



CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

Índice Tema 4

1. Plan de seguridad.
2. Plan de contingencias.
3. Plan de recuperación. Política de salvaguarda.
4. El método MAGERIT de gestión de la seguridad.





CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

TEMA 4

Plan de seguridad. Plan de contingencias. Plan de recuperación. Política de salvaguarda. El método MAGERIT de gestión de la seguridad.

1. PLAN DE SEGURIDAD.

Por política de seguridad se entiende el conjunto de normas, reglas y prácticas, que regulan el modo en que los bienes que contienen información sensible son gestionados, protegidos y distribuidos dentro de una organización (ITSEC). La política de seguridad afecta en general a los cuatro subestados de autenticidad, confidencialidad, integridad y disponibilidad.

En relación con las implicaciones legales:

Para el ejercicio de potestades:

- Adoptar medidas organizativas y técnicas que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información garantizando la restricción de utilización, la prevención de alteraciones y la protección a procesos informáticos (Real Decreto 263/1996).

En relación con la protección de los datos de carácter personal: preparar un «Documento de Seguridad» y comunicarlo a los usuarios (Real Decreto 994/1999); elaborar un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información, en el que se define la normativa de seguridad (Real Decreto 994/1999). El contenido del documento deberá cumplir los siguientes aspectos:

- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
- Funciones y obligaciones del personal.



- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante las incidencias.
- Los procedimientos de realización de copias de respaldo y de recuperación de los datos.
- Mantener actualizado el documento en todo momento y revisarlo siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.
- Adecuar el contenido del documento, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.
- Definir, documentar y dar a conocer las funciones y obligaciones en relación con el acceso a los datos de carácter personal y a los sistemas de información.
- Implantar salvaguardas: medidas organizativas y técnicas.
- Reaccionar ante eventos y registrar incidentes.

En relación con los criterios a tener en cuenta tenemos:

1. Se deben definir y documentar los requisitos y los objetivos de seguridad de la aplicación.
2. Se deben definir y documentar las estrategias, normas, pautas y procedimientos para satisfacer los requisitos de seguridad y alcanzar los mencionados objetivos.
3. Se debe basar la política de seguridad en los resultados del análisis y gestión de riesgos.

Aspectos a recomendar: contenido de la política de seguridad:

- Objeto del documento.
- Ámbito de aplicación de la política de seguridad.
- Recursos protegidos.
- Funciones y obligaciones del personal.
- Normas, procedimientos, reglas, estándares y medidas para garantizar la autenticidad.
- Confidencialidad, integridad, disponibilidad y conservación de la información.
- Identificación, autenticación y control de accesos.
- Gestión de incidencias de seguridad.
- Gestión de soportes y copias de respaldo.
- Acceso a través de redes.

- Contingencias y continuidad del servicio.
- Controles periódicos de verificación del cumplimiento.

Anexos:

- Documentos de notificación y normas de creación de ficheros o de la aplicación para el ejercicio de potestades.
- Descripción de la aplicación y del sistema informático.
- Descripción de la estructura de ficheros o bases de datos.
- Entorno del sistema operativo y de comunicaciones.
- Descripción de locales y equipamientos.
- Análisis y gestión de riesgos.
- Descripción de las funciones y obligaciones del personal.
- Personal autorizado para acceder al fichero/aplicación.
- Procedimientos de control de accesos y perfiles de usuarios.
- Gestión de soportes de información.
- Gestión de copias de respaldo y recuperación.
- Procedimientos de notificación y gestión de incidencias.
- Plan de contingencias.
- Auditorías y controles periódicos.

La organización de la seguridad de la aplicación debe enmarcarse en la organización global de la seguridad: la función de seguridad de sistemas de información, con dedicación completa o compartida con otras funciones, incluye unos contenidos de carácter general, como la aplicación de la política de seguridad, desarrollo de normas, sistemas y procedimientos de detección de amenazas, protección de activos y acción ante eventos; así como la administración de la seguridad y de las correspondientes salvaguardas frente a las anomalías antes (preventivas) o cuando se presenten (correctivas). Además, entre los contenidos específicos figuran:

- Los procesos de los sistemas de organización y los de información que les dan soporte.
- Los distintos tipos de soporte de almacenamiento.
- Las diversas formas de transmisión y transporte.
- Las distintas plataformas del proceso (del procesador central al personal).

- Los diferentes sistemas operativos y los sistemas gestores de bases de datos.
- La conectividad entre sistemas y los sistemas gestores de comunicaciones.
- Los accesos desde las redes de comunicaciones externas.
- Las diferentes herramientas aplicables a todo lo anterior.

En relación con las implicaciones legales:

En relación con las aplicaciones para el ejercicio de potestades:

- Adoptar las medidas de organización necesarias que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información (Real Decreto 263/1996).

En relación con la protección de los datos de carácter personal:

- Adoptar las medidas de índole organizativa necesarias que garanticen la seguridad de los datos de carácter personal (Ley Orgánica 15/1999).

En relación con los criterios a tener en cuenta tenemos:

1. Se debe identificar el papel de los diversos actores en relación con los activos a proteger.

- Propietario del activo, la unidad responsable final de la seguridad del activo a su cargo y en su caso, de la protección del activo información. El propietario del activo puede delegar su autoridad en materia de seguridad a depositarios, a responsables de usuarios o a proveedores de servicios, pero deberá mantener el control para garantizar la seguridad adecuada al sistema, por ejemplo, que las salvaguardas están ya o se han implantado.
- Depositario del activo, habitualmente es el departamento de sistemas de información, que debe instalar y mantener los controles necesarios para proteger la información de acuerdo con el nivel de protección asignado por el propietario. El depositario ejercerá o delegará la función de administrador de seguridad del activo.
- Usuario del activo que debe conocer el nivel de protección de la información que maneja y cumplir con los controles establecidos por el depositario.

2. Se deben definir con claridad las responsabilidades.

- El administrador de seguridad del dominio donde se ejecute la aplicación o se mantengan los activos de información informará al propietario sobre las autorizaciones en vigor y las anomalías en los accesos que se detecten.
- El propietario tendrá bien identificados a los usuarios de los activos y bien documentados los tipos de acceso autorizados.
- El depositario y los usuarios conocerán claramente cuáles son los niveles de protección de cada activo, absteniéndose de utilizarlo en forma diferente a la prevista.

