear, realizada en las unidades implicadas por parte del equipo de proyecto.

3.3.5. Síntesis del proceso P1

3.3.5.1. Hitos de control

Hito de control H1.1:

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

Hito de control H1.2:

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

3.3.5.2. Resultados

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

- Tipología de activos
- Dimensiones de seguridad relevantes
- Criterios de evaluación
- Informe de "Planificación del Proyecto de Análisis y Gestión de riesgos" que contendrá una síntesis de los productos obtenidos en las actividades realizadas en proceso

3.3.6. Lista de control[34] del proceso P1

Organización del proyecto:

- √ Aprobación de la Dirección (P1)
- √ Compromiso explícito de la Dirección (P1)
- √ Apoyo de la Dirección (P1)
- √ Comité de seguimiento (T1.3.2)
- √ Equipo de proyecto (T1.3.2)

34 Esta lista permite comprobar que se han alcanzado todos los objetivos, subobjetivos y productos de salida detallados en las diferentes tareas.

- √ Director de proyecto (T1.2.2)
- √ Enlace operacional (T1.3.2)
- √ Grupos de interlocutores (T1.3.1)
- √ Funciones y método de trabajo (T1.3.2)
- √ Criterios de clasificación de la documentación y procedimientos para tratarla (T1.3.2)

Planificación del proyecto:

- √ Informe preliminar recomendando y justificando la oportunidad de lanzar un proyecto AGR (T1.1.1)
- √ Objetivos expresos y no ambiguos (T1.2.1)
- √ Estimación de dimensiones y coste (T1.2.4)
- √ Plan de entrevistas: personas y fechas (T1.4.3)
- √ Plan de trabajo: hitos (T1.3.3)
- √ Asignación de recursos (T1.4.3)
- √ Sensibilización de la Organización (T1.4.4)
- √ Plan de Proyecto de Análisis y Gestión de Riesgos (P1)

Aspectos técnicos:

- √ Limitaciones generales del proyecto (T1.2.1)
- √ Dominio del proyecto: unidades incluidas en el análisis (T1.2.2)
- √ Entorno del proyecto: otras unidades relacionadas de alguna forma (T1.2.3)
- √ Cuestionarios adaptados (T1.4.1)
- √ Catálogo de tipos de activos (T1.4.2)
- √ Relación de dimensiones de seguridad relevantes (T1.4.2)
- √ Criterios de evaluación (T1.4.2)

3.4. Proceso P2: Análisis de riesgos

Este proceso es el núcleo central de Magerit y su correcta aplicación condiciona la validez y utilidad de todo el proyecto. La identificación y estimación de los activos y de las posibles amenazas que les acechan representa una tarea compleja.

Este proceso 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 implementadas si se trata de un sistema actual, no de un sistema previsto).
- Evaluar el riesgo del sistema en estudio, tanto el riesgo potencial (sin salvaguardas), como el riesgo residual (incluyendo el efecto de las salvaguardas implementadas si se trata de un sistema actual, no de un sistema previsto).
- Mostrar al comité director las áreas del sistema con mayor impacto y/o riesgo.

El punto de partida de este proceso es la documentación del anterior referente a los objetivos del proyecto, los planes de entrevistas, la evaluación de cargas, la composición y reglas de actuación del equipo de participantes, el plan de trabajo y el informe de presentación del proyecto.

Este proceso se desarrolla por medio de las siguientes actividades y tareas:

Actividad 2.1: 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”.

Tareas:

Tarea T2.1.1: Identificación de los activos

Tarea T2.2.2: Dependencias entre activos

Tarea T2.3.3: Valoración de los activos

Actividad 2.2: Caracterización de las amenazas

Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por la frecuencia estimada de ocurrencia y la estimación de daño (degradación) que causarían sobre los activos.

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

Tareas:

Tarea T2.2.1: Identificación de las amenazas

Tarea T2.2.2: Valoración de las amenazas

Actividad 2.3: Caracterización de las salvaguardas

Esta actividad busca identificar las salvaguardas desplegadas en el sistema a analizar, cali-

ficándolas por su eficacia frente a las amenazas que pretenden mitigar.

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

Tareas:

Tarea T2.3.1: Identificación de las salvaguardas existentes

Tarea T2.3.2: Valoración de las salvaguardas existentes

Actividad 2.4: 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

Tareas:

Tarea T2.4.1: Estimación del impacto

Tarea T2.4.2: Estimación del riesgo

Tarea T2.4.3: Interpretación de los resultados

3.4.1. Actividad A2.1: Caracterización de los activos

Esta actividad consta de tres tareas:

T2.1.1: Identificación de los activos

T2.1.2: Dependencias entre activos

T2.1.3: Valoración de los activos

El objetivo de estas tareas es reconocer los activos que componen los procesos, y definir las dependencias entre ellos. Así y a partir de la información recopilada en la actividad anterior, esta actividad profundiza el estudio de las activos con vistas a obtener la información necesaria para realizar las estimaciones de riesgo.

Es frecuente que las tareas relacionadas con los activos se realicen concurrentemente con las tareas relacionadas con las amenazas sobre dichos activos (A2.2) e identificación de las salvaguardas actuales (A2.3), 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.

P2: Análisis de riesgos ***A2.1: Caracterización de los activos*** ***T2.1.1: Identificación de los activos***
Objetivos • Identificar los activos que componen el dominio, determinando sus características, atributos y clasificación en los tipos determinados
Productos de entrada • Inventarios de datos manejados por la Organización • Procesos de negocio • Diagramas de uso • Diagramas de flujo de datos • Inventarios de equipamiento lógico • Inventarios de equipamiento físico • Caracterización funcional de los puestos de trabajo • Locales y sedes de la Organización
Productos de salida • Relación de activos a considerar • Caracterización de los activos
Técnicas, prácticas y pautas • Diagramas de flujo de datos (ver "Guía de Técnicas" 3.2) • Diagramas de procesos (ver "Guía de Técnicas" 3.3) • Entrevistas (ver "Guía de Técnicas" 3.6.1) • Reuniones (ver "Guía de Técnicas" 3.6.2) • Ver también la sección 2.1.1.
Participantes • El equipo de proyecto • Los grupos de interlocutores

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

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

P2: Análisis de riesgos
A2.1: Caracterización de los activos
T2.1.2: 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 (ver "Guía de Técnicas" 3.2)
- Diagramas de procesos (ver "Guía de Técnicas" 3.3)
- Entrevistas (ver "Guía de Técnicas" 3.6.1)
- Reuniones (ver "Guía de Técnicas" 3.6.2)
- Valoración Delphi (ver "Guía de Técnicas" 3.7)
- Ver también la sección 2.1.1.

Participantes

- El equipo de proyecto
- Los grupos de interlocutores

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

P2: Análisis de riesgos
A2.1: Caracterización de los activos
T2.1.3: 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 T1.4.2, Criterios de evaluación
- Resultados de la tarea T2.1.1, Identificación de los activos
- Resultados de la tarea T2.1.2, Dependencias entre activos

Productos de salida

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

Técnicas, prácticas y pautas

- Entrevistas (ver "Guía de Técnicas" 3.6.1)
- Reuniones (ver "Guía de Técnicas" 3.6.2)
- Valoración Delphi (ver "Guía de Técnicas" 3.7)
- Ver también la sección 2.1.1.

Participantes

- El equipo de proyecto
- Los grupos de interlocutores
- El comité de seguimiento
- La dirección

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 servicios, que conocen las consecuencias de la no prestación del servicio o de su prestación degradada
- responsables de los datos, que conocen las consecuencias de la degradación de los datos
- 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

3.4.2. Actividad A2.2: Caracterización de las amenazas

Esta actividad suele discurrir de forma concurrente con las actividades A2.1 y A.2.3 dado que los responsables a entrevistar son los mismos.

Esta actividad consta de dos tareas:

T2.2.1: Identificación de las amenazas

T2.2.2: Valoración de las amenazas

P2: Análisis de riesgos ***A2.2: Caracterización de las amenazas*** ***T2.2.1: Identificación de las amenazas***
Objetivos • Identificar las amenazas relevantes sobre cada activo
Productos de entrada • Resultados de la tarea T1.4.2, Criterios de evaluación • Resultados de la actividad A2.1, Caracterización de los activos
Productos de salida • Relación de amenazas posibles
Técnicas, prácticas y pautas • Catálogos de amenazas (ver "Catálogo de Elementos", capítulo 5) • Árboles de ataque (ver "Guía de Técnicas" 2.3) • Entrevistas (ver "Guía de Técnicas" 3.6.1) • Reuniones (ver "Guía de Técnicas" 3.6.2) • Valoración Delphi (ver "Guía de Técnicas" 3.7) • Ver también la sección 2.1.2.
Participantes • El equipo de proyecto • los grupos de interlocutores

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

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

P2: Análisis de riesgos
A2.2: Caracterización de las amenazas
T2.2.2: 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 T1.4.2, Criterios de evaluación
- Resultados de la tarea T2.2.1, Identificación de las amenazas
- Series históricas de incidentes
- 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" 2.3)
- Entrevistas (ver "Guía de Técnicas" 3.6.1)
- Reuniones (ver "Guía de Técnicas" 3.6.2)
- Valoración Delphi (ver "Guía de Técnicas" 3.7)
- Ver también la sección 2.1.2.

Participantes

- El equipo de proyecto
- Los grupos de interlocutores

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

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

3.4.3. Actividad A2.3: Caracterización de las salvaguardas

Esta actividad suele discurrir de forma concurrente con las actividades A2.1 y A2.2 dado que los responsables a entrevistar son los mismos.

Esta actividad consta de dos tareas:

T2.3.1: Identificación de las salvaguardas existentes

T2.3.2: Valoración de las salvaguardas existentes

P2: Análisis de riesgos ***A2.3: Caracterización de las salvaguardas*** ***T2.3.1: Identificación de las salvaguardas existentes***
Objetivos • Identificar las salvaguardas, de cualquier tipo, que se han previsto y desplegado a fecha de realización del estudio
Productos de entrada • Inventario de procedimientos operativos • Inventario de productos y/o desarrollos *hardware* o *software* de soporte a la seguridad de los sistemas • Plan de formación • Definición de los puestos laborales • Contratos • Acuerdos de externalización de servicios
Productos de salida • Relación de salvaguardas desplegadas
Técnicas, prácticas y pautas • Catálogos de salvaguardas (ver "Catálogo de Elementos" capítulo 6) • Árboles de ataque (ver "Guía de Técnicas" 2.3) • Entrevistas (ver "Guía de Técnicas" 3.6.1) • Reuniones (ver "Guía de Técnicas" 3.6.2) • Ver también la sección 2.1.5.
Participantes • El equipo de proyecto • Los grupos de interlocutores

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

P2: Análisis de riesgos
A2.3: Caracterización de las salvaguardas
T2.3.2: Valoración de las salvaguardas existentes

Objetivos

- Determinar la eficacia de las salvaguardas desplegadas

Productos de entrada

- Inventario de salvaguardas (Catálogo de Elementos)

Productos de salida

- **Evaluación de salvaguardas**: informe de salvaguardas desplegadas, caracterizadas por su grado de efectividad

Técnicas, prácticas y pautas

- Entrevistas (ver "Guía de Técnicas" 3.6.1)
- Reuniones (ver "Guía de Técnicas" 3.6.2)
- Valoración Delphi (ver "Guía de Técnicas" 3.7)
- Ver también la sección 2.1.5.

Participantes

- El equipo de proyecto
- Los grupos de interlocutores
- Especialistas en salvaguardas concretas

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

3.4.4. Actividad A2.4: Estimación del estado de riesgo

En esta actividad se combinan los descubrimientos de las actividades anteriores (A2.1, A2.2 y A2.3) para derivar estimaciones del estado de riesgo de la Organización.

Esta actividad consta de tres tareas:

T2.4.1: Estimación del impacto

T2.4.2: Estimación del riesgo

T2.4.3: Interpretación de los resultados

P2: Análisis de riesgos ***A2.4: Estimación del estado de riesgo*** ***T2.4.1: 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 A2.1, Caracterización de los activos • Resultados de la actividad A2.2, Caracterización de las amenazas • Resultados de la actividad A2.3, 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" 2.1) • Análisis algorítmico (ver "Guía de Técnicas" 2.2) • Ver también la sección 2.1.3 y 2.1.6.
Participantes • El equipo de proyecto

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

P2: Análisis de riesgos ***A2.4: Estimación del estado de riesgo*** ***T2.4.2: 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 A2.1, Caracterización de los activos • Resultados de la actividad A2.2, Caracterización de las amenazas • Resultados de la actividad A2.3, Caracterización de las salvaguardas
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" 2.1) • Análisis algorítmico (ver "Guía de Técnicas" 2.2) • Ver también la sección 2.1.4 y 2.1.7.
Participantes • El equipo de proyecto

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

P2: Análisis de riesgos
A2.4: Estimación del estado de riesgo
T2.4.3: Interpretación de los resultados

Objetivos

- Interpretar los resultados anteriores de impacto y riesgo
- Establecer relaciones de prioridad por activos o grupos de activos, bien por orden de impacto o por orden de riesgo

Productos de entrada

- Resultados de la actividad A2.1, Caracterización de los activos
- Resultados de la actividad A2.2, Caracterización de las amenazas
- Resultados de la actividad A2.3, Caracterización de las salvaguardas
- Resultados de la tarea T2.4.1, Estimación del impacto
- Resultados de la tarea T2.4.2, Estimación del riesgo

Productos de salida

- Informe priorizado de activos sometidos a mayor impacto
- Informe priorizado de activos sometidos a mayor riesgo
- **Estado de riesgo:** informe resumen del impacto y riesgo potencial y residual a que está sometido cada activo del dominio
- **Informe de insuficiencias**: informe que destaca las incoherencias entre las salvaguardas que se necesitan y las que existen y las divergencias entre la magnitud del riesgo y la eficacia actual de las salvaguardas

Técnicas, prácticas y pautas

- Técnicas gráficas (ver "Guía de Técnicas" 3.4)
- Reuniones (ver "Guía de Técnicas" 3.6.2)
- Presentaciones (ver "Guía de Técnicas" 3.6.3)
- Ver también la sección 2.2.1.

Participantes

- El equipo de proyecto
- El comité de seguimiento

3.4.5. Síntesis del proceso P2

3.4.5.1. Hitos de control

Hito de control H2.1:

Aceptación del informe “Modelo de Valor”.

Hito de control H2.2:

Aceptación del informe “Mapa de Riesgos”.

Hito de control H2.3:

Aceptación del informe “Evaluación de Salvaguardas”.

Hito de control H2.4:

Aceptación del informe “Estado de Riesgo”.

Hito de control H2.5:

Aceptación del informe “Informe de Insuficiencias”.

3.4.5.2. Resultados

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.

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.
- **Evaluación de salvaguardas:**

  Informe que detalla las salvaguardas existentes calificándolas en su eficacia para reducir el riesgo que afrontan.
- **Estado de riesgo:**

  Informe que detalla para cada activo el impacto y el riesgo residuales frente a cada amenaza.
- **Informe de insuficiencias:**

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

Esta documentación es un fiel reflejo del estado de riesgo y de las razones por la que este riesgo no es despreciable. Es fundamental entender las razones que llevan a una valoración determinada de riesgo como paso previo al proceso siguiente, P3, que buscará atajar el riesgo o reducirlo a niveles aceptables.

3.4.6. Lista de control del proceso P2

- √ Identificación de activos (T2.1.1)
- √ Caracterización de los activos (T2.1.1)
- √ Dependencias entre activos (T2.1.2)
- √ Dimensiones relevantes de seguridad por activo (T2.1.3)
- √ Valoración de los activos (T2.1.3)
- √ Modelo de valor (A2.1)
- √ Identificación de las amenazas relevantes (T2.2.1)
- √ Estimación de la frecuencia de ocurrencia (T2.2.2)
- √ Estimación del daño (degradación) derivado de la materialización de una amenaza (T2.2.2)
- √ Mapa de riesgos (A2.2)
- √ Identificación de las salvaguardas existentes (T2.3.1)
- √ Estimación de la eficacia de las salvaguardas existentes (T2.3.2)
- √ Evaluación de salvaguardas (A2.3)
- √ Estimación del impacto e impacto residual (T2.4.1)
- √ Estimación del riesgo y riesgo residual (T2.4.2)
- √ Estado de riesgo (P2)
- √ Informe de insuficiencias (P2)

3.5. Proceso P3: Gestión de riesgos

Se procesan los impactos y riesgos identificados en el proceso anterior, bien asumiéndolos, bien afrontándolos. Para afrontar los riesgos que se consideren inaceptables se llevará a cabo un plan de seguridad que corrija la situación actual. Un plan de seguridad se materializa en una colección de programas de seguridad. Algunos programas serán sencillos, mientras que otros alcanzarán suficiente nivel de complejidad y coste como para que su ejecución se convierta en un proyecto propiamente dicho. La serie de programas (y, en su caso, proyectos) se planifica en el tiempo por medio del denominado Plan de Seguridad que ordena y organiza las actuaciones encaminadas a llevar el estado de riesgo a un punto aceptable y aceptado por la Dirección.

Este proceso se desarrolla por medio de las siguientes actividades y tareas:

Actividad A3.1: Toma de decisiones

En esta actividad se traducen las conclusiones técnicas del proceso P2 en decisiones de actuación.

Tareas:

Tarea T3.1.1: Calificación de los riesgos

Actividad A3.2: Plan de seguridad

En esta actividad se traducen las decisiones de actuación en acciones concretas: proyectos de mejora de la seguridad planificados en el tiempo.

Tareas:

Tarea T3.2.1: Programas de seguridad

Tarea T3.2.2: Plan de ejecución

Actividad A3.3: Ejecución del plan

Esta actividad recoge la serie de proyectos que materializan el plan de seguridad y que se van realizando según dicho plan.

