MINISTERIO
DE ADMINISTRACIONES
PÚBLICAS

SECRETARÍA DE ESTADO
PARA LA ADMINISTRACIÓN
PÚBLICA

CONSEJO SUPERIOR DE
INFORMÁTICA Y PARA EL
IMPULSO DE LA
ADMINISTRACIÓN
ELECTRÓNICA

Aplicaciones utilizadas para el ejercicio de potestades

CRITERIOS DE SEGURIDAD

28 de Febrero de 2003

Madrid, febrero de 2003

Índice

Historial del documento

Versión	***Comentarios.***
Versión 1 Final. Presentada al Pleno de CIABSI de 26 de septiembre de 2001.	N/A.
Versión 1.1. Presentada al Pleno de CIABSI de 24 de octubre de 2001.	N/A.
Versión 1.2. Presentada al Pleno de CIABSI de 18 diciembre de 2001.	Versión publicada.
Versión 2. Aprobada por la Sesión plenaria de la CIABSI de 18 diciembre de 2002.	Modificación de los apartados de 'Criterios' y 'Recomendaciones'. *Criterios: medidas que se deben adoptar*; *Recomedaciones: otras medidas complementarias*. Los criterios se numeran para mejor referencia.
Versión 2.1. Revisión editorial.	Revisión editorial con los comentarios recibidos y actualización con lo dispuesto en el 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.

1 Presentación

Introducción

Este documento 'Criterios de seguridad', elaborado por el Consejo Superior de Informática y para el impulso de la Administración Electrónica, expone los requisitos, criterios, y recomendaciones relativos a la implantación de las medidas de seguridad, organizativas y técnicas, en el diseño, desarrollo, implantación y explotación de las aplicaciones cuyo resultado sea utilizado para el ejercicio por los órganos y entidades del ámbito de la Administración General del Estado de las potestades que tienen atribuidas.

El 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, modificado por el 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, encomienda al Consejo Superior de Informática y para el impulso de la Administración Electrónica la aprobación y difusión de los criterios de seguridad de las aplicaciones que efectúen tratamientos de información cuyo resultado sea utilizado por los órganos y entidades del ámbito de la Administración General del Estado para el ejercicio de las potestades que tienen atribuidas.

Asimismo, los 'Criterios de seguridad' abordan la protección de los datos de carácter personal, teniendo en cuenta los requisitos establecidos en la *Ley Orgánica 15/1999 de Protección de datos de carácter personal* y en el *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.*

Por otra parte, la *Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones sobre seguridad de las redes y de la información: Propuesta para un enfoque político europeo* insta a los Estados miembros a fomentar el uso de mejores prácticas basadas en instrumentos existentes, tales como la norma UNE 717799 (norma equivalente a ISO/IEC IS 17799) 'Código de buenas prácticas para la gestión de la seguridad de la información', que constituye un término de referencia fundamental de los criterios y recomendaciones incluidos en este documento.

Adopción de medidas de seguridad organizativas y técnicas

Las aplicaciones utilizadas para el ejercicio de potestades y la información que manejan, especialmente los datos de carácter personal, deben protegerse contra la pérdida de autenticidad, confidencialidad, integridad y disponibilidad.

Al objeto de conseguir la protección adecuada, es necesario implantar un conjunto proporcionado de medidas de seguridad, tanto técnicas como organizativas, que permitan la creación de un entorno seguro para los datos, la información, las aplicaciones y los sistemas que sustentan a todos ellos. Estas medidas organizativas y técnicas permitirán, en líneas generales, lo siguiente:

- Identificar, autenticar y, en su caso, autorizar el acceso a los sistemas de información.
- Identificar fidedignamente a remitente y destinatario de las comunicaciones electrónicas.
- Controlar el acceso para restringir la utilización y el acceso a datos e informaciones a las personas autorizadas y proteger los procesos informáticos frente a manipulaciones no autorizadas.

- Mantener la integridad de la información y elementos del sistema, para prevenir alteraciones o pérdidas de los datos e informaciones.
- Garantizar la disponibilidad de la información y de las aplicaciones.
- Prevenir la interceptación, alteración y acceso no autorizado a la información.
- Gestionar las incidencias de seguridad.
- Auditar y controlar la seguridad.

Objetivos

Los 'Criterios de seguridad' de las aplicaciones utilizadas para el ejercicio de potestades, tienen por objetivo:

- Proporcionar el conjunto de medidas organizativas y técnicas de seguridad que garanticen el cumplimiento de los requisitos legales para la validez y eficacia de los procedimientos administrativos de la Administración General del Estado, que utilicen los medios electrónicos, informáticos y telemáticos en el ejercicio de sus potestades.
- Facilitar la adopción generalizada por parte de la Administración General del Estado de medidas organizativas y técnicas que aseguren la protección proporcionada a los riesgos de los sistemas y aplicaciones que la manejan.
- Promover el máximo aprovechamiento de las tecnologías de la información y las comunicaciones en la actividad administrativa y asegurar a la vez el respeto de las garantías y derechos de los ciudadanos en sus relaciones con la Administración.