3. Se deben definir y documentar procedimientos de seguridad.

Aspectos a recomendar:

- Articular la consulta a especialistas en seguridad de los sistemas de información, internos a la propia Organización, o externos, cuando resulte apropiado.
- En caso de que los sistemas propios estén relacionados con otros sistemas de información, trabajar de forma coordinada con los responsables correspondientes.
- En organizaciones de tamaño mediano o grande conviene establecer un comité de seguridad con responsabilidad en la coordinación de la seguridad de las aplicaciones (normas y responsabilidades específicas, métodos y procesos específicos para la seguridad, coordinar la implantación de medidas de seguridad, respaldar iniciativas, velar por que la seguridad se contemple en la planificación, gestión y operación de las aplicaciones).

La complejidad de los modelos organizativos de seguridad posibles depende del tamaño de las organizaciones, de los recursos humanos disponibles, del número y tipos de activos a proteger, así como del nivel tecnológico alcanzado en materia de seguridad de los sistemas de información.

Una organización de tamaño pequeño ha de contar con un responsable de administración de la seguridad, incluso con dedicación parcial, que rinde cuentas a la Alta Dirección o al Comité Superior de Seguridad.

Un modelo sofisticado para una organización grande puede tener varios niveles, por ejemplo, un responsable de seguridad de los sistemas de información, asistido por un grupo de especialistas (en criptología, detección de intrusiones, protocolos de seguridad, etc.) del que puede depender un administrador central de seguridad informática, así como administradores sectoriales y/o locales.

Si la organización es muy grande, el modelo organizativo tendrá que coordinar distintas infraestructuras organizativas y medidas de seguridad de los sistemas de información por medio de un comité multifuncional de seguridad. Éste estaría constituido por los representantes de las áreas y funciones directivas de la organización que hayan de coordinar la implantación de las medidas adoptadas en materia de seguridad de los sistemas de información.

Funciones del responsable de la aplicación:

- Designar y autorizar a los usuarios que deben utilizar la aplicación.
- Asignar los accesos a que se permite a cada usuario, motivando los mismos.
- Definir los plazos en los que la información deja de tener vigencia administrativa; ampliar de forma motivada el momento o plazo en que la información correspondiente a determinados expedientes deja de tener vigencia administrativa, debido a la existencia de impugnaciones o al requerimiento de la autoridad judicial o de alguno de los órganos de control de la administración.
- Promover la formación del personal relacionado con el desarrollo y explotación de la aplicación así como de otros actores relacionados con los activos a proteger.

Funciones del responsable o administrador de seguridad:

- Dirigir y coordinar los distintos procesos relacionados con la seguridad de la aplicación.
- Elaborar la política de seguridad de la aplicación.
- Diseñar, probar e implantar el plan de contingencias de la aplicación.
- Informar al responsable de la aplicación y, en su caso, a la alta dirección o al comité de seguridad informática, sobre los niveles de seguridad alcanzados en la aplicación.
- Garantizar la buena comunicación con el resto de actores participantes en la seguridad.
- Dirigir las actividades de auditoría y control de la seguridad.
- Preparar los planes de implantación de distintos tipos de salvaguardas.
- Identificar, analizar los distintos incidentes de seguridad e informar al responsable de la aplicación de cualquier incidencia detectada.

Funciones del comité de seguridad:

- Identificar objetivos y estrategias relacionados con la seguridad.
- Revisar la implantación de la política de seguridad.
- Iniciar, dirigir y controlar los procesos de seguridad.
- Aprobar los distintos planes de implantación y asignar los recursos necesarios.
- Vigilar que las medidas de la política planificadas son implantadas tal como se había previsto y dan los resultados esperados.
- Preparar el programa de seguridad así como el plan de formación y concienciación.
- Estar en contacto con los distintos equipos de sistemas.

2. PLAN DE CONTINGENCIAS.

El plan de contingencias es la forma detallada en que la organización debe reaccionar para asegurar que las aplicaciones sigan activas ante determinados eventos, accidentales o deliberados. Por ejemplo, se debe prever el funcionamiento del sistema de información transitoriamente degradado.

La elaboración de un plan de contingencias debe tener en cuenta aspectos tales como la magnitud del riesgo de la aplicación afectada, incluyendo las interdependencias con otras aplicaciones, así como las prioridades de los distintos elementos de la aplicación, considerando el valor que cada elemento supone para la organización.

El análisis y gestión de riesgos genera información sobre las posibles consecuencias de distintos tipos de eventos de carácter accidental o deliberado (desastres, ataques y fallos de la aplicación o de interrupciones del servicio). El plan de contingencias se desarrolla para garantizar la continuidad de la aplicación dentro de un determinado intervalo de tiempo. Este plan debe ser mantenido a lo largo de la vida de la aplicación, y además se deberá formar al personal en su puesta en marcha.

La gestión de la continuidad debe incluir los controles para identificar y reducir riesgos, limitar las consecuencias de incidentes y garantizar la recuperación de las operaciones principales en un intervalo de tiempo aceptable.

En relación con las implicaciones legales:

En relación con las aplicaciones para el ejercicio de potestades:

- Adoptar medidas organizativas y técnicas que aseguren la autenticidad, confidencialidad, integridad y disponibilidad garantizando la restricción de utilización, la prevención de alteraciones y la protección a procesos informáticos (Real Decreto 263/1996).

En relación con la protección de los datos de carácter personal:

- Se adoptarán 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 (Ley Orgánica 15/1999).

En relación con los criterios a tener en cuenta tenemos:

1. Se debe desarrollar un plan de contingencias, basado en los resultados del análisis y gestión de riesgos, que mantenga o restaure el servicio en el menor tiempo posible tras un incidente accidental o deliberado.
2. El plan de contingencias que, de forma fundamental, debe identificar personas de contacto y acciones concretas, debe comprender las acciones organizativas y/o técnicas necesarias para garantizar la continuidad de la aplicación, con el fin de limitar al máximo la necesidad de tomar decisiones durante el período de recuperación y de recuperar los servicios imprescindibles en el menor tiempo posible reduciendo al máximo su impacto económico, estratégico y político.
3. Se debe activar el plan de contingencias como reacción ante un incidente que afecte a la continuidad del servicio proporcionado por la aplicación.