Tareas:

Tarea T3.3.*: Ejecución de cada programa de seguridad

3.5.1. Actividad A3.1: Toma de decisiones

Esta actividad consta de una sola tarea:

T3.1.1: Calificación de los riesgos

P3: Gestión de riesgos ***A3.1: Toma de decisiones*** ***T3.1.1: Calificación de los riesgos***
Objetivos • Calificar los riesgos en una escala: crítico, grave, apreciable o asumible
Productos de entrada • Resultados del proceso P1, Análisis de riesgos • Legislación aplicable, leyes y jurisprudencia • Reglamentación sectorial • Acuerdos y contratos • Informes medio ambientales • Estudios de mercado
Productos de salida • Informe de calificación de impactos y riesgos, incluyendo directrices acerca del plazo de tiempo en que deben estar resueltos
Técnicas, prácticas y pautas • Reuniones (ver "Guía de Técnicas" 3.6.2) • Valoración Delphi (ver "Guía de Técnicas" 3.7) • Ver también la sección 2.2.1.
Participantes • El equipo de proyecto • El comité de seguimiento • El comité de dirección

A la vista de los impactos y riesgos a que está expuesto el sistema, hay que tomar una serie de decisiones de tipo gerencial, no técnico, 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[35] tales como:

35 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

- imagen pública de cara a la Sociedad
- 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 despreciable
- cuando el riesgo residual es despreciable
- cuando el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales

Todas decisiones son propuestas por el comité de seguimiento, oída la opinión del director del proyecto. Todas las decisiones son adoptadas por el comité de dirección.

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

mejor desempeño de las funciones de la Organización en su entorno de operación.

3.5.2. Actividad A3.2: Elaboración del plan seguridad de la información

Se traducen las decisiones de actuación en acciones concretas.

Esta actividad consta de dos tareas:

T3.2.1: Programas de seguridad

T3.2.2: Plan de ejecución

P3: Gestión de riesgos ***A3.2: Elaboración del plan de seguridad de la información*** ***T3.2.1: Programas de seguridad***
Objetivos • Elaborar un conjunto de programas de seguridad
Productos de entrada • Resultados de la tarea T3.1.1, Calificación de los 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 • Análisis de riesgos (ver proceso P2) • Análisis coste-beneficio (ver "Guía de Técnicas" 3.1) • Planificación de proyectos (ver "Guía de Técnicas" 3.5) • Ver también la sección 2.2.2 y 2.2.3.
Participantes • El equipo de proyecto • Especialistas en seguridad • Especialistas en áreas específicas de seguridad

Básicamente, se llevan a cabo dos pasos:

1. Se tomarán en consideración todos los escenarios de impacto y riesgo que se consideren críticos o graves como resultado de la tarea anterior.
2. Se elaborará un conjunto de programas de seguridad que den respuesta a todos y cada uno de los escenarios anteriores, sabiendo que un mismo programa puede afrontar diferentes escenarios y que un escenario puede ser abordado por diferentes programas.

En última instancia se trata de implantar o mejorar la implantación de una serie de salvaguardas que lleven impacto y riesgo a niveles residuales asumidos 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

P3: Gestión de riesgos ***A3.2: Elaboración del plan de seguridad de la información*** ***T3.2.2: Plan de ejecución***
Objetivos • Ordenar temporalmente los programas de seguridad
Productos de entrada • Resultados de la tarea T3.1.1, Calificación de los riesgos • Resultados de la tarea T3.2.1, Programas de seguridad
Productos de salida • Cronograma de ejecución del plan • **Plan de Seguridad**
Técnicas, prácticas y pautas • Análisis de riesgos (ver proceso P2) • Planificación de proyectos (ver "Guía de Técnicas" 3.5)
Participantes • Departamento de desarrollo • Departamento de compras

Hay que ordenar en el tiempo los programas 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.

3.5.3. Actividad A3.3: Ejecución del plan

Esta actividad consta de un número de tareas que depende del plan de seguridad determinado en la actividad A3.2, pues se trata de ir ejecutando los programas allí planificados.

Esta actividad consta de N tareas, tantas como se haya previsto en el plan de seguridad:

T3.3.*: Ejecución de cada programa de seguridad[36]

P3: Gestión de riesgos ***A3.3: Ejecución del plan*** ***T3.3.*: Ejecución de cada programa de seguridad***
Objetivos • Alcanzar los objetivos previstos en el plan de seguridad para cada programa planificado
Productos de entrada • Resultados de la actividad A3.2, Plan de seguridad • Programa de seguridad que nos ocupa • Análisis de riesgos antes de la ejecución del plan
Productos de salida • Salvaguarda implantada • Normas de uso y 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 proceso P2) • Planificación de proyectos (ver "Guía de Técnicas" 3.5)
Participantes • El equipo de proyecto: evolución del análisis de riesgo • Personal especializado en la salvaguarda en cuestión

36 Esta actividad consta de un número indeterminado de tareas a determinar en cada proyecto. De ahí el uno de la notación con *.

3.5.4. Síntesis del proceso P3

3.5.4.1. Hitos de control

Hito de control H3.1:

La Dirección procederá a la aprobación o no del Plan de Seguridad, incluyendo la relación de programas de seguridad y el cronograma propuesto para su ejecución.

Hito de control H3.*:

Compleción de cada programa de seguridad, satisfaciendo los criterios de aceptación impuestos en el Plan de Seguridad.

3.5.4.2. Resultados

Documentación intermedia

- Decisiones de calificación de los escenarios de impacto y riesgo

Documentación final

- Plan de Seguridad

3.5.5. Lista de control del proceso P3

- √ Calificación de los riesgos (T3.1.1)
- √ Identificación de los programas de seguridad necesarios (T3.2.1)
- √ Programas de seguridad
  - √ objetivos
  - √ estimación de esfuerzo
  - √ estimación de coste
  - √ plan de aceptación
  - √ plan de operación
  - √ plan de mantenimiento
  - √ plan de formación
  - √ sistema de controles de eficacia
  - √ sistema de controles de eficiencia
  - √ estimación de impacto y riesgo residuales
- √ Calendario de ejecución (T3.2.2)
- √ Plan de seguridad estratégico: largo plazo (A3.2)
- √ Plan de seguridad táctico: medio plazo (A3.2)
- √ Planes operativos: proyectos singulares (A3.2)

4. 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.

Se pueden identificar dos tipos de actividades diferenciadas:

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

Tras una primera exposición sobre el desarrollo de aplicaciones en general, la sección 4.5 profundiza en su aplicación a Métrica versión 3. Métrica ha sido desarrollada por el CSAE como la “Metodología de Planificación, Desarrollo y Mantenimiento de sistemas de información”.

4.1. Inicialización de los procesos

Hay varias razones que pueden llevar a plantear el desarrollo de una nueva aplicación o la modificación de una existente:

Nuevos servicios y/o datos.

- Requiere el desarrollo de nuevas aplicaciones o la modificación de aplicaciones operativas. Puede implicar la desaparición de aplicaciones 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 nuevas aplicaciones o la modificación de aplicaciones operativas. Puede implicar la desaparición de aplicaciones 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 aplicaciones operativas. Raramente implica el desarrollo de nuevas aplicaciones o la desaparición de aplicaciones operativas.
- La iniciativa la lleva el responsable de seguridad, actuando el responsable de sistemas como subsidiario.

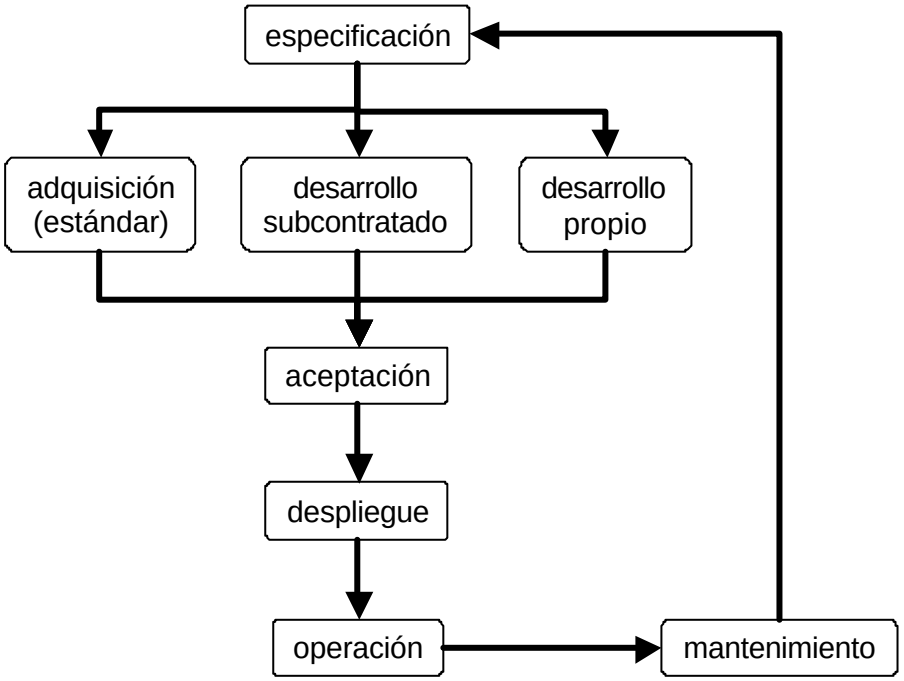
Consideración de nuevas amenazas. La evolución de las tecnologías y los servicios de comunicaciones pueden habilitar nuevas amenazas o convertir amenazas que eran despreciables en el pasado en amenazas relevantes en el futuro.

- Típicamente requiere la modificación de aplicaciones operativas, bien en su codificación o, más frecuentemente, en sus condiciones de explotación. Raramente implica el desarrollo de nuevas aplicaciones o la desaparición de aplicaciones operativas.
- La iniciativa la lleva el responsable de seguridad, actuando el responsable de sistemas como subsidiario.

Modificación de los criterios 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 de aplicaciones operativas. Raramente implica el desarrollo de nuevas aplicaciones o la desaparición de aplicaciones operativas.
- La iniciativa la lleva el responsable de seguridad, actuando el responsable de sistemas como subsidiario.

4.2. Ciclo de vida de las aplicaciones



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

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.

4.2.1. Plan de sistemas

Las aplicaciones informáticas son un componente de los sistemas de información. Es en el marco de un sistema de información donde las diferentes aplicaciones se empotran para hacerse cargo de una fracción de los servicios requeridos. Un plan de sistemas determina el marco de desarrollo y explotación de las aplicaciones informáticas, concretamente:

Los servicios requeridos, tanto para los usuarios internos, como los servicios de soporte a usuarios o aplicaciones internas.

Los datos funcionales que se utilizan.

Las aplicaciones que gestionan dichos datos.

El equipamiento: ordenadores y servicios de comunicaciones.

Desde el punto de vista de seguridad, un plan de sistemas permite

- identificar y valorar los servicios esenciales
- identificar, clasificar y valorar los datos esenciales
- determinar la política de seguridad de la Organización; es decir:
  - el contexto legal en el que opera la Organización
  - los criterios de excelencia en la prestación de los servicios
  - los roles del personal relacionado con los sistemas de información

El plan de sistemas permite establecer el modelo de valor; es decir, los grandes epígrafes (activos) y las primeras valoraciones de lo que acabará siendo un análisis de riesgos detallado.

4.3. Análisis de riesgos

Como parte de un sistema de información, los riesgos asociados a una aplicación deben ser conocidos y estar gestionados. Tanto si son riesgos soportados por la aplicación, o son riesgos repercutidos sobre activos superiores, o son riesgos acumulados sobre activos inferiores.

Magerit permite modelar directamente la aplicación con un activo, estableciendo sus dependencias, bien de activos superiores que dependen de ella, bien de activos inferiores que la soportan. El método permite identificar y valorar amenazas y salvaguardas, derivando información de impacto y riesgo sobre la propia aplicación y los activos relacionados con ella.

AGR autocontenido. Si la Organización no ha realizado un proyecto AGR, será preciso llevarlo a cabo incorporando al menos los activos directa o indirectamente relacionados con la aplicación.

AGR marginal. Si la Organización ya ha realizado un proyecto AGR, basta revisar los resultados de dicho proyecto incorporando los nuevos activos. La aparición de una nueva aplicación puede implicar nuevos servicios, nuevos datos, nuevo equipamiento, nuevos locales y nuevo personal. También puede implicar la desaparición de antiguos activos que se ven superados por la nueva aplicación y sus posibilidades. En cada caso concreto hay que determinar lo que hay que añadir y lo que hay que eliminar, siguiendo las actividades A2.1, A2.2 y

A2.3 del proceso P2, Análisis de riesgos.

Tanto si se ha seguido una u otra aproximación, al final se dispone de una relación de impactos y riesgos, tanto sobre la aplicación como sobre su entorno. Para derivar estos datos se siguen los pasos de la actividad A2.4 del proceso P2. Para interpretar los resultados se recurre a la tarea A2.4.3 del proceso P2, interpretación de los resultados.

4.4. Gestión de riesgos

El proceso P3 de gestión de riesgos recomienda salvaguardas y evalúa el efecto de las salvaguardas desplegadas sobre el impacto y el 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. No obstante, este capítulo se centra en las medidas que deben aplicarse a las aplicaciones para que estas no menoscaben la seguridad del sistema.

Siempre dirigidos por la iniciativa y la corroboración del proceso de gestión de riesgos, hay que tener en cuenta los siguientes aspectos:

Durante la especificación:

- Dimensionado
- Perfiles de usuario
- Requisitos de identificación y autenticación de usuarios
- Requisitos de cifrado
- Requisitos de monitorización (control) y registro *(log)*:
  - de datos de entrada
  - de datos de salida
  - de datos intermedios
  - de acceso a la aplicación
  - de actividad (uso)

Si se adquiere *software* estándar ...

- Contratos de adquisición y mantenimiento

Si se subcontrata el desarrollo de *software* ...

- Contratos de adquisición y mantenimiento
- Entorno de desarrollo: locales, personas, plataforma y herramientas
- Técnicas de programación segura
- Gestión de código fuente
  - control de acceso
  - control de versiones

Si se desarrolla *software* en casa ...

- Condiciones de mantenimiento

- Entorno de desarrollo: locales, personas, plataforma y herramientas
- Técnicas de programación segura
- Gestión de código fuente
  - control de acceso
  - control de versiones

Para realizar la aceptación:

- Pruebas de aceptación
  - 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
  - pruebas en carga
  - 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)*
  - acreditaciones

Para realizar el despliegue:

- Inventario de aplicaciones en operación
- Gestión de cambios: normativa y procedimientos
- Establecimiento de claves

Durante la operación:

- Normativa y procedimientos de ...
  - gestión de usuarios
  - gestión de claves
  - gestión de registros *(log)*
  - gestión de incidencias: registro de evidencias, escalado, plan de emergencia y de recuperación
- Análisis de registros *(log)*: herramientas, criterios, procedimientos, ...
- Manuales de uso: administradores, operadores y usuarios
- Formación: inicial y continua: administradores, operadores y usuarios

En los ciclos de mantenimiento:

- Normativa y procedimientos de ...
  - solicitud

- aprobación, incluyendo el análisis diferencial de riesgos y, aprobación en su caso de las nuevas medidas

Terminación

- Destrucción de datos operacionales
- Copia y custodia de datos, cuando proceda por ley o política interna
- Eliminación del código operativo: ejecutable, datos de configuración y cuentas de usuario
- Revisión de las copias de seguridad

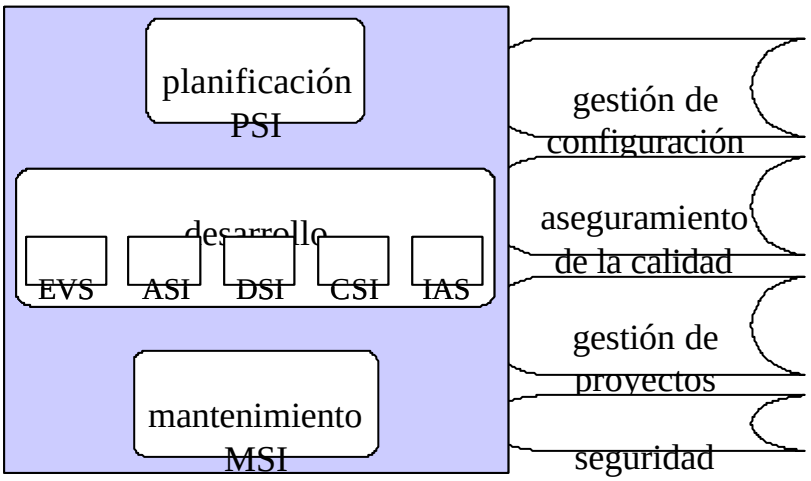
4.5. MÉTRICA versión 3

La metodología MÉTRICA Versión 3 ofrece a las Organizaciones un instrumento útil para la sistematización de las actividades que dan soporte al ciclo de vida del *software* dentro del marco que permite alcanzar los siguientes objetivos:

- Proporcionar o definir sistemas de información que ayuden a conseguir los fines de la Organización mediante la definición de un marco estratégico para el desarrollo de los mismos.
- Dotar a la Organización de productos *software* que satisfagan las necesidades de los usuarios dando una mayor importancia al análisis de requisitos.
- Mejorar la productividad de los departamentos de sistemas y tecnologías de la información y las comunicaciones, permitiendo una mayor capacidad de adaptación a los cambios y teniendo en cuenta la reutilización en la medida de lo posible.
- Facilitar la comunicación y entendimiento entre los distintos participantes en la producción de *software* a lo largo del ciclo de vida del proyecto, teniendo en cuenta su papel y responsabilidad, así como las necesidades de todos y cada uno de ellos.
- Facilitar la operación, mantenimiento y uso de los productos *software* obtenidos.

Cuando el desarrollo de la aplicación se atenga a la metodología MÉTRICA versión 3, los aspectos anteriormente tratados para asegurar que la nueva aplicación no altere incontroladamente el estado de riesgo de la Organización deberán tenerse en cuenta a lo largo del proceso de desarrollo.

MÉTRICA versión 3 identifica 3 procesos, 5 subprocesos y 4 interfaces:



PSI – Planificación del sistema de información

EVS – Estudio de viabilidad del sistema

ASI – Análisis del sistema de información

DSI – Diseño del sistema de información.

CSI – Construcción del sistema de información

IAS – Implantación y aceptación del sistema

MSI – Mantenimiento del sistema de información

La interfaz de seguridad permite la comunicación entre las tareas de desarrollo y las tareas de análisis y gestión 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 riesgo aporta un juicio crítico sobre la seguridad del sistema.