Aspectos recomendados:

Mantener la coherencia con planes de contingencias de otras aplicaciones en la organización.

Probar el plan de contingencias con una cierta periodicidad y mantenerlo actualizado para garantizar su eficacia.

El plan de contingencias puede contar con los siguientes capítulos:

- Objetivos.
- Criterios para invocar el plan de contingencias.
- Vida del plan de contingencias.
- Papeles y responsabilidades de los distintos actores.
- Procedimientos para invocar la situación de contingencia.
- Procedimientos para operar la situación de contingencia.
- Planificación de recursos cuando se opera en situación de contingencia.
- Criterios para el retorno a explotación normal.
- Procedimientos para el retorno a explotación normal.
- Procedimientos de recuperación de datos perdidos/dañados.
- Coste del plan de contingencias.
- Tratamiento del plan después de la contingencia.

Para poner en marcha un plan de contingencia se consideran las siguientes fases:

- Concienciar a la alta dirección de la organización en la necesidad de establecer un plan de contingencias, asignando los recursos necesarios.
- Realizar un análisis y gestión de riesgos.
- Determinar, como resultado del proceso anterior, los elementos del sistema a los que se les aplica el Plan.
- Formar un equipo que participe en la definición e implantación del plan de contingencia.
- Desarrollar y documentar la estrategia del plan.
- Definir procesos a realizar manualmente.
- Identificar cada uno de los procesos críticos y el nivel aceptable de funcionamiento degradado.
- Planificar contingencias.

- Evaluar costes.
- Identificar y seleccionar modalidades de implantación.
- Definir y documentar hechos que requieran el arranque del plan de contingencia.
- Definir procedimientos de recuperación de la información perdida o dañada.
- Establecer equipos de trabajo que participen en el plan y en la recuperación de la situación normal.
- Formar y entrenar al personal implicado.
- Realizar pruebas del plan.
- Actualizar el plan de acuerdo con las experiencias de las pruebas.
- Mantener el plan actualizado, de acuerdo con los diversos cambios en la organización y sus sistemas.

3. PLAN DE RECUPERACIÓN. POLÍTICA DE SALVAGUARDA.

El plan de recuperación en caso de una contingencia DRP (Disaster Recovery Plan) contempla acciones precisas que van orientadas a recuperar las aplicaciones críticas del negocio, las cuales en su mayoría soportan las funciones/procesos críticos del negocio, utilizando diferentes estrategias de recuperación de información, que van desde recuperar la información de un respaldo (Back up), hasta utilizar un equipo alternativo, minimizando con esto el impacto y el costo que pudiera tener hacia el negocio.

Los responsables primarios son: la unidad de informática, ya que el área de TI es la que es especialista en cuestión de aplicaciones y hardware que interviene en el DRP.

¿Por qué debemos tener un Plan de Recuperación?

En la actualidad la disponibilidad de la Tecnología de Información (IT) es crucial para mantener la continuidad de las operaciones y la competitividad de la empresa. Hoy la gran mayoría de organizaciones requieren un alto nivel de disponibilidad continua de 24 horas x 7 días a la semana, los 365 días del año. Una prolongada interrupción del servicio informático puede causar pérdidas muy significativas, no sólo financieras, sino también pérdida de la credibilidad con los clientes y aún peor:

La pérdida del negocio. Cerca del 75 por 100 de todas las compañías de los Estados Unidos de Norteamérica han experimentado una interrupción de operaciones:

- 72 por 100 causadas por fallos eléctricos.
- 52 por 100 resultado problemas de hardware.

- 46 por 100 causadas por fallos de telecomunicaciones.
- 43 por 100 resultado fallos con software.
- 43 por 100 nunca reabrieron sus operaciones y el 29 por 100 cerraron en los siguientes tres años.
- 93 por 100 sufrieron una pérdida de datos significativa cerraron en los siguientes cinco años.
- 20 por 100 de pequeñas y medianas empresas sufren un gran desastre cada cinco años.

Estrategias para Recuperación en caso de Desastre.

El tipo de negocio y el entorno tecnológico, así como sus requerimientos determinan el nivel apropiado económico del nivel de disponibilidad.

Algunas organizaciones que trabajan de lunes a viernes de 9 a 18 horas, solamente requieren disponibilidad de sus aplicaciones durante las horas de negocio. Para otras compañías que sus operaciones están basadas en Web, como distribuidores, comerciantes, financieros, que no se pueden dar el lujo de una interrupción, esta situación se vuelve intolerable.

La siguiente tabla nos muestra los diferentes niveles que existen para llevar a cabo una Estrategia de Recuperación:

NIVEL 1: SALVADO Y RESTAURACIÓN (BACK UP AND RESTORE).

El nivel mínimo de protección es el salvado de la información por lo que fácilmente se podrá restaurar la información, si es necesario. Los respaldos de información por lo regular se generan diariamente a un horario determinado.

Por lo tanto, cuando una organización que depende de sus operaciones en un ambiente de 7 x 24, no se puede permitir para sus operaciones un par de horas para efectuar el respaldo de su información; deberá utilizar el siguiente nivel.

NIVEL 2: CONTROL EFECTIVO DEL MANEJO DE JOURNALING Y COMMITMENT CONTROL.

El Plan de Recuperación deberá contemplar en la aplicación la captura de cambios de datos, al menos en el último salvado de información. Todos los sistemas de manejadores de bases de datos ofrecen estas funciones para cubrir las necesidades de journaling y commitment control.

NIVEL 3: SISTEMAS DE FUERZA SIN INTERRUPCIÓN (UPS O NO-BREAK).

La disponibilidad de los sistemas tienen dos dimensiones cuando sufren una caída: frecuencia y duración. Los fallos de energía eléctrica son la principal causa de que fallen los sistemas abruptamente. Por lo que los equipos de fuerza sin interrupción (UPS) reducen la frecuencia de caída de los equipos.

NIVEL 4: REDUNDANCIA EN DISCOS.

El sistema RAID5 (Redundant Arrays of Independent Disks) permite que cuando un disco falle, a través de un algoritmo de reconstrucción de información, el disco que se coloca en lugar del dañado tenga la misma información sin pérdida ninguna.

El RAID5 no protege cuando se daña al mismo tiempo más de dos discos o cuando éstos están relacionados a un controlador, un procesador de I/O o un bus.

NIVEL 5: SISTEMAS MÚLTIPLES.

(Recuperación en minutos).

Este quinto nivel le ofrece a su empresa una significativa ventaja sobre el resto de los niveles ya que en el momento en que ocurre la contingencia o hay un fallo de procesadores, puede conmutar sus equipos y continuar con sus operaciones críticas funcionando como si sólo hubiera sido un pequeño fallo de minutos y así no afecta a su imagen ante el cliente y no detiene el negocio.

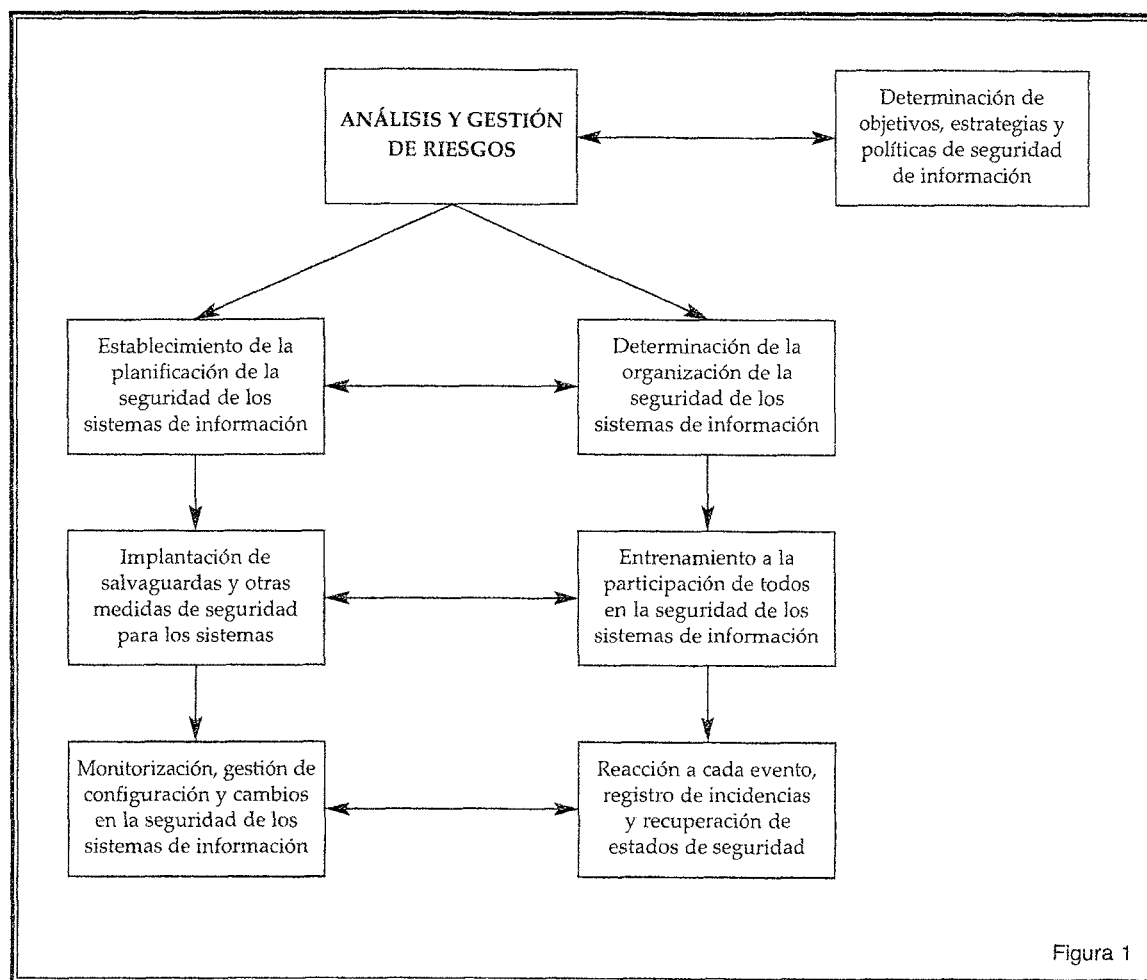
4. EL MÉTODO MAGERIT DE GESTIÓN DE LA SEGURIDAD.

Los responsables y los usuarios de la tecnología de la información son conscientes de la necesidad de disponer de instrumentos tales como metodologías que ayuden a la investigación del estado de seguridad de los sistemas de información (SI) y a la selección de medidas de seguridad proporcionadas, tanto para paliar las insuficiencias de los sistemas existentes, como para aquellos otros que precisen de reforma o de nuevo desarrollo. Para responder a esta necesidad, el Consejo Superior de Informática ha elaborado la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, MAGERIT, un método formal para investigar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

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, las empresas y la propia Administración Pública, pero que también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en su utilización. MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados que permitirán a la gestión de riesgos seleccionar e implantar las medidas de seguridad adecuadas para conocer, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. Este Análisis y Gestión de Riesgos determina la implantación de medidas de salvaguarda que responden al objetivo de mantener la continuidad de los procesos organizacionales soportados por los sistemas de información. Asimismo intenta minimizar tanto el coste global de la ejecución de dichos procesos como las pérdidas de los recursos asignados a su funcionamiento.

El Análisis y Gestión de Riesgos es, en consecuencia, el «corazón» de toda actuación organizada de materia de seguridad y, por tanto, de la gestión global de la seguridad. Influye incluso en las fases y actividades de tipo estratégico (implicación de la dirección, objetivos, políticas) y condiciona la profundidad de las fases y actividades de tipo logístico (planificación, organización, implantación de salvaguardas, sensibilización, acción diaria y mantenimiento).

La figura siguiente recoge este ciclo de fases de la gestión global de la seguridad:



MAGERIT tiene un objetivo doble:

- Estudiar los riesgos que soporta un sistema de información y el entorno asociable a él, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio.
- Recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados.