Es decir que se manejan simultáneamente diferentes requisitos:

- de servicio, procedentes de la dirección
- técnicos, procedentes del equipo de desarrollo
- de seguridad, procedentes del equipo de análisis de riesgo

Esto da pie a una interrelación continua entre el equipo de desarrollo y el equipo de seguridad que, a través de la interfaz de seguridad, van cerrando cada etapa de Métrica. Es importante destacar que el alcance de un nivel de seguridad puede requerir modificaciones en los componentes técnicos del sistema; al tiempo que los detalles técnicos pueden alterar el análisis de seguridad. En cualquier caso, el punto de acuerdo entre los componentes (activos) y el estado de seguridad (impacto y riesgo) debe ser aprobado por la dirección de la Organización.

Como se indica más arriba, se puede distinguir entre la seguridad del proceso de desarrollo (tareas SPD) y la seguridad del sistema de información (SSI). Las tareas de la interfaz se organizan según su pertenencia a uno u otro objetivo de seguridad.

4.5.1. 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:

Tareas afectadas en la Interfaz de Seguridad de Métrica v3
PSI: Planificación del sistema de información
SEG 1: Planificación de la seguridad requerida en el proceso PSI
PSI-SEG 1.1: Estudio de la seguridad requerida en el proceso PSI
PSI-SEG 1.2: Organización y planificación
SEG 4: Catalogación de los productos generados durante el proceso PSI
PSI-SEG 4.1: Clasificación y catalogación de los productos generados durante el proceso PSI

Tareas afectadas en la Interfaz de Seguridad de Métrica v3
EVS: Estudio de viabilidad del sistema
SEG 1: Estudio de la seguridad requerida en el proceso EVS
EVS-SEG 1.1: Estudio de la seguridad requerida en el proceso EVS
SEG 2: Selección del equipo de seguridad
EVS-SEG 2.1: Selección del equipo de seguridad
SEG 6: Catalogación de los productos generados durante el proceso EVS
EVS-SEG 6.1: Clasificación y catalogación de los productos generados durante el proceso EVS
ASI: Análisis del sistema de información
SEG 1: Estudio de la seguridad requerida en el proceso ASI
ASI-SEG 1.1: Estudio de la seguridad requerida en el proceso ASI
SEG 4: Catalogación de los productos generados durante el proceso ASI
ASI-SEG 4.1: Clasificación y catalogación de los productos generados durante el proceso ASI
DSI: Diseño del sistema de información
SEG 1: Estudio de la seguridad requerida en el proceso DSI
DSI-SEG 1.1: Estudio de la seguridad requerida en el proceso DSI
SEG 5: Catalogación de los productos generados durante el proceso DSI
DSI-SEG 5.1: Clasificación y catalogación de los productos generados durante el proceso DSI
CSI: Construcción del sistema de información
SEG 1: Estudio de la seguridad requerida en el proceso CSI
CSI-SEG 1.1: Estudio de la seguridad requerida en el proceso CSI
SEG 4: Clasificación de los productos generados durante el proceso CSI
CSI-SEG 4.1: Clasificación y catalogación de los productos generados durante el proceso CSI
IAS: Implantación y aceptación del sistema
SEG 1: Estudio de la seguridad requerida en el proceso IAS
IAS-SEG 1.1: Estudio de la seguridad requerida en el proceso IAS
SEG 4: Catalogación de los productos generados durante el proceso IAS
IAS-SEG 4.1: Clasificación y catalogación de los productos generados durante el proceso IAS
MSI: Mantenimiento del sistema de información
SEG 1: Estudio de la seguridad requerida en el proceso MSI
MSI-SEG 1.1: Estudio de la seguridad requerida en el proceso MSI
SEG 3: Catalogación de los productos generados durante esta etapa
MSI-SEG 3.1: Clasificación y catalogación de los productos generados durante esta etapa

Activos a considerar

En cada proceso se requiere un análisis de riesgo 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 riesgo recibe a través del director de seguridad la información de los activos involucrados
3. el equipo de análisis de riesgo realiza el análisis riesgos
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 riesgo 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

4.5.2. SSI – Seguridad del sistema de información

Todo 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.

La utilización de herramientas de soporte debe permitir

1. capturar un modelo inicial (PSI),
2. estudiar variaciones (EVS y ASI),
3. pasar de lo general a lo concreto, previniendo amenazas potenciales y preparando mecanismos de detección y reacción (DSI y CSI)
4. dirigir su aceptación y explotación (IAS)
5. revisar periódicamente los cambios que se propongan (MSI)

Uso de las tareas de la metodología Magerit

Proceso P1: Planificación

Actividad A1.1: Estudio de oportunidad

Tarea T1.1.1: Determinar la oportunidad

Esta tarea se reduce a la decisión, interna, de desarrollar el sistema de información teniendo en cuenta la seguridad.

Actividad A1.2: Determinación del alcance del proyecto

Tarea T1.2.1: Objetivos y restricciones generales

Los del sistema de información bajo desarrollo.

Tarea T1.2.2: Determinación de dominio y límites

Los del sistema de información bajo desarrollo.

Tarea T1.2.3: Identificación del entorno

Los del sistema de información bajo desarrollo.

Tarea T1.2.4: Estimación de dimensiones y coste

Parte de proyecto (o proyectos) de desarrollo del sistema de información.

Actividad A1.3: Planificación del proyecto

Tarea T1.3.1: Evaluar cargas y planificar entrevistas

Esta tarea se lleva a cabo como en cualquier proyecto AGR. Esta tarea se debe realizar con el primer proceso, PSI, quedando establecida la relación de entrevistas para el resto de los procesos, salvo ajustes puntuales que se detecten necesarios.

Tarea T1.3.2: Organizar a los participantes

Esta tarea se lleva a cabo como en cualquier proyecto AGR. Durante el primer proceso, PSI, debe establecerse la relación de participantes a entrevistar, sin precisar más allá el role que desempeñan. Según vaya avanzando el desarrollo del sistema, se irá identificando a las personas que satisfacen los roles previstos.

Tarea T1.3.3: Planificar el trabajo

Parte de proyecto (o proyectos) de desarrollo del sistema de información.

Actividad A1.4: Lanzamiento del proyecto

Tarea T1.4.1: Adaptar los cuestionarios

Esta tarea se lleva a cabo como en cualquier proyecto AGR. Esta tarea se debe realizar con el primer proceso, PSI, quedando establecidos para el resto de los procesos, salvo ajustes puntuales.

Tarea T1.4.2: Criterios de evaluación

Esta tarea se lleva a cabo como en cualquier proyecto AGR. Esta tarea se debe realizar con el primer proceso, PSI, quedando establecidos para el resto de los procesos.

Tarea T1.4.3: Recursos necesarios

Parte de proyecto (o proyectos) de desarrollo del sistema de información.

Tarea T1.4.4: Sensibilización

Parte de proyecto (o proyectos) de desarrollo del sistema de información.

Proceso P2: Análisis de riesgos

Actividad A2.1: Caracterización de los activos

Tarea T2.1.1: Identificación de los activos

En los primeros procesos, PSI, se identifican activos genéricos. Según se avanza en el desarrollo, esta identificación se va precisando de forma que los activos genéricos se traducen en activos concretos. La concreción debe ser máxima al llegar al proceso CSI.

Tarea T2.1.2: Dependencias entre activos

En los primeros procesos, PSI, aparecen relaciones de trazo grueso. Según se avanza en el desarrollo, las dependencias se van precisando según los activos genéricos se traducen en activos concretos. La concreción debe ser máxima al llegar al proceso CSI.

Tarea T2.1.3: Valoración de los activos

La valoración de los servicios últimos y de los datos esenciales se puede realizar prácticamente desde el primer proceso PSI, si bien según avance el desarrollo pueden segmentarse los servicios y/o los datos, requiriendo una valoración singular que nunca

deberá suponer la superación de la valoración de los servicios o datos agregados. Es decir, pueden desagregarse los servicios y/o los datos en fracciones de menor valor.

Típicamente la valoración del resto de los activos puede analizarse como simple valor acumulado desde los activos superiores, explotando las relaciones de dependencia.

Actividad A2.2: Caracterización de las amenazas

Tarea T2.2.1: Identificación de las amenazas

Las amenazas sobre activos genéricos pueden incorporarse desde el primer proceso PSI; pero según se vaya concretando el conjunto detallado de componentes habrá que incorporar amenazas específicas de la tecnología que se emplea.

Tarea T2.2.2: Valoración de las amenazas

Esta tarea se lleva a cabo como en cualquier proyecto AGR.

Actividad A2.3: Caracterización de las salvaguardas

Tarea T2.3.1: Identificación de las salvaguardas existentes

Buena parte de las salvaguardas pueden incorporarse desde el primer proceso PSI.

No obstante, las salvaguardas de carácter técnico, deberán irse precisando según se vaya concretando el conjunto detallado de componentes y la tecnología que se emplea.

Tarea T2.3.2: Valoración de las salvaguardas existentes

Esta tarea se lleva a cabo como en cualquier proyecto AGR.

Actividad A2.4: Estimación del estado de riesgo

Tarea T2.4.1: Estimación del impacto

Esta tarea se lleva a cabo como en cualquier proyecto AGR.

Tarea T2.4.2: Estimación del riesgo

Esta tarea se lleva a cabo como en cualquier proyecto AGR.

Tarea T2.4.3: Interpretación de los resultados

Esta tarea se lleva a cabo como en cualquier proyecto AGR.

Proceso P3: Gestión de riesgos

Actividad A3.1: Toma de decisiones

Tarea T3.1.1: Calificación de los riesgos

Esta tarea se lleva a cabo como en cualquier proyecto AGR.

En la toma de decisiones debe participar tanto el equipo de desarrollo como el equipo de análisis de riesgos.

Actividad A3.2: Elaboración del plan director de seguridad de la información

Tarea T3.2.1: Programas de seguridad

Esta tarea queda subsumida en las tareas de desarrollo.

Tarea T3.2.2: Plan de ejecución

Esta tarea queda subsumida en las tareas de desarrollo.

Actividad A3.3: Ejecución del plan

Tarea T3.3.*: Ejecución de cada programa de seguridad

Estas tareas quedan subsumidas en las tareas de desarrollo.

Otras consideraciones

Es importante llevar a cabo los diferentes análisis de riesgos de una forma evolutiva, incorporando mayor detalle según avanza el desarrollo; pero nunca volviendo a comenzar desde cero.

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.

Las normas y procedimientos que se derivan en cada proceso van constituyendo el conjunto de normas y procedimientos que se emplearán durante la explotación del sistema.

- Típicamente la normativa debe cerrarse en los primeros procesos: PSI, EVS y ASI, siendo infrecuente su modificación en los procesos siguientes.
- Por el contrario, los procedimientos no se pueden derivar hasta concretar el detalle en los procesos DSI, CSI e IAS. No deberían modificarse, salvo ajustes y correcciones, en los procesos siguientes.
- El proceso IAS pasa normas y procedimientos a explotación.
- El proceso MSI puede suponer la reparación de normas o procedimientos erróneos, o la extensión de normas o procedimientos incompletos que no hayan contemplado todas las circunstancias prácticas.

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.

Tareas afectadas en la Interfaz de Seguridad de Métrica v3
PSI: Planificación del sistema de información
SEG 2: Evaluación del riesgo para la arquitectura tecnológica
PSI-SEG 2.1: Estudio y evaluación del riesgo de las alternativas de arquitectura tecnológica
PSI-SEG 2.2: Revisión de la evaluación del riesgo de las alternativas de arquitectura tecnológica
SEG 3: Determinación de la seguridad en el plan de acción
PSI-SEG 3.1: Determinación de la seguridad en el plan de acción
EVS: Estudio de viabilidad del sistema
SEG 3: Recomendaciones adicionales de seguridad para el SI
EVS-SEG 3.1: Elaboración de recomendaciones de seguridad
SEG 4: Evaluación de la seguridad de las alternativas de solución
EVS-SEG 4.1: Valoración y evaluación de la seguridad de las alternativas de solución
SEG 5: Evaluación detallada de la seguridad de la solución propuesta
EVS-SEG 5.1: Descripción detallada de la seguridad de la solución propuesta
ASI: Análisis del sistema de información
SEG 2: Descripción de las funciones y mecanismos de seguridad
ASI-SEG 2.1: Estudio de las funciones y mecanismos de seguridad a implantar
SEG 3: Definición de los criterios de aceptación de la seguridad
ASI-SEG 3.1: Actualización del plan de pruebas

Tareas afectadas en la Interfaz de Seguridad de Métrica v3
DSI: Diseño del sistema de información
SEG 2: Especificación de requisitos de seguridad del entorno tecnológico
DSI-SEG 2.1: Análisis de los riesgos del entorno tecnológico
SEG 3: Requisitos de seguridad del entorno de construcción
DSI-SEG 3.1: Identificación de los requisitos de seguridad del entorno de construcción
SEG 4: Diseño de pruebas de seguridad
DSI-SEG 4.1: Diseño de las pruebas de seguridad
CSI: Construcción del sistema de información
SEG 2: Evaluación de los resultados de pruebas de seguridad
CSI-SEG 2.1: Evaluación de los resultados de pruebas de seguridad
SEG 3: Elaboración del plan de formación de seguridad
CSI-SEG 3.1: Elaboración del plan de formación de seguridad
IAS: Implantación y aceptación del sistema
SEG 2: Revisión de medidas de seguridad en el entorno de operación
IAS-SEG 2.1: Revisión de medidas de seguridad en el entorno de operación
SEG 3: Evaluación de resultados de pruebas de seguridad de implantación del sistema
IAS-SEG 3.1: Estudio de los resultados de pruebas de seguridad de implantación del sistema
SEG 5: Revisión de medidas de seguridad en el entorno de producción
IAS-SEG 5.1: Revisión de medidas de seguridad en el entorno de producción
MSI: Mantenimiento del sistema de información
SEG 2: Especificación e identificación de las funciones y mecanismos de seguridad
MSI-SEG 2.1: Estudio de la petición
MSI-SEG 2.2: Análisis de las funciones y mecanismos de seguridad afectados o nuevos

4.6. Referencias

- NIST Special Publication 800-64, “Security Considerations in the Information System Development Life Cycle”, Rev.1. June 2004.
- NIST Special Publication 800-27 Rev. A, “Engineering Principles for Information Technology Security (A Baseline for Achieving Security)”, Rev. A, June 2004.
- “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.

5. 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. 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.

5.1. 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[37] o como elementos de valoración[38]. 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[39].

37 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.

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

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

Identificación de activos

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

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

No siempre es evidente qué es un activo en singular. 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.

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.

5.2. Para descubrir y modelar las dependencias entre activos

A veces es más difícil de lo que 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.

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?
- si usted quisiera detener este servicio, ¿dónde atacaría?

Este planteamiento de “póngase en el lugar del atacante” es el que da pie a las técnicas denominadas “árboles de ataque”[40] 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[41]. 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 de-

40 Ver “Guía de Técnicas”, sección 2.3.

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

pendencias, pues las dependencias de dichos servicios se interpretan sin ambigüedad como dependencia de todos los elementos que prestan el servicio.

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.

Errores típicos

No es correcto decir que una aplicación depende de los datos 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: los datos dependen de la aplicación. En términos de valor, se puede asegurar que la aplicación no vale nada sin datos. Como el valor es una propiedad de los datos, es ese valor el que hereda la aplicación. Luego los datos dependen de la aplicación. Desde otro punto de vista, a través de la aplicación puede accederse a los datos, convirtiéndose la aplicación en la vía de ataque a los datos.

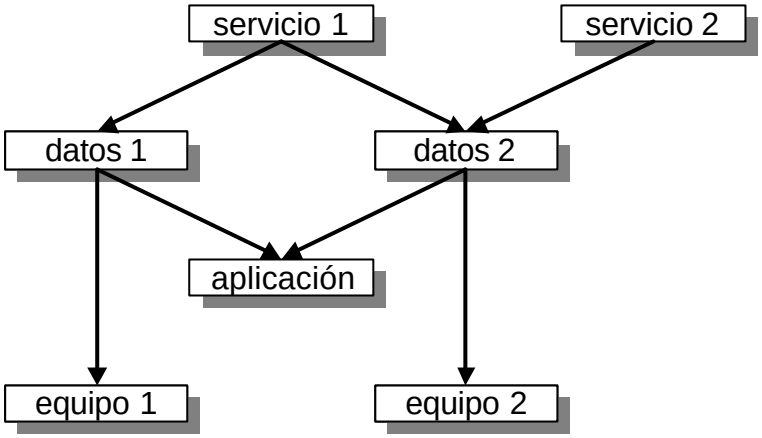
Dado que datos y aplicaciones suelen aunar esfuerzos para la prestación de un servicio, el valor del servicio se transmite tanto a los datos como a las aplicaciones intervinientes.

mal	***bien***
• servicio aplicación • aplicación datos	• servicio datos • datos aplicación • servicio aplicación

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

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



¿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.

5.3. Para valorar activos

Siempre conviene valorar la información o datos que constituyen la razón de ser del sistema de información.

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

Es fácil identificar activos de tipo datos o 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.

El resto de los activos puede frecuentemente pasar sin valorar, pues su valor más importante es soportar los datos 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[42]: 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[43].

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.

5.4. 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.

42 Ver "Guía de Técnicas", capítulo 3.7.

43 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.

5.5. Para valorar amenazas

La tarea es desmoralizadora: para cada activo en cada dimensión, determinar la degradación que causarían y la frecuencia probable 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[44]
- que no requiera gran inversión en equipo por parte del atacante[45]
- 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

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 e 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.

44 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).

45 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.

5.6. 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.

5.7. 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 riesgo es imperfecto, evidentemente; pero cabe confiar en que lleve en la dirección 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.

5.7.1. 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 puede 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/IEC 17799:2005
- normas nacionales, por ejemplo los “Criterios de Seguridad”
- normas sectoriales
- normas corporativas, especialmente frecuentes en pequeñas delegaciones de grandes organizaciones

Las ventajas de protegerse por catálogo son:

- es muy rápido
- no cuesta apenas esfuerzo
- 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 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.

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 inci-

dencias 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 las vulnerabilidades

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.

5.8. Referencias

- ISO/IEC 17799:2005, “Information technology – Security techniques – Code of practice for information security management”, Junio 2005.
- “Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades”, MAP, 2004
- C. Alberts and A. Dorofee, “Managing information Security Risks. The OCTAVE Approach”, Addison Wesley, 2003.
- UNE-ISO/IEC 17799:2002, “Tecnología de la Información. Código de Buenas Prácticas de la Gestión de la Seguridad de la Información”, 2002.
- United States General Accounting Office, Accounting and Information Management Division, “Information Security Risk Assessment -- GAO Practices of Leading Organizations.
- Ministerio de Administraciones Públicas, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, MAP, versión 1.0, 1997.