Como objetivo a más largo plazo, MAGERIT prepara su lógica articulación con los mecanismos de evaluación, homologación y certificación de seguridad de sistemas de información. Para ello toma como referencia sistemática los criterios ITSEC (Information Technology Security Evaluation Criteria) objeto de la Recomendación del Consejo de la Unión Europea, de 7 de abril de 1995, y los Criterios Comunes de Evaluación de la Seguridad de los Productos y Sistemas de Información, redactados por la Unión Europea, EE.UU. y Canadá, y actualmente en fase de prueba.

En este proceso MAGERIT persigue:

- Aportar racionalidad en el conocimiento del estado de seguridad de los Sistemas de Información y en la introducción de medidas de seguridad.

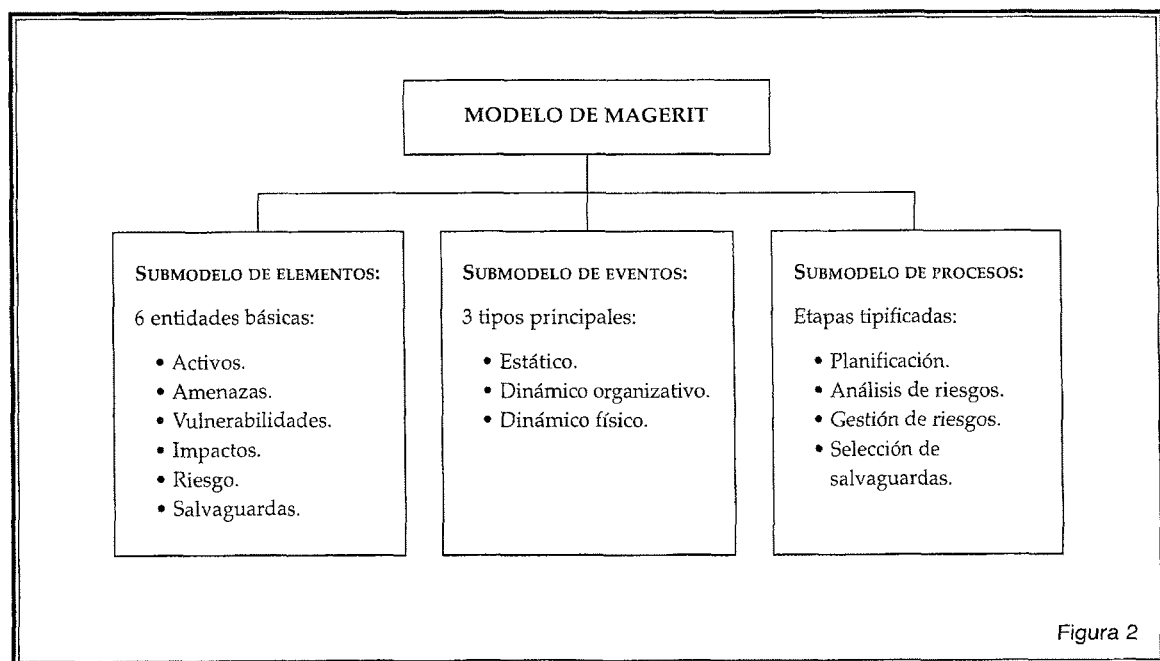
- Ayudar a garantizar una adecuada cobertura en extensión, de forma que no haya elementos del sistema de información que queden fuera del análisis, y en intensidad, de forma que se alcance la profundidad necesaria en el análisis del sistema.
- Incrustación de mecanismos de seguridad en el corazón de los sistemas de información:
 - Tanto paliando las insuficiencias de los sistemas vigentes.
 - Como asegurando el desarrollo de cualquier tipo de sistemas reformados o nuevos en todas las fases de su ciclo de desarrollo, desde la planificación hasta la implantación y mantenimiento.

MAGERIT es aplicable a la totalidad del ciclo de vida del sistema de información y se puede llevar a cabo en diferentes momentos, con diferentes grados de precisión, detalle y rigor, dependiendo del tamaño de la organización y de la complejidad del sistema de información. Para ello incorpora interfaces con la Metodología de Planificación y Desarrollo de Sistemas de Información, Métrica.

El modelo normativo de MAGERIT se apoya en tres submodelos:

- Submodelo de Elementos de Seguridad.
- Submodelo de Eventos de Seguridad.
- Submodelo de Procesos de Seguridad.

El Submodelo de Elementos proporciona los «componentes» que el Submodelo de Eventos va a relacionar entre sí y con el tiempo, mientras que el Submodelo de Procesos será la descripción funcional («el esquema explicativo») del proyecto de seguridad a construir.



MAGERIT contempla seis entidades clásicas en análisis y gestión de riesgos, cada una de ellas dotada de ciertos atributos y relacionada con las otras, que son: Activos, Amenazas, Vulnerabilidades, Impactos, Riesgos y Salvaguardas.

ACTIVOS:

Los Activos del dominio se definen como 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. Cada activo se caracteriza por su estado -en materia- de seguridad y se concreta estimando los niveles de los subestados de Autenticación, Confidencialidad, Integridad y Disponibilidad que MAGERIT define y valora.

AMENAZAS:

Se definen como los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. Las amenazas se pueden materializar y transformarse en agresiones.

VULNERABILIDAD:

Definida como la potencialidad o posibilidad de ocurrencia de materialización de una amenaza sobre un activo, la vulnerabilidad es una propiedad de la relación entre un Activo y una Amenaza. La Vulnerabilidad tiene dos aspectos: el estático, ligado a la función (forma parte del «estado de seguridad» del Activo); y el dinámico, ligado al mecanismo (convierte la amenaza en agresión).

IMPACTO:

Se define como daño producido a la organización por un posible incidente y es el resultado de la agresión sobre el Activo, o visto de manera más dinámica, la diferencia en las estimaciones de los estados (de seguridad) obtenidas antes y después del evento. El impacto puede ser cuantitativo, si representa pérdidas cuantitativas monetarizables directas o indirectas; cualitativo con pérdidas orgánicas, por ejemplo, de fondo de comercio, daño de personas; y cualitativo con pérdidas funcionales, o de los subestados de seguridad.