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).

1.1. Términos en español

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	**Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección.** 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: Anything that has value to the organization. [13335-1:2004] 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]
AGR	Análisis y Gestión de Riesgos
Amenaza	**Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.** Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos. [Mage-

	rit: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: A potential cause of an incident which may result in harm to a system or organization. [17799:2005][13335-1:2004]
	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. [800-53:2004]
	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.**
	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 analysis: Systematic use of information to identify sources and to estimate the risk. [17799:2005][Guide 73:2002]
	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: The systematic process of estimating the magnitude of risks. [13335-1:2004]
	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] 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	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	**Aseguramiento de la identidad u origen.** 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. [800-53:2004] Authenticity: The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems, and information. [13335-1:2004]
Certificación	Confirmación del resultado de una evaluación, y que los criterios de evaluación utilizados fueron correctamente aplicados.
Confidencialidad	**Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.** Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso. [17799:2002] 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. [800-53:2004] 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]

	Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [7498-2:1989]
Contra medida	Véase salvaguarda.
Control	Véase salvaguarda.
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.** Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados. [17799:2002] 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. [800-53:2004] 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. [7498-2:1989]
Documento de selección de controles	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.
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.**
Gestión de riesgos	**Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.** 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] Risk management: Coordinated activities to direct and control an organization with regard to risk. [17799:2005][Guide 73:2002]

	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 que sobre un activo tiene la materialización de una amenaza. [Magerit:1997] Impact: The result of an information security incident. [13335-1:2004] 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	**Evento con consecuencias en detrimento de la seguridad del sistema de información.** Information security event: An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant. [17799:2005] Information security incident: Any unexpected or unwanted event that might cause a compromise of business activities or information security. [13335-1:2004] 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	**Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.** Garantía de la exactitud y completitud de la información y los métodos de su procesamiento. [17799:2002] 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] Integrity: Guarding against improper information modification or destruc-

	tion, and includes ensuring information non-repudiation and authenticity. [800-53:2004] Integrity: the property of safeguarding the accuracy and completeness of assets. [13335-1:2004] 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]
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 programas de seguridad que permiten materializar las decisiones de gestión de riesgos.**
Programa de seguridad	**Agrupación de tareas orientadas a afrontar 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.**
Proyecto de seguridad	**Programa de seguridad cuya envergadura es tal que requiere una planificación específica.**
Riesgo	**Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.** Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la Organización. [Magerit:1997] 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: combination of the probability of an event and its consequence. [17799:2005][Guide 73:2002] Risk: A measure of the potential degree to which protected information is subject to loss through adversary exploitation. [OPSEC]

	Risk: the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. [13335-1:2004]
	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 residual	**Riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información.**
	Riesgo que se da tras la aplicación de salvaguardas dispuestas en un escenario de simulación o en el mundo real. [Magerit:1997]
	Residual risk: The risk that remains after risk treatment. [13335-1:2004]
	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]
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 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.
Salvaguarda	**Procedimiento o mecanismo tecnológico que reduce el riesgo.**
	Control: Means of managing risks, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management or legal nature. [17799:2005]
	Countermeasure: Anything which effectively negates or mitigates an adversary's ability to exploit vulnerabilities. [OPSEC]
	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. [800-53:2004]
	Safeguard: a practice, procedure or mechanism that treats risk. [13335-1:2004]
	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.** 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]
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 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]
Trazabilidad	**Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.** 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: The property that ensures that the actions of an entity may be traced uniquely to the entity. [13335-1:2004] 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	**Estimación de la exposición efectiva de un activo a una amenaza. Se determina por dos medidas: frecuencia de ocurrencia y degradación causada.** 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: A weakness of an asset or group of assets that can be exploited by one or more threats. [17799:2005][13335-1:2004] 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]

1.2. Términos anglosajones

Breve diccionario inglés-español de términos habituales en análisis y gestión de riesgos:

Accountability	Trazabilidad
ALE	Annual Loss Expectancy
ARO	Annual Rate of Occurrence
Authenticity	Autenticidad
Availability	Disponibilidad
Asset	Activo
BIA	Business Impact Analysis
Business Impact Analysis	Análisis de impacto
Confidentiality	Confidencialidad
Countermeasure	Contra medida
Frequency	Frecuencia
Impact	Impacto
Integrity	Integridad
Residual risk	Riesgo residual
Risk	Riesgo
Risk analysis	Análisis de riesgos
Risk assessment	Análisis de riesgos
Risk management	Gestión de riesgos
Risk map	Mapa de riesgo
Safeguard	Salvaguarda
Security	Seguridad

Statement of applicability	Documento de selección de controles
Traceability	Trazabilidad
Threat	Amenaza
Value	Valor
Vulnerability	Vulnerabilidad

En alguna ocasión la correspondencia no es directa. Así ocurre en el caso de la norma ISO/IEC 17799:2005 que estructura los conceptos de acuerdo a la Guía 73 de ISO [2002]:

Risk: combination of the probability of an event and its consequence.

Risk analysis: systematic use of information to identify sources and to estimate risk.

Risk assessment: overall process of risk analysis and risk evaluation.

Risk evaluation: process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

Risk management: coordinated activities to direct and control an organization with regard to risk.

Risk treatment: process of selection and implementation of measures to modify risk.

Nótese que se le da nombre propio a algunas tareas de esta metodología. Así, “risk evaluation” corresponde a la tarea

1.3. Referencias

[DRAE]
Real Academia Española. Diccionario de la Lengua Española. 22.ª edición, 2001. http://buscon.rae.es/diccionario/drae.htm

[OPSEC]
OPSEC Glossary of Terms, http://www.ioss.gov/docs/definitions.html

[17799:2005]
ISO/IEC 17799:2005, “Information technology -- Code of practice for information security management”, 2005.

[15443-1:2005]
ISO/IEC TR 15443:2005, “Information technology -- Security techniques -- A framework for IT security assurance -- Part 1: Overview and framework”, 2005.

[800-53:2004]
NIST, “Recommended Security Controls for Federal Information Systems”, National Institute of Standards and Technology, special publication 800-53, 2004.

[13335-1:2004]
ISO/IEC 13335-1:2004, “Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management”, 2004.

[CRAMM:2003]
“CCTA Risk Analysis and Management Method (CRAMM)”, Version 5.0, 2003.

[Octave:2003]
C. Alberts and A. Dorofee, “Managing information Security Risks. The OCTAVE Approach”, Addison Wesley, 2003.

[TDIR:2003]
Texas Department of Information Resources, “Practices for Protecting Information Resources Assets“, Revised September 2003.

[CNSS:2003]
Committee on National Security Systems, Instruction No. 4009, “National Information Assurance (IA) Glossary“, May 2003.

[17799:2002]
UNE ISO/IEC :2002, “Tecnología de la Información – Código de Buenas Prácticas para la Gestión de la Seguridad de la Información”, 2002.

[CIAO:2000]
Critical Infrastructure Assurance Office, “Practices for Securing Critical Information Assets”, January 2000.

[CC:1999]
ISO/IEC 15408:1999, “Information technology — Security techniques — Evaluation criteria for IT security”, 1999.

[NSTISS:1998]
National Security Telecommunications and Information Systems Security Committee, “Index of National Security Telecommunications Information Systems Security Issuances”, NSTISSI no. 4014, NSTISSC Secretariat, 1998.

[CESID:1997]
Centro Superior de Información de la Defensa, “Glosario de Términos de Criptología”, Ministerio de Defensa, 3ª edición, 1997.

[Magerit:1997]
Ministerio de Administraciones Públicas, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, MAP, versión 1.0, 1997.

[Ribagorda:1997]
A. Ribagorda, “Glosario de Términos de Seguridad de las T.I.”, Ediciones CODA, 1997.

[7498-2:1989]
ISO 7498-2:1989, “Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture”, 1989.

Apéndice 2. Referencias

Aunque los capítulos y apéndices incluyen referencias bibliográficas específicas al tema que enfocan, en este apéndice se recopilan las referencias a métodos y metodologías que afrontan el análisis y gestión de riesgos como actividad integral. Las referencias se ordenan temporalmente: de más recientes a más antiguas.

- Federal Office for Information Security (BSI). “IT Baseline Protection Manual”, October 2003. Germany.
  http://www.bsi.de/gshb/english/etc/index.htm
- “The Vulnerability Assessment and Mitigation Methodology”, P.S. Antón et al., RAND National Defense Research Institute, MR-1601-DARPA, 2003.
- “Managing Information Security Risks: The OCTAVE Approach”, C.J. Alberts and A.J. Dorofee, Addison-Wesley Pub Co; 1st edition (July 9, 2002)
  http://www.cert.org/octave/
- “Information Security Risk Analysis”, T.R. Peltier, Auerbach Pub; 1st edition (January 23, 2001)
- “Risk Management: Multiservice Tactics, Techniques, and Procedures for Risk Management”, Air Land Sea Application Center, FM 3-100.12, MCRP 5-12.1C, NTTP 5-03.5, AFTTP(I) 3-2.30. February 2001.
- Air Force Pamphlet 90-902, “Operational Risk Management (ORM) Guidelines and Tools”, December 2000.
- KPMG Peat Marwick LLP, “Vulnerability Assessment Framework 1.1“, October 1998.
- Magerit, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, MAP, versión 1.0, 1997
  http://www.csi.map.es/csi/pg5m20.htm
- GMITS, ISO/IEC TR 13335-2:1997, “Information technology - Security techniques - Guidelines for the management of IT security - Part 2: Managing and planning IT security”.

Por último se debe citar una herramienta que lleva implícitamente una metodología. Al ser un producto, le fecha se limita a indicar la de la ultima versión en el mercado.

- CRAMM, “CCTA Risk Analysis and Management Method (CRAMM)”, Version 5.0, 2003.

Apéndice 3. Marco legal

En este apéndice se recopila la 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 un proyecto AGR. 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..

La documentación actualizada puede encontrarse en las páginas web del SSISTAD[46] del CSAE[47]:

http://www.csi.map.es/

Por último, 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.

3.1. Procedimiento administrativo

- Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, LRJ-PAC.
- Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.
- Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.
- Resolución de 26 de mayo de 2003 de la Secretaría de Estado para la Administración Pública por la que se dispone la publicación del Acuerdo del Pleno de la Comisión Interministerial de Adquisición de Bienes y Servicios Informáticos (CIABSI) de 18 de diciembre de 2002 por el que se aprueban los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas por la Administración General del Estado en el ejercicio de sus potestades.
- Orden PRE/1551/2003, de 10 de junio, por la que se desarrolla la Disposición final primera del Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

3.2. Protección de datos de carácter personal

- LOPD, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

3.3. 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,

46 SSITAD: Seguridad de los Sistemas de Información y Protección de Datos Personalizados Automatizados, comité técnico del CSAE.

47 CSAE: Consejo Superior de Administración Electrónica.

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.

3.4. 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)

3.5. 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
- Guías de la OCDE para la seguridad de los sistemas de información y redes. 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.

4.1. Sistemas de gestión de la seguridad de la información (SGSI)

Los problemas de seguridad de los sistemas de información tienen un origen técnico pero son tan complejos que la solución no puede ser solamente técnica. La tecnología es demasiado rica en oportunidades y por tanto hay que mantenerla bajo control asegurando que trabaje para los objetivos de la Organización.

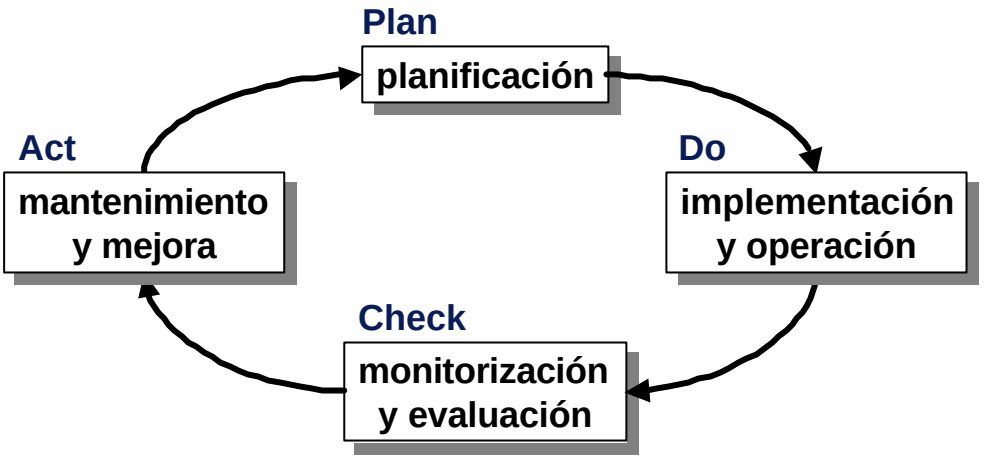
Seguridad es estar prevenido (antes); es estar preparado para reaccionar a las emergencias, previstas o imprevistas; y es saber rehacerse tras el desastre. Todo esto no es gratis: cuesta dinero, tiempo y esfuerzo. Por ello es necesario racionalizar, con criterio económico, una solución equilibrada entre lo que se evita que ocurra, lo que se monta para detectar fallos, y lo que se tiene preparado para cuando ocurra lo que, teóricamente, nunca debiera haber ocurrido. Y, todo eso, sin olvidar la dimensión tiempo, porque hay que racionalizar gastos e inversiones tanto para lo que sabemos hoy como para lo que descubriremos mañana.

Aparece pues un componente de gestión, tan necesario como los componentes técnicos.

Sistema de gestión de la seguridad de la información

> Es un sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información. El sistema es la herramienta de que dispone la Dirección de las organizaciones para llevar a cabo las políticas y los objetivos de seguridad (integridad, confidencialidad y disponibilidad, asignación de responsabilidad, autenticación, etc.). Proporciona mecanismos para la salvaguarda de los activos de información y de los sistemas que los procesan, en concordancia con las políticas de seguridad y planes estratégicos de la organización. [UNE 71502:2004]

Esta es la esencia del modelo PDCA (de inglés *Plan, Do, Check, Act*) que se usa en los modelos de gestión de la calidad.



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 los objetivos propuestos.

4.1.1. La certificación

Certificar un sistema de gestión de la seguridad consiste en que alguien, competente, afirma que un sistema está sano y 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 or-

ganigrama 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 caso es tener una estrategia, marcada por la política y el detalle del mapa de riesgos.

Un análisis de riesgo 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.

Los resultados del análisis de riesgos permiten elaborar un documento de selección de controles, así como una justificación de la calidad que deben tener. 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” (por ejemplo, en España, disponemos de la norma UNE 71502).

La norma UNE 71502:2004 tiene por objeto la especificación de “los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información de acuerdo con la norma UNE ISO/IEC 17799:2002 dentro del contexto de los riesgos identificados por las organizaciones. Especifica los requisitos de los controles de seguridad de acuerdo con las necesidades de las organizaciones con independencia de su tipo, tamaño o área de actividad.”

La norma UNE 71502:2004 parte de una relación de controles basada en la norma UNE-ISO/IEC 17799:2002, relación que hay que ajustar a la organización sujeta a evaluación, obviando los elementos que no son pertinentes. De considerarse necesario se seleccionarán controles específicos adicionales, fuera de la UNE-ISO/IEC 17799, para cada organización, adecuados a su modelo particular de negocio, así como los objetivos que se pretenden obtener con los mismos, justificando la selección.

La relación básica es la siguiente:

Política de seguridad

- Revisión y evaluación periódica de la política de seguridad
- Control y gestión de la documentación

Aspectos organizativos para la seguridad

- Asignación de responsabilidades sobre Seguridad de la Información
- Identificación de riesgo por el acceso de terceros
- Contratación de servicios
- Contratación de outsourcing
- Contratación de empresas colaboradoras

Clasificación y control de activos

- Inventario de activos

- Clasificación de activos
- Clasificación de la información
- Revisión y clasificación periódica de activos
- Revisión periódica del análisis de riesgos
- Marcado y tratamiento de la información

Seguridad ligada al personal

- Contratación del personal
- Formación
- Comunicación de incidencias

Seguridad física y del entorno

- Instalación y protección de los equipos
- Mantenimiento de los equipos

Gestión de comunicaciones y operaciones

- Procesos operativos
- Control de cambios
- Gestión de incidencias
- Medidas y controles contra *software* dañino
- Recuperación de información
- Gestión de soportes removibles
- Eliminación de soportes
- Seguridad del correo electrónico
- Disponibilidad de sistemas públicos
- Control de entrada, almacenamiento y salida de información
- Análisis y gestión de registros
- Planificación de la capacidad del sistema
- Intercambio físico de información
- Intercambio lógico de información
- Autorización de salida de material y/o información
- Copias de respaldo y restauración

Control de accesos

- Identificación y autenticación de usuarios
- Restricción de acceso a la información
- Control de acceso a la red
- Control de acceso al sistema operativo
- Control de acceso lógico a la información
- Gestión de contraseñas
- Gestión remota de equipos

Desarrollo y mantenimiento de sistemas

- Control del paso de desarrollo a pruebas
- Control de paso de pruebas a producción
- Control de cambios de sistema operativo
- Control de cambios en el *software*
- Selección, control y aprobación de *software* externo

Control del diseño de aplicaciones

Especificación de los requerimientos de seguridad

Control de *software* en operación

Gestión de continuidad del negocio

Gestión de la continuidad de negocio

Mantenimiento y evaluación de los planes de continuidad

Conformidad

Identificación de la legislación aplicable

Revisión de cumplimiento de legislación

Auditorías internas

4.1.2. 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.

4.1.3. 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 SP 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.

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.

4.1.4. Referencias

- ISO/IEC 17799:2005, *"Information technology -- Code of practice for information security management",* 2005.
- UNE 71502:2004, *"Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI)",* 2004.
- UNE-ISO/IEC 17799:2002, *"Tecnología de la Información. Código de Buenas Prácticas de la Gestión de la Seguridad de la Información",* 2002.
- ISO Guide 72:2001, *"Guidelines for the justification and development of management system standards",* 2001.
- European Co-Operation for Accreditation, "Guidelines for the Accreditation of Bodies Operating Certification / Registration of Information Security Management Systems", *EA-7/03, February 2000.*

4.2. 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

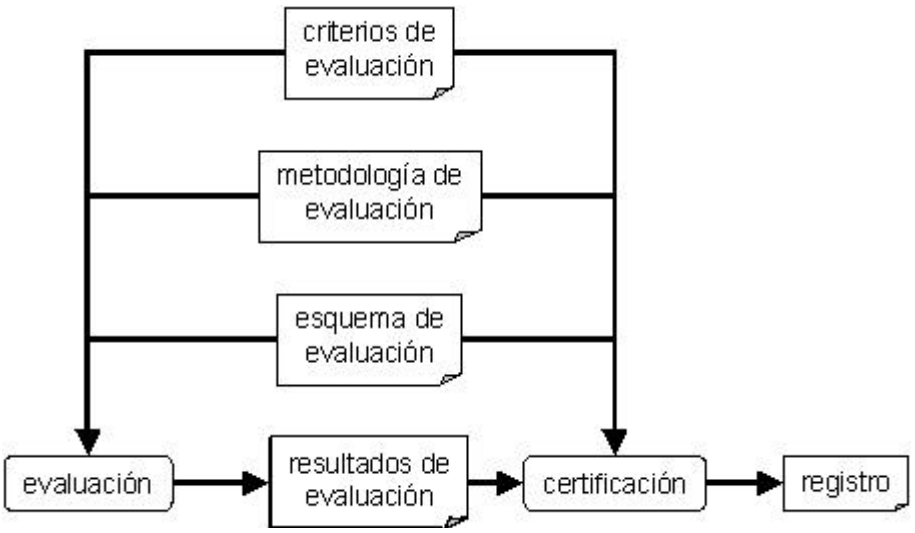
1. definir las funciones de seguridad[48] de los productos y sistemas (en tecnologías de la información) y
2. determinar los criterios para evaluar [la calidad] de dichas funciones.

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"[49].

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[50] que fije el marco administrativo y regulatorio bajo el que se realiza la certificación



48 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.

49 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.

50 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/ .

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[51]:

EAL0: sin garantías

EAL1: probado funcionalmente

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+[52].

4.2.1. 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 realiza-

51 **EAL:** *Evaluation Assurance Level*

52 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.

das en cualquier parte

Todos estos participantes convergen sobre un objeto a evaluar denominado **TOE** *(Target Of Evaluation)*, que no es sino 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.

4.2.2. 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 denomina **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[53].

Los ST, dado su carácter específico, cubren un producto concreto. Suelen ser preparados por los propios fabricantes que de esta manera formalizan su oferta[54].

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***

1. Introduction
2. TOE description
3. Security environment
  1. assumptions
  2. threats
  3. organizational security policies
4. Security objectives
  1. for the TOE
  2. for the environment
5. Security requirements
  1. for the environment
  2. TOE functional requirements
  3. TOE assurance requirements
6. Rationale
	1. Introduction
	2. TOE description
	3. Security environment
	  1. assumptions
	  2. threats
	  3. organizational security policies
	4. Security objectives
	  1. for the TOE
	  2. for the environment
	5. Security requirements
	  1. for the environment
	  2. TOE functional requirements
	  3. TOE assurance requirements
	6. TOE summary specification
	7. PP claims
	  • PP reference
	  • PP tailoring
	  • PP additions
	8. Rationale

53 Un ejemplo típico de PP podría ser aquel que fija las características de seguridad que se deben exigir a un cortafuegos.

54 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.

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.

4.2.3. 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

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	ASE: ST evaluation
FPR: Privacy	APE: PP evaluation
FPT: Protection of the TOE security functions	ATE: Tests
FRU: Resource utilisation	AVA: Vulnerability assessment
FTA: TOE access	AMA: Maintenance of assurance
FTP: Trusted path/channels	

4.2.4. 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.

4.2.5. 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.

4.2.6. Referencias

- "Arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes en el campo de la Seguridad de las Tecnologías de la Información", Mayo, 2000.
- CC, "Common Criteria for Information Technology Security Evaluation", Versión 2.2, 2004.
  - Part 1: Introduction and general model
  - Part 2: Security functional requirements
  - Part 3: Security assurance requirements

  La versión 2.1, de 1999, es norma ISO/IEC 15408, partes -1, -2 y -3.
- ITSEC, European Commission, "Information Technology Security Evaluation Criteria", versión 1.2, 1991.
- TCSEC, Department of Defensa, "Trusted Computer System Evaluation Criteria", DOD 5200.28-STD, Dec. 1985.

Apéndice 5. Herramientas

La realización de un proyecto AGR 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 a los proyectos AGR 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[55]. 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 de los programas. 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

55 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.

capítulo 5 del "Catálogo de Elementos".

- 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

5.1. 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 está completamente desarrollada en Java, pudiendo emplearse sobre cualquier plataforma que soporte este entorno de programación, sin depender de licencias de productos de terceras partes. El resultado es una aplicación gráfica monopuesto.

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 programas 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:

- Criterios de Seguridad, normalización y conservación

- UNE-ISO/IEC 17799:2002: sistemas de gestión de la seguridad
- RD 994/1999: datos de carácter personal

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.

5.2. Referencias

CARVER

"Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability", National Infrastructure Institute's Center for Infrastructure Expertise, USA.

COBRA

"Security Risk Analysis & Assessment, and ISO 17799 / BS7799 Compliance", C&A Systems Security Ltd, UK.

CRAMM

"CCTA Risk Analysis and Management Method". Insight Consulting. UK.

The CRAMM Risk Analysis and Management Method is owned, administered and maintained by the Security Service on behalf of the UK Government.

EBIOS

"Méthode pour l'Expression des Besoins et l'Identification des Objectifs de Sécurité". Service Central de la Sécurité des Systèmes d'Information. France.

RIS2K

Soporte de Magerit v1.0. Ministerio de Administraciones Públicas. España.

PILAR

"Procedimiento Informático-Lógico para el Análisis de Riesgos". Centro Nacional de Inteligencia. Ministerio de Defensa. España.

Apéndice 6. Evolución de Magerit versión 1.0

La versión 1.0 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. Esta segunda versión no parte con ánimo de ruptura, sino que se plantea con ánimo de mejora, adaptándola al tiempo presente e incorporando la experiencia de estos años.

Las siguientes secciones servirán de guía dentro de la versión 2 a los profesionales familiarizados con la versión 1.

6.1. Libro I. Guía de aproximación a la seguridad de los sistemas de información

En estos años la consciencia de la necesidad de la seguridad ha avanzado enormemente y ya no se ha considerado necesario una aproximación tan general. La introducción es más sucinta y toda la guía se centra en el análisis y gestión de riesgos.

La Guía de Aproximación señalaba una serie de salvaguardas, denominadas mínimas, que siguen vigentes:

1. Documentación de la política de seguridad
2. Asignación de funciones y responsabilidades
3. Responsabilidades del usuario en el acceso
4. Proceso de selección
5. Comportamiento ante incidentes
6. Controles físicos de seguridad
7. Seguridad del equipamiento
8. Cumplimiento de obligaciones jurídicas
9. Protección, transporte y destrucción
10. Gestión externa de servicios

Todos ellos recogidos en el catálogo de salvaguardas que se incluye en el "Catálogo de Elementos". Esta guía no pretende en cambio extenderse en estas salvaguardas, sino que prefiere referir al lector a la abundante bibliografía disponible, tanto técnica como de organismos internacionales de normalización.

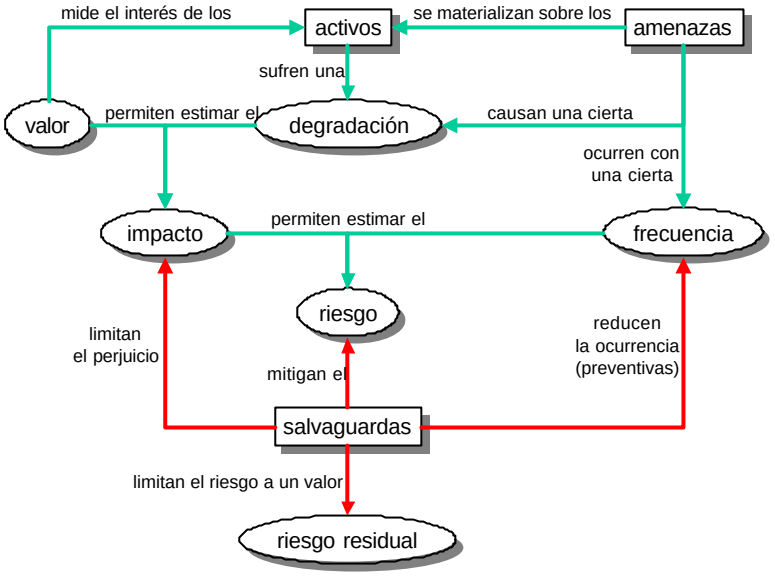
6.2. Libro II. Guía de procedimientos

El submodelo de elementos se respeta en su mayor parte, aunque se evita la voz submodelo en beneficio de una terminología más directa.

El término “vulnerabilidad” (de los activos frente a las amenazas), origen de algunas confusiones, se ha sustituido por una denominación genérica de “valoración de las amenazas” que, como antes, se traduce en dos medidas: frecuencia de ocurrencia y degradación del activo.

El concepto de impacto recibe un trato de primer rango, paralelo al de riesgo.

Los tipos de activos han merecido capítulo íntegro en el “Catálogo de Elementos”. En particular se recomienda no introducir como activos los valores intangibles de la Organización que se incorporarán al modelo como criterios de valoración (también en capítulo íntegro en el “Catálogo de Elementos”)



El submodelo de procesos se ha redenominado “aproximación formal”. Las etapas de la versión 1.0 han evolucionado a procesos en esta versión 2.

La Etapa 1, “Planificación del análisis y gestión de riesgos”, se reproduce en el proceso P1, manteniendo la estructura de actividades y tareas.

La Etapa 2, “Análisis de riesgos”, se ha reordenado en el proceso P2, con una estructuración más sistemática. Es explícito el análisis de las salvaguardas existentes. Se eleva la medida de impacto de mero paso intermedio a resultado final. Se formalizan los informes emitidos.

De la Etapa 3, “Gestión del riesgo”, la primera tarea, “Interpretación del riesgo”, pasa a ser el colofón del proceso P2, diferenciándola de la tarea de “Calificación de los riesgos” que si es parte del proceso P3.

Las etapas E3, “Gestión del riesgo”, y E4, “Selección de salvaguardas” se han condensado en el proceso P3 que se vertebra alrededor de la generación de un “Plan de Seguridad”, reconociendo que la selección e implantación de mecanismos de seguridad es frecuentemente objeto de proyectos de envergadura que conviene singularizar dentro de un marco estratégico que garantice la unidad de objetivo.

Globalmente, el proceso P2 se convierte en subsidiario del proceso P3, que recurrirá a aquel para todos los replanteamiento evolutivos; o sea, recálculo de los valores residuales de impacto y riesgo.

6.3. Libro III. Guía de técnicas

Se ha aligerado notablemente, manteniéndose los procesos Delphi de valoración en escenarios de incertidumbre, las técnicas gráficas y los modelos de cálculo mediante tablas y algoritmos, que se exponen con más detalle por ser técnicas específicas de los proyectos de análisis y gestión de riesgos.

Se presentan como libro anejo.

6.4. Libro IV. Guía para desarrolladores de aplicaciones

El paso de Métrica v2.1 a Métrica v3.0 ha supuesto una completa revisión de este punto. Aquí aparece en el capítulo de “Desarrollo de Sistemas Informáticos”, enfatizando primero el desarrollo de aplicaciones aisladas y luego el proceso de desarrollo de sistemas de información completos.

6.5. Libro V. Guía para responsables del dominio protegible

Toda esta información se ha distribuido en la nueva estructuración. Hay partes en la aproximación informal, en el método formal, en los consejos prácticos y en el "Catálogo de Elementos".

6.6. Libro VI. Arquitectura de la información y especificaciones de la interfaz para el intercambio de datos

Se presentaba un modelo de datos orientado a una herramienta, lo que se ha considerado excesivo detalle para una guía metodológica.

Lo que si se incluye en esta nueva versión es una serie de especificaciones XML para el intercambio de información. Esta guía incluye la estructura para compartir modelos de valor (activos) y el "Catálogo de Elementos" incluye estructuras para compartir otros tipos de información.

6.7. Libro VII. Referencia de normas legales y técnicas

Actualizada, pasa al apéndice 3 de esta guía.

Apéndice 7. Caso práctico

A título de ejemplo, este apéndice analiza el caso de una unidad administrativa que utiliza sistemas de información propios y de terceros para sus tareas internas y para prestar servicios de atención a los ciudadanos (administración electrónica).

El ejemplo sólo pretende ser ilustrativo, sin que el lector deba derivar mayores consecuencias o conclusión alguna de obligado cumplimiento. Incluso ante los mismos impactos y riesgos, las soluciones pueden ser diferentes, sin poder extrapolarse ciegamente de una a otra circunstancia. En particular hay que destacar el papel de la Dirección de la Organización como último punto de decisión respecto de qué política adoptar para mantener impactos y riesgos bajo control.

Buena parte del texto que sigue presenta la situación en palabras “normales”, tal y como puede llegarle al equipo de trabajo a lo largo de las entrevistas. Es la misión de este equipo traducir el conocimiento adquirido a los términos formales definidos por esta metodología.

7.1. La historia

La unidad objeto de estudio no es de nueva creación, sino que lleva años tramitando expedientes de forma local, antes manualmente, ahora por medio de un sistema informático propio. A este sistema informático se le ha añadido recientemente una conexión a un archivo central que funciona como “memoria histórica”: permite recuperar datos y conservar los expedientes cerrados. La última novedad consiste en ofrecer un servicio propio de la administración electrónica, en el que los usuarios pueden realizar sus tramitaciones vía web, usando su NIF como identificación, mas una contraseña personal. El mismo sistema de tramitación es usado localmente por un funcionario que atiende a los ciudadanos que se personan en las dependencias de la unidad.

El responsable del proyecto de administración electrónica, alarmado por las noticias aparecidas en los medios sobre la inseguridad de Internet, y sabiendo que un fallo en el servicio conllevaría un serio daño a la imagen de su unidad, asume el papel de promotor. En este papel escribe un informe interno[56], dirigido al director de la unidad, en el que da cuenta de

- los medios informáticos con que se está trabajando y los que se van a instalar
- las incidencias acaecidas desde que la unidad existe
- las incertidumbres que le causa el uso de Internet para la prestación del servicio

En base a dicho informe argumenta la conveniencia de lanzar un proyecto AGR.

La dirección, convencida de la necesidad de tomar medidas antes de que ocurra una desgracia, crea un comité de seguimiento formado por los responsables de los servicios involucrados: atención a usuarios, asesoría jurídica, servicios informáticos y seguridad física.

Se determina que el alcance del proyecto (actividad A1.2) será el servicio de tramitación electrónica, presencial y remoto. También se estudiará la seguridad de la información que se maneja: expedientes. Respecto del equipamiento, se analizarán equipos y redes de comunicaciones. Se toma la decisión de dejar fuera del estudio elementos que pudieran ser relevantes en un análisis más detallado como pudieran ser los datos de identificación y autenticación de los usuarios de los sistemas, las áreas de trabajo del personal que los maneja, la sala de equipos (centro de proceso de datos) y las personas relacionadas con el proceso. Esta previsto lanzar un futuro proyecto AGR más detallado que profundice en dichos aspectos.

Explícitamente se excluirá la evaluación de la seguridad de los servicios remotos que se emplean. El análisis es local, circunscrito a la unidad que nos ocupa. Dichos servicios remotos se consi de-

56 Como es habitual, en estas fases iniciales el proyecto no esté formalizado; no obstante, se está realizando el “Informe Preliminar” resultado de la actividad “A1.1. Estudio de oportunidad”.

ran, a efectos de este análisis, “de calidad suficiente”.

El lanzamiento del proyecto (actividad A1.4) incluye una reunión de la dirección con el comité de seguimiento en la que se exponen los puntos principales del análisis somero realizado por el promotor que queda habilitado como director del proyecto AGR en el que participaran dos personas de su equipo de desarrollo junto con un contrato de asesoría establecido con una empresa consultora externa. Uno de los miembros del equipo interno tendrá un perfil técnico: ingeniero de sistemas. A la consultora externa se le exige identificar nominalmente a las personas que van a participar y firmar un acuerdo de confidencialidad.

El proyecto se anuncia internamente mediante comunicación general a todo el personal de la unidad y notificación personal a aquellas personas que se verán directamente afectadas. En estas comunicaciones se identifican las personas responsables del proyecto.

7.2. Proceso P2: Análisis de riesgos

La fase de análisis de riesgos arranca con una serie de entrevistas a los responsables designados por el comité de seguimiento, entrevistas en las que participan

- la persona de enlace, como introductor
- el personal de la consultora externa como director de la entrevista
- el personal propio como secretario: acta de la reunión y recopilación de datos

Se identifica un servicio básico a usuarios externos: el de tramitación.

Servicio de tramitación

El servicio de tramitación se presta por medio de una aplicación informática desarrollada en el pasado sobre una base de datos. A esta aplicación se accede a través de una identificación local del usuario que controla sus privilegios de acceso. En la faceta de tramitación presencial, es la persona que está atendiendo al usuario final la que se identifica frente al sistema. En el caso de la tramitación remota, a la aplicación se accede con una identificación de usuario virtual.

Toda la tramitación incluye una fase de solicitud (y entrada de datos) y una fase de respuesta (y entrega de datos). El usuario realiza sus solicitud y espera una notificación para recoger la respuesta. La notificación es por correo, certificado en el caso de tramitación presencial, y electrónico en el caso de tramitación electrónica.

Iniciar una tramitación supone abrir un expediente que se almacena localmente en la oficina. También supone recabar una serie de datos del archivo central de información, datos que se copian localmente. Al cierre del expediente, los datos y un informe de las actuaciones realizadas se remiten al archivo central para su custodia, eliminándose la información de los equipos locales.

El personal de la unidad se identifica por medio de su cuenta de usuario, mientras que los usuarios remotos se identifican por su NIF. En ambos casos el sistema requiere una contraseña para autenticarlos.