RIESGO:

Se ha definido como la posibilidad de que se produzca un impacto dado en la organización. Este riesgo calculado permite tomar decisiones racionales para cumplir el objetivo de seguridad de la organización. Para dar soporte a dichas decisiones, el riesgo calculado se compara con el umbral de riesgo, un nivel determinado con ayuda de la política de seguridad de la organización. Un riesgo calculado superior al umbral implica una decisión de reducción de riesgo. Un riesgo calculado inferior al umbral queda como un riesgo residual que se considera asumible.

«FUNCIÓN O SERVICIO» DE SALVAGUARDA, «MECANISMO» DE SALVAGUARDA:

Para reducir el riesgo se necesita la mejora de Salvaguardas existentes o la incorporación de otras nuevas. Se define la función o servicio de salvaguarda como la acción que reduce el riesgo; el mecanismo de salvaguarda como dispositivo, físico o lógico, capaz de reducir el riesgo y opera bien de for-

ma preventiva sobre la vulnerabilidad, «neutralizando» la materialización de la amenaza, antes de que actúe ésta, o bien de forma curativa sobre el impacto, modificando el estado de seguridad del Activo agredido y reduciendo el resultado de la agresión, o sea después de ésta.

MAGERIT ofrece un Submodelo de Eventos con tres «vistas» usadas como «esqueletos» de los productos y herramientas del método: vista estática, vista dinámica organizativa y vista dinámica física.

- La vista estática:

Refleja las relaciones generales entre las Entidades reseñadas en el Submodelo de Elementos y se necesita para establecer el Modelo Lógico de Datos que requerirá toda herramienta de apoyo a la aplicación de MAGERIT.

- La vista dinámica de tipo organizativo:

Recoge el funcionamiento detallado de la interacción de los Elementos de MAGERIT y se necesita para dar soporte al Submodelo de Procesos y para estructurar sus manuales de Procedimientos para los usuarios; para articular las técnicas de cálculo de riesgos y de selección de salvaguardas; y para construir las herramientas de apoyo a la aplicación de MAGERIT.

- La vista dinámica de tipo físico:

No es imprescindible para la comprensión de MAGERIT y sólo es necesaria para dar soporte a ciertas técnicas de cálculo de riesgos y selección de salvaguardas, como las de simulación y para ofrecer elementos de coherencia a partir de los modelos estado-acción ampliamente comprobados en el mundo físico.

El Submodelo de Procesos de MAGERIT está dividido en etapas, compuestas por actividades y éstas se desglosan en tareas (y en caso necesario en subtareas). En cada etapa se indican los hitos de control, los resultados intermedios y finales y el papel del equipo de proyecto de Análisis y Gestión de Riesgos. Para cada tarea se señalan sus objetivos, las técnicas que permiten llevarla a cabo y los productos resultantes.



El Submodelo de Procesos de MAGERIT comprende 4 Etapas:

1. Planificación del Proyecto de Riesgos.

Como consideraciones iniciales para arrancar el proyecto de análisis y gestión de riesgos, se estudia la oportunidad de realizarlo, se definen los objetivos que ha de cumplir y el ámbito que abarcará, planificando los medios materiales y humanos para su realización e inicializando el propio lanzamiento del proyecto.

2. Análisis de riesgos.

Se identifican y valoran las diversas entidades, obteniendo una evaluación del riesgo, así como una estimación del umbral de riesgo deseable.

3. Gestión de riesgos.

Se identifican las funciones y servicios de salvaguarda reductoras del riesgo, seleccionando los que son aceptables en función de las salvaguardas existentes y las restricciones, tras simular diversas combinaciones.

4. Selección de salvaguardas.

Se prepara el plan de implantación de los mecanismos de salvaguarda elegidos y los procedimientos de seguimiento para la implantación. Se recopilan los documentos del AGR, para obtener los documentos finales del proyecto y realizar las presentaciones de resultados a diversos niveles.

Para poder construir proyectos específicos de seguridad, MAGERIT posee interfaces de enlace con Métrica. MAGERIT permite añadir durante el desarrollo del sistema la consideración de los requerimientos de seguridad, sin interferir en los procedimientos de Métrica, pero utilizándolos para identificar y documentar los procedimientos y productos de aseguramiento. Estas interfaces tienen ventajas inmediatas: analizar la seguridad del Sistema antes de su desarrollo, incorporar defensas antes de completarlo (lo que es más barato y efectivo) y controlar su consistencia a lo largo de todo el ciclo de vida del Sistema.

MAGERIT enlaza con las cinco Fases de Planificación, Análisis, Diseño, Construcción e Implantación de Métrica. En cada enlace, se plantea la ampliación de los procedimientos (actividades y tareas) de la Fase, recoge productos, los trata con procedimientos específicos de aseguramiento y devuelve salvaguardas.

La estructura de MAGERIT no responde al modelo secuencial clásico, sino que la metodología contempla realimentaciones entre tareas y etapas evitando los problemas de un modelo en cascada. Por otra parte, MAGERIT cubre un espectro muy amplio de intereses de sus usuarios y responde con el enfoque de adaptarse de la forma más eficaz posible a cada organización, teniendo en cuenta la diversidad de sensibilidades en materia de seguridad global y cada preocupación concreta, así como las distintas variantes de proyectos que pueden presentarse en función de aspectos tales como la envergadura del riesgo, la situación en el «ciclo» de estudio y las posibles aplicaciones de seguridad en función de requisitos específicos.

De tal forma que en cada caso se deben seleccionar las Etapas, Actividades, Tareas y, en su caso, Subtareas sin tener que realizar todas obligatoriamente.

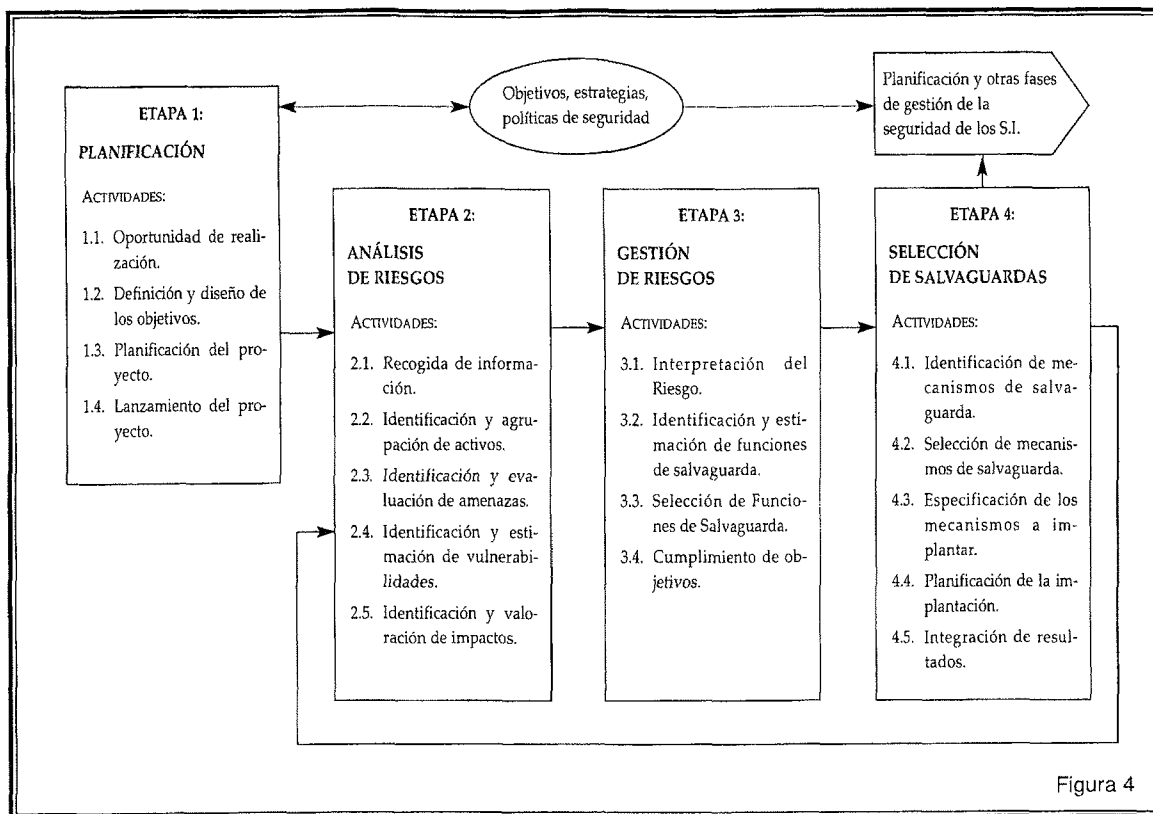


Figura 4

Como se observa en la figura anterior se anotan los enlaces de MAGERIT con fases de la gestión global de la seguridad de los sistemas de información tales como «Objetivos, Estrategia y Política de Seguridad» (que es anterior y concomitante con MAGERIT) y «Planificación de los Mecanismos de Salvaguarda» (que inicia el resto de la Gestión de la Seguridad). La aplicación de MAGERIT (o sea la acción para ampliar el estado de seguridad de un Dominio) se presenta como un proyecto de desarrollo de seguridad consistente en dos etapas sucesivas (a la manera de muchos métodos generales, Métrica entre ellos):

- La primera etapa es una adaptación del método que tiene como estado inicial el modelo canónico de método presentado aquí y como estado final una variante metodológica de este modelo adaptada o dimensionada a la medida del proyecto específico.
- La segunda etapa parte de esta variante metodológica y del «estado inicial» de seguridad del SI, para llegar al «estado final» de seguridad deseado.

Por otra parte los proyectos de complejidad media o alta en materia de seguridad requieren la realización de más de un ciclo de gestión global de seguridad. La primera aplicación del ciclo de gestión abarca todo el sistema en estudio, es decir, arranca de la fase de análisis y gestión de riesgos, enfocada a grandes rasgos para conseguir una primera dicotomía o clasificación en dos grandes bloques de los componentes del sistema:

- Los componentes que implican riesgos menores, a los que bastará aplicar globalmente medidas básicas de seguridad «práctica».
- Los componentes que implican riesgos mayores, a cada uno de los cuales será necesario aplicar un nuevo análisis y gestión de riesgos más detallado, con un nivel de detalle proporcionado al riesgo detectado.

El esquema completo de Etapas, Actividades y Tareas del Submodelo de Procesos de MAGERIT es el siguiente:

ETAPA 1: PLANIFICACIÓN DEL ANÁLISIS Y GESTIÓN DE RIESGOS.

ACTIVIDADES	TAREAS
1.1. Oportunidad de realización.	1.1.1. (única) Clarificar la oportunidad de realización.
1.2. Definición de dominio y objetivos.	1.2.1. Especificar los objetivos del proyecto. 1.2.2. Definir el dominio y los límites del proyecto. 1.2.3. Identificar el entorno y restricciones generales. 1.2.4. Estimar dimensión, coste y retornos del proyecto.
1.3. Planificación del proyecto.	1.3.1. Evaluar cargas y planificar entrevistas. 1.3.2. Organizar a los participantes. 1.3.3. Planificar el trabajo.
1.4. Lanzamiento del proyecto.	1.4.1. Adaptar los cuestionarios. 1.4.2. Seleccionar criterios de evaluación y técnicas. 1.4.3. Asignar los recursos necesarios.

ETAPA 2: ANÁLISIS DE RIESGOS.

ACTIVIDADES	TAREAS
2.1. Recogida de información.	2.1.1. Preparar la información. 2.1.2. Realización de las entrevistas. 2.1.3. Analizar la información recogida.
2.2. Identificación y agrupación de activos.	2.2.1. Identificar activos y grupos de activos. 2.2.2. Identificar mecanismos de salvaguarda existentes. 2.2.3. Valorar activos.
2.3. Identificación y evaluación de amenazas.	2.3.1. Identificar y agrupar amenazas. 2.3.2. Establecer los árboles de fallos generados por amenazas.
2.4. Identificación y estimación de vulnerabilidades.	2.4.1. Identificar vulnerabilidades. 2.4.2. Estimar vulnerabilidades.
2.5. Identificación y valoración de impactos.	2.5.1. Identificar impactos. 2.5.2. Tipificar impactos. 2.5.3. Valorar impactos.
2.6. Evaluación del riesgo.	2.6.1. Evaluar el riesgo intrínseco. 2.6.2. Analizar las funciones de salvaguarda existentes. 2.6.3. Evaluar el riesgo efectivo.