Por último, hay que destacar el papel que presta la mensajería electrónica en todo el proceso de tramitación, usado tanto como medio interno de comunicación entre el personal, y como mecanismo de notificación a los usuarios externos. Como norma, no se debe emplear el correo como transporte de documentos; estos siempre serán servidos por medio de accesos web.

Servicio de archivo central

En forma de intranet, se presta un servicio centralizado de archivo y recuperación de documentos. Los usuarios acceden por medio de una interfaz web local, que se conecta por medio de una red privada virtual con el servidor remoto, identificándose por medio de su NIF. Este servicio sólo está disponible para el personal de la unidad y para el empleado virtual que presta el servicio de trami-

tación remota.

Equipamiento informático

La unidad dispone de varios equipos personales de tipo PC situados dentro de los locales. Estos equipos disponen de un navegador web, de un cliente de correo electrónico sin almacenamiento local de los mensajes y un paquete ofimático estándar (procesador de textos y hoja de cálculo).

Existe una capacidad de almacenamiento local de información en el disco del PC, del que no se realizan copias de seguridad; es más, existe un procedimiento de instalación / actualización que borra el disco local y reinstala el sistema íntegro.

Los equipos no disponen de unidades de disco removible de ningún tipo: disquetes, CD, DVD, USB, etc.

Se dispone de un servidor de tamaño medio, de propósito general, dedicado a las tareas de:

- servidor de ficheros
- servidor de mensajería electrónica, con almacenamiento local y acceso vía web
- servidor de bases de datos: expedientes en curso e identificación de usuarios
- servidor web para la tramitación remota y para la intranet local

Comunicaciones

Se dispone de una red de área local que cubre las dependencias de trabajo y la sala de equipos. Está explícitamente prohibida la instalación de módems de acceso remoto y redes inalámbricas, existiendo un procedimiento rutinario de inspección.

Existe una conexión a Internet, de ADSL, contratada a un operador comercial. Sobre este enlace se prestan múltiples servicios

- servicio (propio) de tramitación remota
- servicio de correo electrónico (como parte del servicio de tramitación remota)
- servicio (propio) de acceso a información
- red privada virtual con el archivo central

La conexión a Internet se realiza única y exclusivamente a través de un cortafuegos que limita las comunicaciones a nivel de red, permitiendo únicamente:

- el intercambio de correo electrónico con el servidor de correo
- el intercambio web con el servidor web

La red privada virtual con el archivo central utiliza una aplicación informática *software*. La red se establece al inicio de la jornada, cortándose automáticamente a la hora de cierre. En el establecimiento los equipos terminales se reconocen mutuamente y establecen una clave de sesión para la jornada. No hay intervención de ningún operador local.

Hay una sensación de que muchos servicios dependen de la conexión a Internet. Además, en el pasado ha habido incidencias tales como cortes de servicio debidos a obras municipales y a una deficiente prestación del servicio por parte del proveedor. Por todo ello:

1. se ha establecido un contrato de servicio que establece un cierto nivel de calidad, por encima del cual el operador debe abonar unas indemnizaciones pactadas de antemano en proporción al periodo de interrupción o a la lentitud (insuficiente volumen de datos transmitidos en periodos determinados de tiempo) del enlace.
2. se ha contratado con otro proveedor un enlace digital (RDSI) de respaldo, enlace que habitualmente no está establecido, pero que se activa automáticamente cuando el enlace ADSL

se interrumpe durante más de 10 minutos

Durante la entrevista se descubre que estos enlaces se prestan sobre la misma acometida de red telefónica que presta los servicios de voz de la unidad.

Seguridad física

El personal trabaja en los locales de la unidad, principalmente en zonas interiores, salvo una serie de terminales en los puntos de atención al público. El acceso a las zonas interiores está limitado a las horas de oficina, quedando cerrado con llave fuera de dicho horario. En horas de oficina hay un control de entrada que identifica a los empleados y registra su hora de entrada y de salida.

La sala de equipos es simplemente una habitación interior que permanece cerrada con llave, de la que es custodio el administrador de sistemas. La sala dispone de un sistema de detección y extinción de incendios que se revisa anualmente. Esta sala dista 50 metros de la canalización de agua más cercana.

Los locales de la unidad ocupan íntegramente la planta 4ª de un edificio de oficinas de 12 plantas. Los controles de acceso son propios de la unidad, no del edificio, que es de uso compartido con otras actividades. No hay ningún control sobre qué hay en el piso de arriba o en el piso de abajo.

7.2.1. Tarea T2.1.1. Identificación de activos

Resultado de las anteriores entrevistas se determina trabajar con el siguiente conjunto de activos[57]:

[SP] Servicios al público

- [S] servicios
  - [S_T_presencial] Tramitación presencial
  - [S_T_remota] Tramitación remota
- [D] datos / información
  - [D_exp] Expedientes en curso
- [SW] aplicaciones *(software)*
  - [SW_exp] Tramitación de expedientes

[SI] Servicios internos

- [S] servicios
  - [email] Mensajería electrónica
  - [archivo] Archivo histórico central

[E] Equipamiento

- [HW] equipos informáticos *(hardware)*
  - [PC] Puestos de trabajo
  - [SRV] Servidor
  - [firewall] Cortafuegos
- [COM] redes de comunicaciones
  - [LAN] Red local
  - [ADSL] Conexión a Internet

57 La relación de activos agrupa a estos en tres capas (en negrita). La estructuración en capas es mero artilugio de ordenación de la información. En cada capa se indican qué activos hay de cara tipo. Se ha empleado la relación del “Catálogo de Elementos”, capítulo “2. Tipos de activos”.

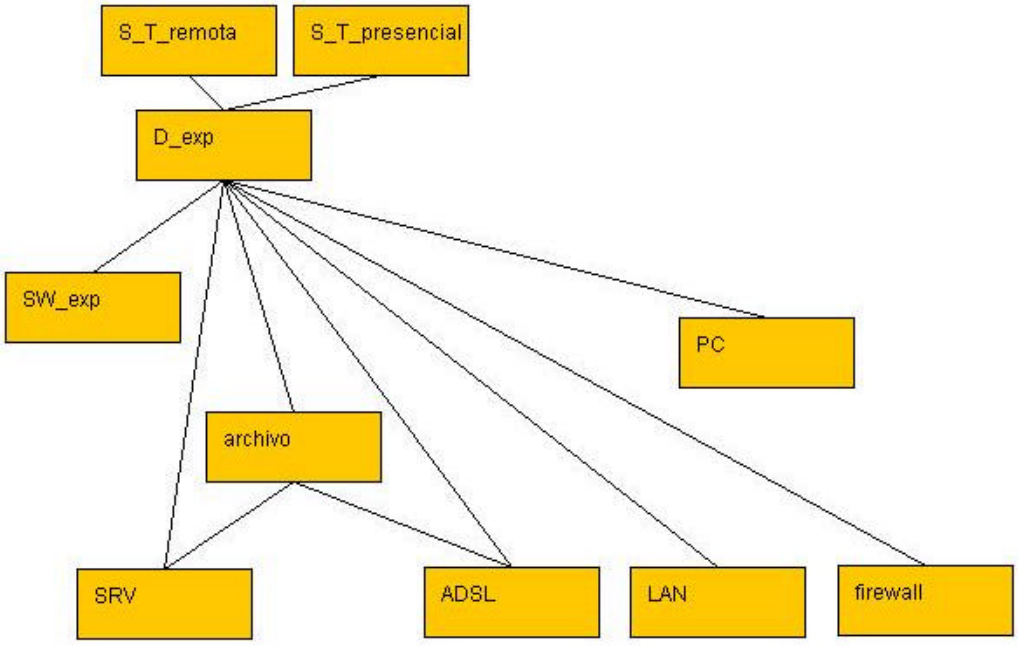
Donde se han usado los tipos de activos del capítulo 2 del "Catálogo de Elementos".

7.2.2. Tarea T2.1.2: Dependencias

Teniendo en cuenta las dependencias para operar (disponibilidad) y de almacenamiento de datos (integridad y confidencialidad), se ha determinado la siguiente matriz de dependencias entre activos:

	[S_T_presencial]	[S_T_remota]	[D_exp]	[SW_exp]	[email]	[archivo]	[PC]	[SRV]	[firewall]	[LAN]	[ADSL]
[S_T_presencial]											
[S_T_remota]											
[D_exp]											
[SW_exp]											
[email]											
[archivo]											
[PC]											
[SRV]											
[firewall]											
[LAN]											
[ADSL]											

Estas tablas se pueden representar gráficamente, cuidando de que no haya una saturación de dependencias; es decir, rara vez se puede presentar todo el sistema en un sólo gráfico. Para el caso de los datos de expedientes en curso, el gráfico de dependencias queda así:



7.2.3. Tarea T2.1.3: Valoración

La dirección está preocupada por el potencial abuso de los procesos de tramitación, algunos de los cuales pueden incluir el abono de cantidades económicas importantes, bien a beneficio de la Organización, bien a beneficio de los usuarios. La existencia de un móvil económico puede incitar al abuso tanto al personal interno como a los usuarios remotos, existiendo una especial incomodidad relacionada con la impunidad de atacantes que pudieran perpetrar ataques desde cualquier remoto punto del planeta.

También hay una especial sensibilidad relativa a la disponibilidad de los servicios. En particular hay preocupación porque no se pudiera atender una demanda presencial.

Los servicios web a usuarios externos, se consideran “emblemáticos” y se quieren cuidar con esmero para dar una imagen de modernidad, eficacia y vocación de servicio. Todo lo que suponga dar una mala imagen, bien porque no está disponible el servicio, bien porque se presta de forma errónea, bien porque las incidencias no son atendidas con presteza, ..., todas estas situaciones se quieren evitar en la medida de lo posible.

Las bases de datos locales hospedan información relativa a personas que quedarán adscritos al nivel medio dentro de la calificación de datos de carácter personal.

En vista de todo ello, se ha consensuado la siguiente valoración[58] de los activos del sistema. Sólo se han valorado explícitamente los activos superiores del árbol de dependencias, que quedan de la siguiente manera:

58 Para cada activo se indica su valoración en cada dimensión de seguridad.

Como criterios de valoración se ha empleado el capítulo “4. Criterios de valoración” del “Catálogo de Elementos”.

Como dimensiones de seguridad se ha empleado la relación del capítulo “3. Dimensiones de valoración” del “Catálogo de Elementos”.

	dimensiones de seguridad						
activo	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_T_presencial] Tramitación presencial	[5](1)			[7](2)		[6](3)	
[S_T_remota] Tramitación remota	[3](4)			[7](5)		[6](6)	
[D_exp] Expedientes en curso		[5](7)	[6](8)		[5](9)		[5](10)

Donde se han usado

- las dimensiones de seguridad descritas en el capítulo 3 del "Catálogo de Elementos" y
- los niveles y criterios de valoración descritos en el capítulo 4 del "Catálogo de Elementos"

Concretamente, los niveles se han asignado por las siguientes razones (llamadas en la tabla anterior):

(1) [5.1] Probablemente cause la interrupción de las actividades propias de la Organización

(2) [7.3] Probablemente tenga un gran impacto en otras organizaciones
[5.3] Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación

(3) [6.3] Probablemente quebrante seriamente la ley o regulaciones de protección de información personal

(4) [3.2] Probablemente cause la interrupción de las actividades propias de la Organización

(5) [7.3] Probablemente tenga un gran impacto en otras organizaciones
[6.2] Probablemente afecte gravemente a un grupo de individuos
[5.3] Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación

(6) [6.3] Probablemente quebrante seriamente la ley o regulaciones de protección de información personal

(7) [5.2] Probablemente cause un cierto impacto en otras organizaciones

(8) [6.3] Probablemente quebrante seriamente la ley o regulaciones de protección de información personal

(9) [5.3] Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación

(10) [5.3] Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación

Cuando esta valoración se propaga a través del árbol de dependencias[59], resulta la siguiente tabla de valor acumulado en cada uno de los activos del sistema (se muestra sobre fondo blanco lo que es valor propio, y sobre fondo de color lo que es acumulado):

	dimensiones de seguridad						
activo	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_T_presencial] Tramitación presencial	[5]			[7]		[6]	
[S_T_remota] Tramitación remota	[3]			[7]		[6]	

59 Ver “Guía de Técnicas” sección “2.2.1. Modelo cualitativo”.

	dimensiones de seguridad						
activo	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[D_exp] Expedientes en curso	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[SW_exp] Tramitación de expedientes	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[email] Mensajería electrónica	[5]			[7]		[6]	
[archivo] Archivo histórico central	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[PC] Puestos de trabajo	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[SRV] Servidor	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[firewall] Cortafuegos	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[LAN] Red local	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[ADSL] Conexión a Internet	[5]	[5]	[6]	[7]	[5]	[6]	[5]

En este punto se obtiene el "Modelo de Valor"[60] de la organización.

7.2.4. Actividad A2.2: Caracterización de las amenazas

Se han detectado en el pasado, en la aplicación tradicional de tramitación, intentos de abuso de privilegios por parte del personal propio, así como intentos de suplantación y engaño por parte de los usuarios del servicio que pretenden no ser quienes son, o introducen datos falsos.

Es habitual la ocurrencia de errores no intencionados en el suministro de datos, más habitual por parte de los usuarios de los servicios.

En previsión de ambos tipos de incidencias se han previsto la aprobación de los datos introducidos por una tercera persona. También se ha minimizado la cantidad de información que se introduce manualmente, primando la recuperación de información consolidada en el archivo central.

Los casos detectados de fraude se han atajado a tiempo, tomando medidas disciplinarias sobre el personal propio. Así mismo se mantiene un registro local de incidencias, tanto de personal propio como de usuarios externos, registro que se consulta regularmente introduciendo controles adicionales cuando el histórico levanta sospechas. Este registro no ha sido sometido a dictamen por parte de asesoría jurídica.

La conexión a Internet se analiza regularmente por medio de un detector de intrusión situado fuera del cortafuegos. Se aprecia una actividad continua de intentos de penetración, barriendo puertos e intentando explotar vulnerabilidades de los servicios de mensajería y web. En el caso del servicio web, en una ocasión los atacantes lograron penetrar y vaciar algunos datos del sistema de servicio. No llegaron a poder modificar la configuración, ni a acceder a las bases de datos. El incidente se detectó casualmente por el administrador (revisión rutinaria de *logs*) que bloqueó el acceso hasta haber instalado un nuevo aplicativo servidor. Desde entonces se siguen rigurosamente todos los informes de actualización de *software* en los servidores de mensajería y web.

Con todas estas consideraciones, la siguiente tabla[61] muestra las amenazas que se han considerado potencialmente más frecuentes. Nótese que hay una diferencia entre la percepción del usuario (recopilada en los párrafos anteriores) y las amenazas potenciales en el sistema. Esta diferencia se debe a la existencia de salvaguardas, que se tendrá en cuenta más adelante.

60 Ver "Apéndice 4.1. Modelo de valor" del "Catálogo de Elementos".

61 La primera columna muestra las amenazas más relevantes para el activo. La segunda columna recoge la frecuencia de ocurrencia expresada como tasa anual (incidencias por año). Las demás columnas recogen la degradación del activo expresada como porcentaje de su valor. Hay una columna por dimensión de seguridad (véase "Catálogo de Elementos", capítulo "3. Dimensiones de valoración").

		dimensiones de seguridad						
activo ***amenaza***	***fre***	***[D]***	***[I]***	***[C]***	***[A_S]***	***[A_D]***	***[T_S]***	***[T_D]***
[S_T_presencial] Tramitación presencial								
[E.1] Errores de los usuarios	100	10%						
[A.5] Suplantación de la identidad	100				100%			
[A.11] Acceso no autorizado	100				50%			
[S_T_remoto] Tramitación remota								
[E.1] Errores de los usuarios	100	10%						
[A.5] Suplantación de la identidad	100				100%			
[A.11] Acceso no autorizado	100				50%			
[D_exp] Expedientes en curso								
[E.16] Introducción de falsa información	100		1%					
[A.11] Acceso no autorizado	100		10%	50%	50%			
[SW_exp] Tramitación de expedientes			10%					
[E.8] Difusión de *software* dañino	100	10%		10%	10%	10%	10%	10%
[email] Mensajería electrónica								
[E.1] Errores de los usuarios	100	10%						
[A.5] Suplantación de la identidad	100				100%			
[A.11] Acceso no autorizado	100				10%			
[archivo] Archivo histórico central								
[E.1] Errores de los usuarios	100	10%	10%					
[A.5] Suplantación de la identidad	100		50%	50%	100%	100%		
[A.11] Acceso no autorizado	100		10%	50%	50%			

En este punto se obtiene el "Mapa de Riesgos"[62] de la organización.

7.2.5. Actividad A2.4: Estimación de impacto y riesgo

Sin tener todavía en cuenta las salvaguardas, se derivan las siguientes estimaciones de impacto y riesgo acumulado sobre los diferentes activos[63]. Sólo se muestran los impactos y riesgos más elevados.

activo	***amenaza***	***dim***	***I***	***R***
[S_T_remota] Tramitación remota	[A.5] Suplantación de la identidad	[A_S]	[7]	[13]
[S_T_presencial] Tramitación presencial	[A.5] Suplantación de la identidad	[A_S]	[7]	[13]
[archivo] Archivo histórico central	[A.5] Suplantación de la identidad	[A_S]	[7]	[13]

62 Ver "Apéndice 4.2. Mapa de riesgos" del "Catálogo de Elementos".

63 La tabla recoge en la primera columna el activo expuesto a la amenaza que aparece en la segunda columna. La tercera columna muestra la dimensión de seguridad en que el activo se vería afectado. La cuarta columna muestra el impacto y la quinta el riesgo.

Para el cálculo del impacto acumulado se sigue lo indicado en la sección "2.1.3. Paso 4: Determinación del impacto", donde se tiene en cuenta el valor acumulado sobre el activo (en la citada dimensión), la frecuencia de la amenaza y la degradación causada por la amenaza (en la citada dimensión).

Para el cálculo del riesgo acumulado se sigue lo indicado en la sección "2.1.4. Determinación del riesgo", donde se incorpora la frecuencia estimada de ocurrencia de la amenaza.