ETAPA 3: GESTIÓN DE RIESGOS.

ACTIVIDADES	TAREAS
3.1. Interpretación del Riesgo.	3.1.1. (única) Interpretar los riesgos.
3.2. Identificación y estimación de Funciones de salvaguarda.	3.2.1. Identificar funciones de salvaguarda. 3.2.2. Estimar la efectividad de las funciones de salvaguarda.
3.3. Selección de Funciones de Salvaguarda.	3.3.1. Aplicar los parámetros de selección. 3.3.2. Evaluar el riesgo.
3.4. Cumplimiento de objetivos.	3.4.1. (única) Determinar el cumplimiento de los objetivos.

ETAPA 4: SELECCIÓN DE SALVAGUARDAS.

ACTIVIDADES	TAREAS
4.1. Identificación de mecanismos de salvaguarda.	4.1.1. Identificar mecanismos posibles. 4.1.2. Estudiar mecanismos implantados. 4.1.3. Incorporar restricciones.
4.2. Selección de mecanismos de salvaguarda.	4.2.1. Identificar mecanismos a implantar. 4.2.2. Evaluar el riesgo (mecanismos elegidos). 4.2.3. Seleccionar mecanismos a implantar.
4.3. Especificación de los mecanismos a implantar.	4.3.1. (única) Especificar los mecanismos a implantar.
4.4. Planificación de la implantación.	4.4.1. Priorizar mecanismos. 4.4.2. Evaluar los recursos necesarios. 4.4.3. Elaborar cronogramas tentativos.
4.5. Integración de resultados.	4.5.1. (única) Integrar los resultados.

Cada una de las Tareas del Submodelo de Procesos en la Guía de Procedimientos indica las técnicas empleadas para realizarla. MAGERIT tipifica las técnicas recomendadas como:

- Técnicas Comunes con otros métodos relativos a los SI (Métrica y Eurométodo).
- Técnicas Específicas (y Algoritmos) del Análisis y Gestión de Riesgos (AGR).
- Técnicas Complementarias.

La Guía de Técnicas detalla básicamente las Técnicas Específicas, aunque ofrece también referencia de la descripción de las Técnicas Comunes y de las Complementarias que se encuentran en otras Guías de fácil acceso (por ejemplo la Guía de Técnicas del método Métrica). En todo caso, las particulariza o las complementa para su mejor empleo por MAGERIT.

TÉCNICAS COMUNES CON MÉTRICA	<ul style="list-style-type: none"> • Técnica de entrevistas. • Técnica de Factores críticos de éxito. • Técnica de Análisis Coste Beneficio. • Técnicas matriciales comunes. • Diagramas de flujo de datos (y Diagramas de flujo). • Modelado de datos.
TÉCNICAS COMUNES CON EUROMÉTODO	<ul style="list-style-type: none"> • Técnica de factores situacionales. • Técnicas de planificación de proyectos.
TÉCNICAS Y ALGORITMOS ESPECÍFICOS DEL ANÁLISIS Y GESTIÓN DE RIESGOS	<ul style="list-style-type: none"> • Técnicas matriciales específicas. • Técnicas Algorítmicas. • Técnicas avanzadas (lógica difusa, probabilidad bayesiana). • Experiencia del Grupo de Trabajo en la aplicación de MAGERIT.
TÉCNICAS COMPLEMENTARIAS	<ul style="list-style-type: none"> • Técnica gráficas (Diagramas Gantt, Kiviat o de barras, de Pareto). • Técnica Delphi. • Técnica de dirección y gestión de proyectos. • Técnicas de asignación presupuestaria y de selección de personal. • Técnica de elaboración de cuestionarios. • Técnica de elaboración de informes. • Técnicas de presentación. • Técnicas estadísticas. • Técnica de Simulación.

MAGERIT consta de un conjunto de guías y de unas herramientas para su aplicación.

I. Guías MAGERIT.

Guía de Aproximación.

Presenta los conceptos básicos de seguridad de los sistemas de información y ofrece una introducción al núcleo básico de MAGERIT.

Guía de Procedimientos.

Representa el núcleo del método, que se completa con la Guía de Técnicas.

Guía de Técnicas.

Proporciona las claves para comprender y seleccionar las técnicas más adecuadas para los procedimientos de análisis y gestión de riesgos de seguridad de los sistemas de información.

Guía para Responsables del Dominio protegible.

Se dirige a los Directivos, cuyas Organizaciones, para el cumplimiento de sus fines, utilicen sistemas de información.

Guía para Desarrolladores de Aplicaciones.

Está orientada a contemplar los mecanismos de seguridad en cada caso apropiados durante el desarrollo de toda nueva aplicación.

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

Estructura de la información para intercambio con otro producto informatizado semejante o relacionado con la herramienta MAGERIT.

Referencia de Normas legales y técnicas.

Lista de normas en materia de seguridad a fecha 31 de diciembre de 1996 de interés para un especialista en la materia.

II. Herramientas de apoyo.

1. Introductoria.

Permite una primera aproximación al Análisis y Gestión de Riesgos y constituye un apoyo en la identificación de riesgos menores a los que bastará aplicar globalmente medidas básicas de seguridad «práctica» y de riesgos mayores a cada uno de los cuales será necesario aplicar un nuevo Análisis y Gestión de Riesgos más detallado. Se apoya en el uso de técnicas matriciales y no requiere que el usuario tenga necesariamente un nivel avanzado de especialización en seguridad de los sistemas de información.

2. Avanzada.

Permite realizar un Análisis y Gestión de riesgos detallado y afrontar así proyectos de complejidad media o alta en materia de seguridad. Se apoya en el uso de técnicas algorítmicas, de lógica difusa y de Bayes. Permite un análisis detallado de los Activos del Dominio y de sus dependencias, de la relación entre éstos y las Amenazas, las Funciones y los Mecanismos de Seguridad, y de los Riesgos (intrínseco, efectivo, residual). Requiere que el usuario tenga un cierto nivel de especialización en seguridad de los sistemas de información.