Véase también la sección "2.2.1. Modelo cualitativo" de la "Guía de Técnicas".

activo	*amenaza*	*dim*	*I*	*R*
[email] Mensajería electrónica	[A.5] Suplantación de la identidad	[A_S]	[7]	[13]
[SW_exp] Tramitación de expedientes	[A.5] Suplantación de la identidad	[A_S]	[7]	[13]
[SW_exp] Tramitación de expedientes	[A.22] Manipulación de programas	[A_S]	[7]	[11]
[SW_exp] Tramitación de expedientes	[A.8] Difusión de *software* dañino	[A_S]	[7]	[10]
[LAN] Red local	[A.5] Suplantación de la identidad	[A_S]	[7]	[8]
[ADSL] Conexión a Internet	[A.5] Suplantación de la identidad	[A_S]	[7]	[8]
[SW_exp] Tramitación de expedientes	[A.4] Manipulación de la configuración	[A_S]	[7]	[4]
[D_exp] Expedientes en curso	[A.4] Manipulación de la configuración	[A_S]	[7]	[4]
[email] Mensajería electrónica	[A.4] Manipulación de la configuración	[A_S]	[7]	[4]
[archivo] Archivo histórico central	[A.4] Manipulación de la configuración	[A_S]	[7]	[4]
[S_T_presencial] Tramitación presencial	[A.4] Manipulación de la configuración	[A_S]	[7]	[4]
[S_T_remota] Tramitación remota	[A.4] Manipulación de la configuración	[A_S]	[7]	[4]

Los mismos cálculos, en términos de impacto y riesgo repercutido[64], dan pie a la siguiente relación, centrándonos solamente en el servicio de tramitación remota:

activo inferior	*amenaza*	*D*	*I*	*R*
[SW_exp] Tramitación de expedientes	[A.5] Suplantación de la identidad	[A_S]	[7]	[13]
[email] Mensajería electrónica	[A.5] Suplantación de la identidad	[A_S]	[7]	[13]
[archivo] Archivo histórico central	[A.5] Suplantación de la identidad	[A_S]	[7]	[13]
[S_T_remota] Tramitación remota	[A.5] Suplantación de la identidad	[A_S]	[7]	[13]
[SW_exp] Tramitación de expedientes	[A.22] Manipulación de programas	[A_S]	[7]	[11]
[SW_exp] Tramitación de expedientes	[A.8] Difusión de *software* dañino	[A_S]	[7]	[10]
[LAN] Red local	[A.5] Suplantación de la identidad	[A_S]	[7]	[8]
[ADSL] Conexión a Internet	[A.5] Suplantación de la identidad	[A_S]	[7]	[8]
[SW_exp] Tramitación de expedientes	[A.4] Manipulación de la configuración	[A_S]	[7]	[4]
[S_T_remota] Tramitación remota	[A.4] Manipulación de la configuración	[A_S]	[7]	[4]
[D_exp] Expedientes en curso	[A.4] Manipulación de la configuración	[A_S]	[7]	[4]
[archivo] Archivo histórico central	[A.4] Manipulación de la configuración	[A_S]	[7]	[4]
[email] Mensajería electrónica	[A.4] Manipulación de la configuración	[A_S]	[7]	[4]

64 Para el cálculo del impacto repercutido se sigue lo indicado en la sección “2.1.3. Paso 4: Determinación del impacto”, donde se tiene en cuenta el valor propio del activo “servicio de tramitación remota” (en la citada dimensión), la frecuencia de la amenaza y la degradación causada por la amenaza sobre el activo inferior indicado en la tabla (en la citada dimensión).

Para el cálculo del riesgo repercutido se sigue lo indicado en la sección “2.1.4. Determinación del riesgo”, donde se incorpora la frecuencia estimada de ocurrencia de la amenaza sobre el activo inferior indicado.

Véase también la sección “2.2.1. Modelo cualitativo” de la “Guía de Técnicas”.

7.2.6. Actividad A2.3: Caracterización de las salvaguardas

A la hora de evaluar el estado de seguridad de la unidad bajo estudio, hay que indagar una serie de aspectos generales y una serie de aspectos específicos de cada activo. En esta indagación hay que tener en cuenta tanto la naturaleza de los activos como su valor y las amenazas a que está expuesto.

En aspectos generales hay que averiguar

- cómo se organiza la seguridad: responsables, toma de decisiones, contactos externos, etc.
- si hay una identificación de roles del personal, asociados a privilegios de acceso
- si hay hay segregación efectiva de tareas
- si existe una política de seguridad documentada y revisada periódicamente
- cómo se gestionan las incidencias
- cómo se gestionan los registros de actividad
- si existe un plan de contingencia: gestión de emergencias, continuidad y recuperación

Respecto de los servicios prestados por la Organización, hay que averiguar

- si existe normativa y procedimientos de uso, conocidos y empleados
- si hay una planificación de capacidades
- si hay mecanismos de prevención del repudio
- si hay mecanismos de prevención de ataques de denegación de servicio
- cómo se gestionan los usuarios
- qué registro queda de lo que se hace

Respecto de los datos manejados por la Organización, hay que averiguar

- si hay un inventario de ficheros, con identificación de responsable
- si existe normativa y procedimientos de uso, conocidos y empleados
- si se hacen copias de respaldo y con qué calidad
- si se han previsto mecanismos para garantizar el secreto
- si se han previsto mecanismos para garantizar la integridad
- si se han previsto mecanismos de registro de acceso

Respecto de los aplicativos en uso, hay que averiguar

- cómo se gestiona su mantenimiento
- cómo se controla su configuración, en particular de usuarios y derechos de acceso
- si se ha inspeccionado el código, especialmente frente a puertas traseras de acceso

Respecto del servicio de mensajería (email), hay que averiguar

- si existe normativa y procedimientos de uso, conocidos y empleados
- cómo se gestionan los usuarios
- cómo se controla el contenido de los mensajes y de los ficheros adjuntos
  - desde el punto de vista de fugas de información
  - desde el punto de vista de inyección de programas dañinos (por ejemplo, virus)

  - desde el punto de vista de autenticidad del origen
- cómo se asegura la disponibilidad del servicio

Respecto del servicio de archivo, hay que averiguar

- si existe normativa y procedimientos de uso, conocidos y empleados
- cómo se controla quién accede a su uso
- cómo se garantiza el secreto de los datos que transportan
- cómo se garantiza su disponibilidad

Respecto del equipamiento informático, hay que averiguar

- si existe normativa y procedimientos de uso, conocidos y empleados
- cómo se gestiona su mantenimiento
- cómo se controla su configuración, en particular de usuarios y derechos de acceso
- cómo se garantiza su disponibilidad

Respecto de las comunicaciones, hay que averiguar

- si existe normativa y procedimientos de uso, conocidos y empleados
- cómo se controla quién accede a su uso
- cómo se garantiza el secreto de los datos que transportan
- cómo se garantiza su disponibilidad

Tenga en cuenta el lector que esto es sólo un ejemplo que no pretende ser exhaustivo. Se han referenciado los aspectos más relevantes; no todos. Es especialmente de destacar la ausencia de un análisis de las instalaciones físicas y del personal, que han quedado fuera por mantener el ejemplo reducido..

Indagando se averigua que:

- Existe una política de seguridad heredada de la Organización matriz de la unidad que nos ocupa. Al ser una unidad de pequeñas dimensiones, existe un responsable único de seguridad que informa directamente a la Dirección y es el contacto frente a otras organizaciones. Además existe un procedimiento local de escalado de incidencias que puede provocar un escalado más allá de la propia unidad.
- El servidor central hospeda una tabla para controlar qué privilegios de acceso tiene cada usuario, en particular diferenciando la capacidad administrativa para dar curso a los expedientes a lo largo de su proceso. Toda la actividad se registra en un fichero al que sólo se tiene acceso el operador y que se remite diariamente al archivo central.
- Los procedimientos de trabajo con los sistemas no están escritos. Se confía en que las propias aplicaciones web adapten las actividades que se pueden realizar en cada momento según el estado del expediente en curso y los privilegios del usuario. Sí se realiza un registro de todas y cada una de las actuaciones del personal sobre los servicios web. Para el proceso manual existen una serie de impresos disponibles con instrucciones incluidas sobre cuándo usarlos, qué datos proporcionar y cómo tramitarlos.
- Una persona de la unidad tiene las funciones de operador, encargándose de todas las tareas de instalación, configuración y resolución de incidencias. Esta persona dispone de procedimientos escritos para las actividades rutinarias; pero debe improvisar en situaciones atípicas, para las que puede recurrir al soporte técnico de la Organización matriz.
- No existe ningún plan de contingencia.

- Existen contratos de mantenimiento con los suministradores de los equipos y de los programas básicos: sistema operativo, ofimática, correo y servidores web.
- Los usuarios internos son administrados por el operador, que requiere solicitud por escrito de altas, bajas y cambios. Dicha solicitud debe venir firmada por el gerente.
- Los usuarios externos se dan de alta personalmente, indicando su NIF. Para recabar su contraseña deben personarse físicamente la primera vez. Una vez registrados no se hace un seguimiento de las cuentas, que duran indefinidamente.
- Tanto los usuarios internos como externos se identifican por medio de un nombre de usuario y una contraseña. Todos reciben unas someras instrucciones sobre cómo elegir contraseñas; pero no se verifica que las cumplan, ni que las contraseñas se cambien regularmente.
- Se ha realizado recientemente una auditoría de los datos de carácter personal, habiendo sido superada plenamente en todos los aspectos.
- Los datos procedentes del archivo central se consideran correctos. Los datos introducidos por los ciudadanos deben ser validados por el personal de la unidad. Los datos introducidos por los usuarios internos deben ser validados por un segundo usuario; normalmente los introduce una persona y los valida quien firma el progreso del expediente.
- El aplicativo de tramitación de expedientes es suministrado por la Organización matriz, considerándose “de calidad suficiente”.
- Se ha instalado un sistema anti-virus y se ha contratado un servicio de mantenimiento 24x7 a través de la Organización matriz con un tiempo de respuesta inferior a 1 día.
- El servicio de mensajería se centraliza en el servidor de forma que el acceso de los usuarios internos es a través de una interfaz web. Sistemáticamente se elimina todo tipo de anexo en el correo saliente y se analiza con el anti-virus los anexos del correo entrante.
- El servicio de archivo central es un servicio prestado externamente que se va a considerar “de calidad suficiente”. En un análisis más detallado habrá que entrar en la prestación de este servicio.
- Las comunicación a Internet responde a un contrato ADSL estándar, no habiéndose realizado un estudio de necesidades, ni estar prevista ninguna cláusula contractual de calidad de servicio o ampliación de capacidad.
- La conexión al archivo central se realiza sobre Internet, usando una red privada virtual que se establece entre los extremos. Esta red está configurada y mantenida desde el archivo central, sin tener capacidad local de configuración alguna. Se considerará “de calidad suficiente”.

En este punto se obtiene la “Evaluación de Salvaguardas”[65] de la organización.

Insuficiencias detectadas

Cotejados los descubrimientos, se aprecian las siguientes insuficiencias:

- La segregación de tareas es adecuada excepto en el caso del administrador de sistemas que dispone de amplia capacidad de acceso a todos los sistemas, instalaciones y configuraciones.
- Debería existir un plan de contingencia: gestión de emergencias, plan de continuidad y plan de recuperación.
- Deberían existir procedimientos escritos para todas las tareas ordinarias y para las incidencias previsibles, incluyendo todas las que se hayan dado en el pasado.

65 Ver “Apéndice 4.3. Evaluación de salvaguardas” del “Catálogo de Elementos”.

- Debería realizarse un estudio del uso de la conexión ADSL y su evolución para poder planificar una ampliación de capacidad. También debería establecerse con el proveedor un acuerdo de calidad de servicio que incluyera un canal alternativo de comunicación en caso de caída.
- Deberían establecerse mecanismos para detectar y reaccionar a un ataque de denegación de servicio.
- Debería hacerse un seguimiento de las cuentas de los usuarios externos, al menos detectando largos periodos de inactividad, intentos de penetración y comportamientos anómalos en general.
- El uso de contraseñas como mecanismo de autenticación se considera "débil", recomendándose el uso de tarjetas criptográficas de identificación.

En este punto se obtiene el "Informe de Insuficiencias"[66] de la organización.

7.2.7. Actividad A2.4: Estimación del estado de riesgo

Conocidos el "Modelo de Valor", el "Mapa de Riesgos" y la "Evaluación de Salvaguardas" se procede a la estimación del los indicadores de impacto y riesgo, tanto acumulados (sobre los activos inferiores) como repercutidos (sobre los activos superiores).

Impacto residual acumulado

Evaluado el impacto, arroja los siguientes indicadores[67] (la columna D indica la dimensión de seguridad afectada; las columnas I e IR recogen el impacto y el impacto residual):

activo	*amenaza*	*D*	*I*	*IR*
[S_T_remota] Tramitación remota	[A.5] Suplantación de la identidad	[A_S]	[7]	[3]
[S_T_presencial] Tramitación presencial	[A.5] Suplantación de la identidad	[A_S]	[7]	[3]
[archivo] Archivo histórico central	[A.5] Suplantación de la identidad	[A_S]	[7]	[3]
[email] Mensajería electrónica	[A.5] Suplantación de la identidad	[A_S]	[7]	[3]
[SW_exp] Tramitación de expedientes	[A.5] Suplantación de la identidad	[A_S]	[7]	[2]
[SW_exp] Tramitación de expedientes	[A.22] Manipulación de programas	[A_S]	[7]	[2]
[SW_exp] Tramitación de expedientes	[A.8] Difusión de *software* dañino	[A_S]	[7]	[2]
[LAN] Red local	[A.5] Suplantación de la identidad	[A_S]	[7]	[1]
[ADSL] Conexión a Internet	[A.5] Suplantación de la identidad	[A_S]	[7]	[1]
[SW_exp] Tramitación de expedientes	[A.4] Manipulación de la configuración	[A_S]	[7]	[2]
[D_exp] Expedientes en curso	[A.4] Manipulación de la configuración	[A_S]	[7]	[0]
[email] Mensajería electrónica	[A.4] Manipulación de la configuración	[A_S]	[7]	[3]
[archivo] Archivo histórico central	[A.4] Manipulación de la configuración	[A_S]	[7]	[3]

66 Ver "Apéndice 4.5. Informe de insuficiencias" del "Catálogo de Elementos".

67 La primera columna recoge el activo amenazado. La segunda, la amenaza. La tercera indica en qué dimensión de seguridad se vería afectado. La cuarta columna indica el impacto acumulado sobre el activo si no hubiera salvaguardas. La quinta columna muestra el impacto residual calculado teniendo en cuenta las salvaguardas presentes.

Para el cálculo del impacto residual se sigue lo indicado en la sección "2.1.6. Revisión del paso 4: impacto residual. Véase también la sección "2.2.1. Modelo cualitativo" de la "Guía de Técnicas".

activo	amenaza	D	I	IR
[S_T_presencial] Tramitación presencial	[A.4] Manipulación de la configuración	[A_S]	[7]	[3]
[S_T_remota] Tramitación remota	[A.4] Manipulación de la configuración	[A_S]	[7]	[3]

Riesgo residual

Evaluado el riesgo, arroja los siguientes indicadores[68] (la columna D indica la dimensión de seguridad afectada; las columnas R y RR recogen el riesgo y el riesgo residual):

activo	amenaza	D	R	RR
[S_T_remota] Tramitación remota	[A.5] Suplantación de la identidad	[A_S]	[13]	[6]
[S_T_presencial] Tramitación presencial	[A.5] Suplantación de la identidad	[A_S]	[13]	[6]
[archivo] Archivo histórico central	[A.5] Suplantación de la identidad	[A_S]	[13]	[6]
[email] Mensajería electrónica	[A.5] Suplantación de la identidad	[A_S]	[13]	[6]
[SW_exp] Tramitación de expedientes	[A.5] Suplantación de la identidad	[A_S]	[13]	[6]
[SW_exp] Tramitación de expedientes	[A.22] Manipulación de programas	[A_S]	[11]	[4]
[SW_exp] Tramitación de expedientes	[A.8] Difusión de *software* dañino	[A_S]	[10]	[3]
[LAN] Red local	[A.5] Suplantación de la identidad	[A_S]	[8]	[1]
[ADSL] Conexión a Internet	[A.5] Suplantación de la identidad	[A_S]	[8]	[1]
[SW_exp] Tramitación de expedientes	[A.4] Manipulación de la configuración	[A_S]	[4]	[0]
[D_exp] Expedientes en curso	[A.4] Manipulación de la configuración	[A_S]	[3]	[0]
[email] Mensajería electrónica	[A.4] Manipulación de la configuración	[A_S]	[4]	[0]
[archivo] Archivo histórico central	[A.4] Manipulación de la configuración	[A_S]	[4]	[0]
[S_T_presencial] Tramitación presencial	[A.4] Manipulación de la configuración	[A_S]	[4]	[0]
[S_T_remota] Tramitación remota	[A.4] Manipulación de la configuración	[A_S]	[4]	[0]

Impacto residual repercutido

Los impactos anteriormente recopilados sobre el servicio “[S_T_remota] Tramitación remota” evolucionan de la siguiente forma:

activo inferior	amenaza	D	I	IR
[SW_exp] Tramitación de expedientes	[A.5] Suplantación de la identidad	[A_S]	[7]	[2]
[email] Mensajería electrónica	[A.5] Suplantación de la identidad	[A_S]	[7]	[3]

68 La primera columna recoge el activo amenazado. La segunda, la amenaza. La tercera indica en qué dimensión de seguridad se vería afectado. La cuarta columna indica el riesgo acumulado sobre el activo si no hubiera salvaguardas. La quinta columna muestra el riesgo residual calculado teniendo en cuenta las salvaguardas presentes.

Para el cálculo del riesgo residual se sigue lo indicado en la sección “2.1.7. Revisión del paso 5: riesgo residual. Véase también la sección “2.2.1. Modelo cualitativo” de la “Guía de Técnicas”.

activo inferior	*amenaza*	*D*	*I*	*IR*
[archivo] Archivo histórico central	[A.5] Suplantación de la identidad	[A_S]	[7]	[3]
[S_T_remota] Tramitación remota	[A.5] Suplantación de la identidad	[A_S]	[7]	[3]
[SW_exp] Tramitación de expedientes	[A.22] Manipulación de programas	[A_S]	[7]	[2]
[SW_exp] Tramitación de expedientes	[A.8] Difusión de *software* dañino	[A_S]	[7]	[2]
[LAN] Red local	[A.5] Suplantación de la identidad	[A_S]	[7]	[1]
[ADSL] Conexión a Internet	[A.5] Suplantación de la identidad	[A_S]	[7]	[1]
[SW_exp] Tramitación de expedientes	[A.4] Manipulación de la configuración	[A_S]	[7]	[2]
[S_T_remota] Tramitación remota	[A.4] Manipulación de la configuración	[A_S]	[7]	[3]
[D_exp] Expedientes en curso	[A.4] Manipulación de la configuración	[A_S]	[7]	[0]
[archivo] Archivo histórico central	[A.4] Manipulación de la configuración	[A_S]	[7]	[3]
[email] Mensajería electrónica	[A.4] Manipulación de la configuración	[A_S]	[7]	[3]

Riesgo residual repercutido

Los riesgos anteriormente recopilados sobre el servicio “[S_T_remota] Tramitación remota” evolucionan de la siguiente forma:

activo inferior	*amenaza*	*D*	*R*	*RR*
[SW_exp] Tramitación de expedientes	[A.5] Suplantación de la identidad	[A_S]	[13]	[6]
[email] Mensajería electrónica	[A.5] Suplantación de la identidad	[A_S]	[13]	[6]
[archivo] Archivo histórico central	[A.5] Suplantación de la identidad	[A_S]	[13]	[6]
[S_T_remota] Tramitación remota	[A.5] Suplantación de la identidad	[A_S]	[13]	[6]
[SW_exp] Tramitación de expedientes	[A.22] Manipulación de programas	[A_S]	[11]	[4]
[SW_exp] Tramitación de expedientes	[A.8] Difusión de *software* dañino	[A_S]	[10]	[3]
[LAN] Red local	[A.5] Suplantación de la identidad	[A_S]	[8]	[1]
[ADSL] Conexión a Internet	[A.5] Suplantación de la identidad	[A_S]	[8]	[0]
[SW_exp] Tramitación de expedientes	[A.4] Manipulación de la configuración	[A_S]	[4]	[0]
[S_T_remota] Tramitación remota	[A.4] Manipulación de la configuración	[A_S]	[4]	[0]
[D_exp] Expedientes en curso	[A.4] Manipulación de la configuración	[A_S]	[4]	[0]
[archivo] Archivo histórico central	[A.4] Manipulación de la configuración	[A_S]	[4]	[0]
[email] Mensajería electrónica	[A.4] Manipulación de la configuración	[A_S]	[4]	[0]

En este punto se obtiene el “Estado de Riesgo”[69] de la organización. Este “Estado de Riesgo” viene documentado por el informe de “Evaluación de Salvaguardas” que recoge de despliegue actual de seguridad, y el “Informe de Insuficiencias”[70] que recoge las debilidades descubiertas.

69 Ver “Apéndice 4.4. Estado de riesgo” del “Catálogo de Elementos”.
70 Ver “Apéndice 4.5. Informe de insuficiencias” del “Catálogo de Elementos”.

7.3. Proceso P3: Gestión de riesgos

7.3.1. Actividad A3.1: Toma de decisiones

Vistos los indicadores de riesgo residual y las insuficiencias de la unidad, la Dirección decide clasificar en los siguientes niveles los programas de seguridad a desarrollar:

De carácter urgente
P1: Desarrollar un plan de contingencia P2: Monitorizar y gestionar las cuentas de usuarios externos
Consideraciones importantes
P3.1: Documentar todos los procedimientos de trabajo, revisando los actuales y añadiendo los que falten P3.2: Segregar las funciones del administrador de sistemas
Temas a considerar en el futuro
• Uso de tarjetas de identificación • Relaciones con el proveedor de comunicaciones para garantizar la calidad del servicio • Contratación de un servicio alternativo de comunicaciones • Medidas frente a ataques de denegación de servicio

7.3.2. Actividad A3.2: Plan de seguridad

Todas las consideraciones anteriores hay que plasmarlas en un “Plan de Seguridad”[71] que organiza las actividades de forma planificada y gestionada.

El desarrollo del plan de contingencia (programa P1) se traduce en un proyecto específico para el que

1. este año se realizará una estimación de costes del proyecto y una solicitud de propuestas que se completará con la adjudicación a un contratista externo
2. a la vista de la oferta ganadora se destinarán fondos el año que viene para la realización del plan; en esta realización se incluirán todas las tareas administrativas (dimensionado, selección de soluciones, procedimientos, etc.), exceptuándose las posibles ejecuciones de obra civil o contratación de servicios externalizados de continuidad, que serán objeto de futuras licitaciones

Para la monitorización de cuentas (programa P2) se lanza un proyecto para el desarrollo de un sistema de gestión de cuentas que incluya la detección de intrusiones y el lanzamiento de alarmas. Se estima que este proyecto se puede lanzar inmediatamente y que su duración será de un año.

Para la documentación de todos los procedimientos (programa P3.1) se recurrirá a una ampliación del contrato de consultoría y asesoramiento que la Organización matriz tiene actualmente. En esta ampliación, consultores externos se encargarán de recabar la información pertinente, completando los manuales actuales. Esta tarea no se acometerá hasta el próximo ejercicio. En la elaboración de procedimientos se definirán las tareas específicas de un operador (local) y un administrador (remoto) de forma que se alcance el objetivo del programa P3.2. Se negocia con archivo central la disposición de un servicio centralizado de administración, dejando a nivel local las meras funciones de operación.

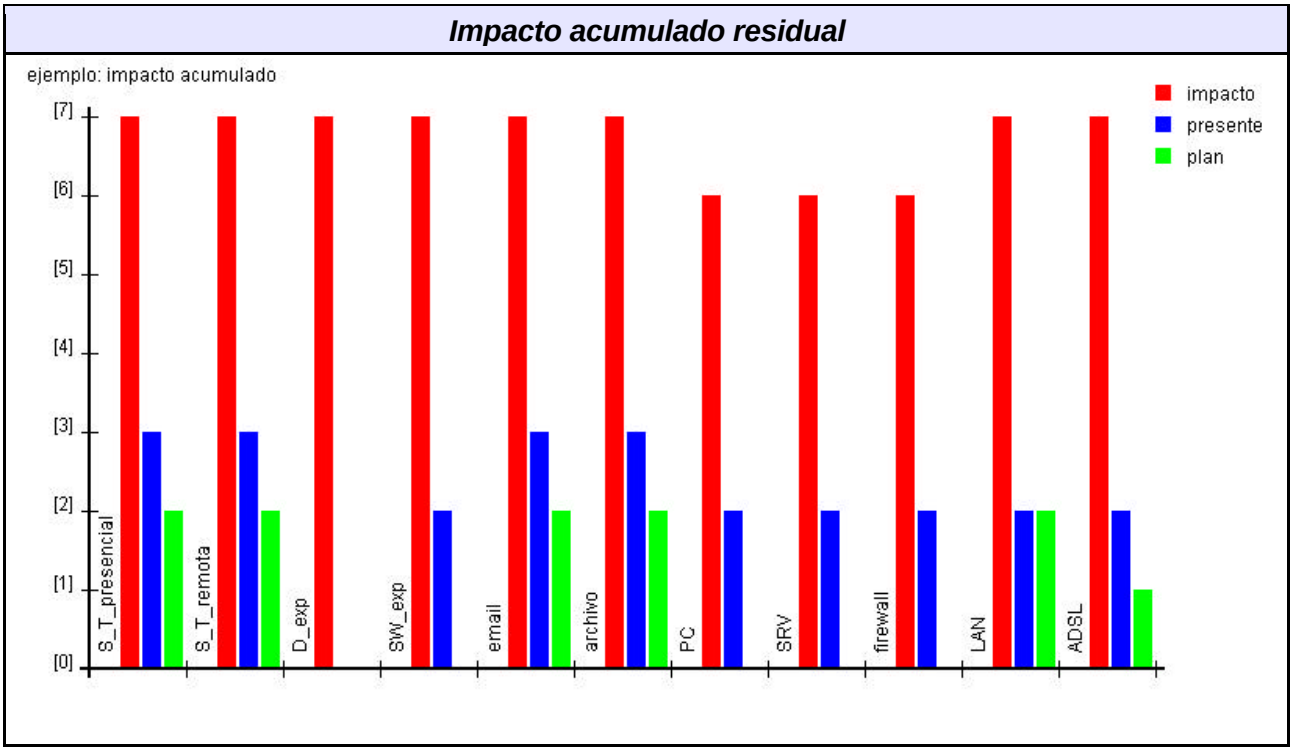
71 Ver “Apéndice 4.6. Plan de seguridad” del “Catálogo de Elementos”.

Por último se recaba de la Organización matriz información sobre el uso de tarjetas de identificación corporativas e incluso del DNI electrónico, como medios que pudieran utilizarse en el futuro para mejorar la autenticidad de los usuarios. Para el próximo ejercicio se contratará un estudio de las modificaciones requeridas para incorporar dichos mecanismos, tanto para los usuarios internos como para los usuarios externos. Parte de ese estudio será un plan detallado de realización, que en ningún caso se acometerá antes de dos años.

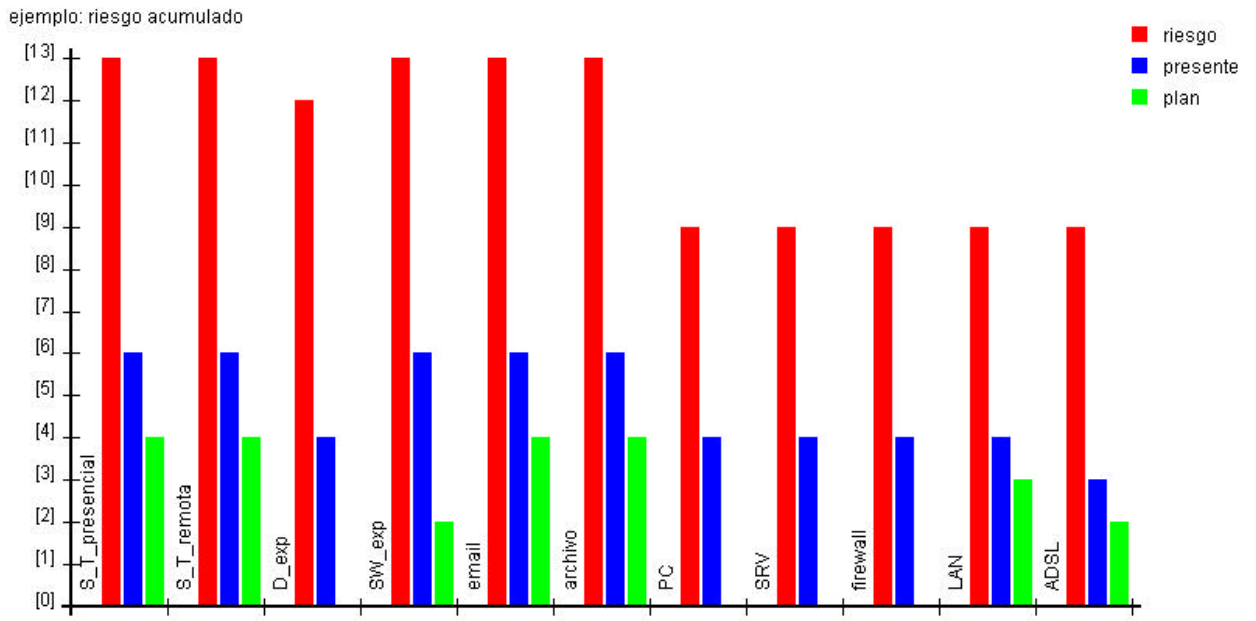
7.3.3. Evolución de los indicadores de impacto y riesgo

Las siguientes figuras muestran la evolución de los indicadores de impacto y riesgo, acumulado y repercutido, en tres instantes de la gestión del sistema de información sometido a estudio:

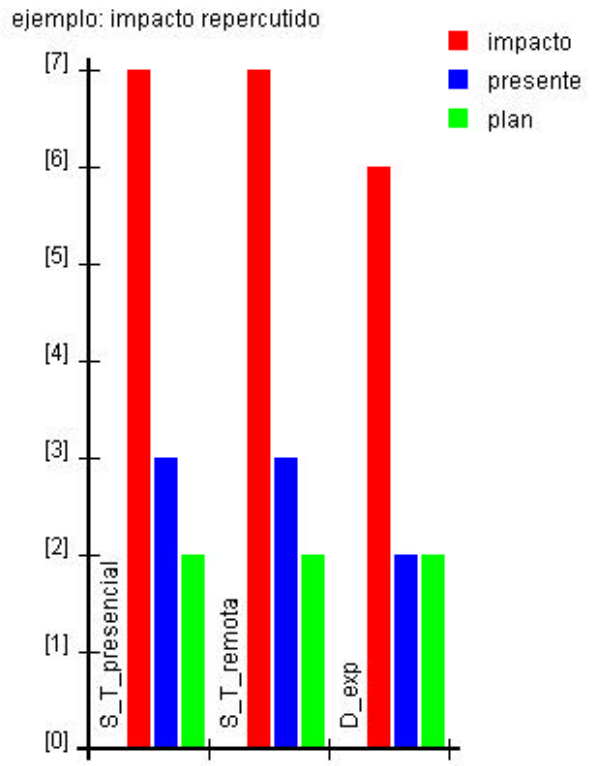
- sin salvaguardas
- en el momento presente
- tras la ejecución de los programas P1, P2 y P3 del plan de seguridad



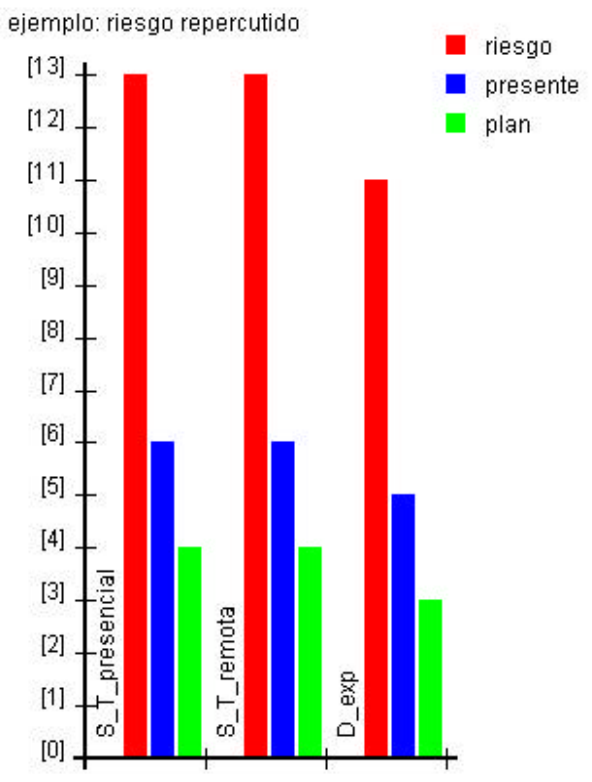
Riesgo acumulado residual



Impacto repercutido residual

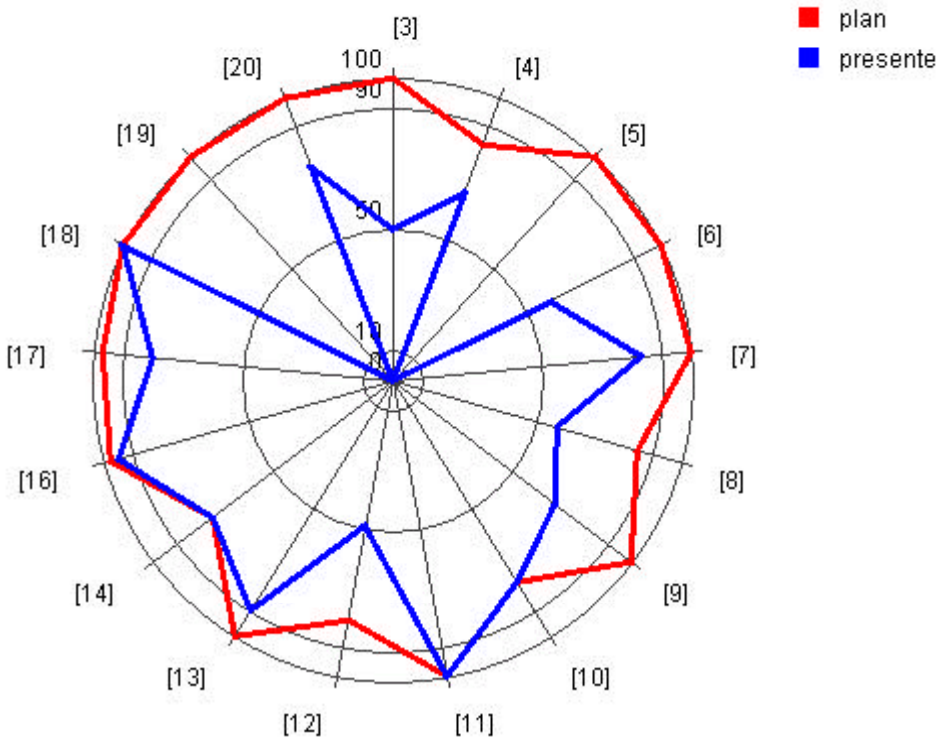


Riesgo repercutido residual



7.3.4. Calificación según los Criterios de Seguridad del CSAE

Los “Criterios de Seguridad, Normalización y Conservación de las Aplicaciones Utilizadas para el Ejercicio de Potestades” proporcionan en su libro de “Criterios de Seguridad” una larga relación de salvaguardas que deben implantarse en los sistemas. La siguiente gráfica muestra el grado de satisfacción de dichos criterios a lo largo del desarrollo del plan de seguridad (los números que



etiquetan los ejes se refieren a los capítulos del libro de criterios, que se relacionan al pie):

Criterios de Seguridad	
[3] Política de seguridad	[12] Disponibilidad
[4] Organización y planificación de la seguridad	[13] Control de acceso
[5] Análisis y gestión de riesgos	[14] Acceso a través de redes
[6] Identificación y clasificación de activos a proteger	[15] Firma electrónica (no es aplicable en este ejemplo)
[7] Salvaguardas ligadas al personal	[16] Protección de soportes de información y copias de respaldo
[8] Seguridad física	[17] Desarrollo y explotación de sistemas
[9] Autenticación	[18] Gestión y registro de incidencias
[10] Confidencialidad	[19] Plan de contingencias
[11] Integridad	[20] Auditoría y control de la seguridad