Estructura y contenidos

El documento se compone de 19 capítulos, además de esta introducción:

- Gestión global de la seguridad de la información
- Política de seguridad
- Organización y planificación de la seguridad
- Análisis y gestión de riesgos
- Identificación y clasificación de activos a proteger
- Aspectos de seguridad ligados al personal
- Seguridad física
- Autenticación
- Confidencialidad
- Integridad
- Disponibilidad
- Control de acceso
- Acceso a través de redes
- Firma electrónica
- Protección de soportes de información y copias de respaldo
- Desarrollo y explotación de sistemas
- Gestión y registro de incidencias
- Plan de contingencias
- Auditoría y control de la seguridad

La relación entre los capítulos puede visualizarse en el siguiente esquema:

Cada capítulo consta de:

- Relación de las prescripciones o requisitos legales, que obligan a aplicar distintas medidas de seguridad, en particular en relación con la validez de los procedimientos administrativos y con los datos de carácter personal.
- Los *criterios* que señalan las medidas de seguridad organizativas y técnicas que con carácter general se deben adoptar para satisfacer los requisitos anteriores. Se numeran para facilitar su localización y referencia. Son criterios de mínimos, esto es, condiciones armonizadoras a partir de las cuales se pueden añadir protecciones adicionales.
- Las *recomendaciones* que complementan a los criterios expuestos con otras medidas técnicas u organizativas complementarias a los criterios, si bien pueden ser exigibles en las aplicaciones que se citan.
- Los *niveles de seguridad* desarrollan los niveles de medidas de seguridad definidos por el Real Decreto 994/1999, de 11 de junio, Reglamento de medidas de seguridad de los ficheros automatizados que contienen datos de carácter personal.
- La *ampliación técnica* da referencias que permiten profundizar y ampliar los conceptos técnicos y organizativos en los que se fundamentan las distintas medidas de seguridad.

Adicionalmente, en ciertos capítulos se incluyen ***consideraciones*** que matizan el alcance o contenidos de los mismos; un apartado denominado ***conceptos*** con explicación o definición de aspectos clave; y, finalmente, otro apartado denominado ***ejemplo de solución*** con algunas orientaciones más concretas, todo ello de forma muy resumida.

Proporcionalidad

Ha de tenerse en cuenta que la aplicación de las medidas de seguridad organizativas y técnicas expuestas en este documento debe realizarse atendiendo al **principio de proporcionalidad** que relaciona la naturaleza de los datos y de los tratamientos con los riesgos a los que estén expuestos y el estado de la tecnología, y, en particular, a las medidas exigidas en relación con la **protección de los datos de carácter personal**.

Convenciones

En la formulación de los criterios o recomendaciones se utiliza la voz "aplicación" o "aplicaciones" con el mismo significado que emplea el Real Decreto 263/1996: "aplicación: Programa o conjunto de programas

cuyo objeto es la resolución de un problema mediante el recurso a un sistema de tratamiento de la información".

Modo de utilización

Es importante hacer notar que la aplicación práctica de los presente Criterios de seguridad deberá hacerse de manera conjunta, habida cuenta de la estrecha interdependencia de unos capítulos con otros.

Por ejemplo, la finalidad última de la seguridad es proteger la autenticación, la confidencialidad, la integridad o la disponibilidad. No se consigue satisfacer esa finalidad considerando únicamente los Criterios de capítulos con esos títulos, sino que son coadyuvantes necesarios las funciones o mecanismos de seguridad, cuyos criterios se detallan en el control de acceso, acceso a través de redes, firma electrónica, protección de soportes de información y copias de respaldo, desarrollo y explotación de sistemas y gestión y registro de incidencias. Así mismo será preciso identificar y clasificar los activos a proteger. Las salvaguardas ligadas al personal, serán a su vez resultado de la gestión global de la seguridad de la información y la política de seguridad, cuya implementación en el seno de los departamentos administrativos deberá tener en cuenta: el análisis y gestión de riesgos y la seguridad física; la continuidad de los servicios exigirá el Plan de contingencias. Finalmente, la verificación del cumplimiento del conjunto de los Criterios se realizará mediante la auditoría y control de la seguridad.

Destinatarios

Los presentes Criterios se dirigen a los responsables de la adquisición, diseño, desarrollo, implantación y explotación de las aplicaciones informáticas utilizadas para el ejercicio de potestades en el ámbito de la Administración General del Estado, así como al personal, técnico o no, afectado por dichas aplicaciones.

Actualizaciones

Por la naturaleza de su contenido, la evolución de la tecnología y el crecimiento del número de aplicaciones, ha de tenerse en cuenta que éste es un **documento vivo** que ha de verse **sometido a actualizaciones regulares**, para añadir, perfeccionar o completar los apartados que lo requieran. Se invita a enviar comentarios o sugerencias a la Secretaría de SSITAD, por correo electrónico (secretaria.ssitad@map.es) o a través de los cauces administrativos.

2 Gestión global de la seguridad de la información

CONSIDERACIONES:

La gestión de la seguridad de cada aplicación debe estar enmarcada dentro de la gestión global de la seguridad de la información en la organización. La gestión global de la seguridad afecta, en general a la salvaguarda de la autenticidad, confidencialidad, integridad y disponibilidad de la información.

La gestión global de la seguridad afecta así mismo a todos los actores implicados: responsable o propietario de la aplicación o del fichero de datos de carácter personal, depositarios de la aplicación o del fichero y usuarios.

MARCO LEGAL:

En relación con las aplicaciones 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. (RD 263/1996, arts. 4.2 y 4.3)

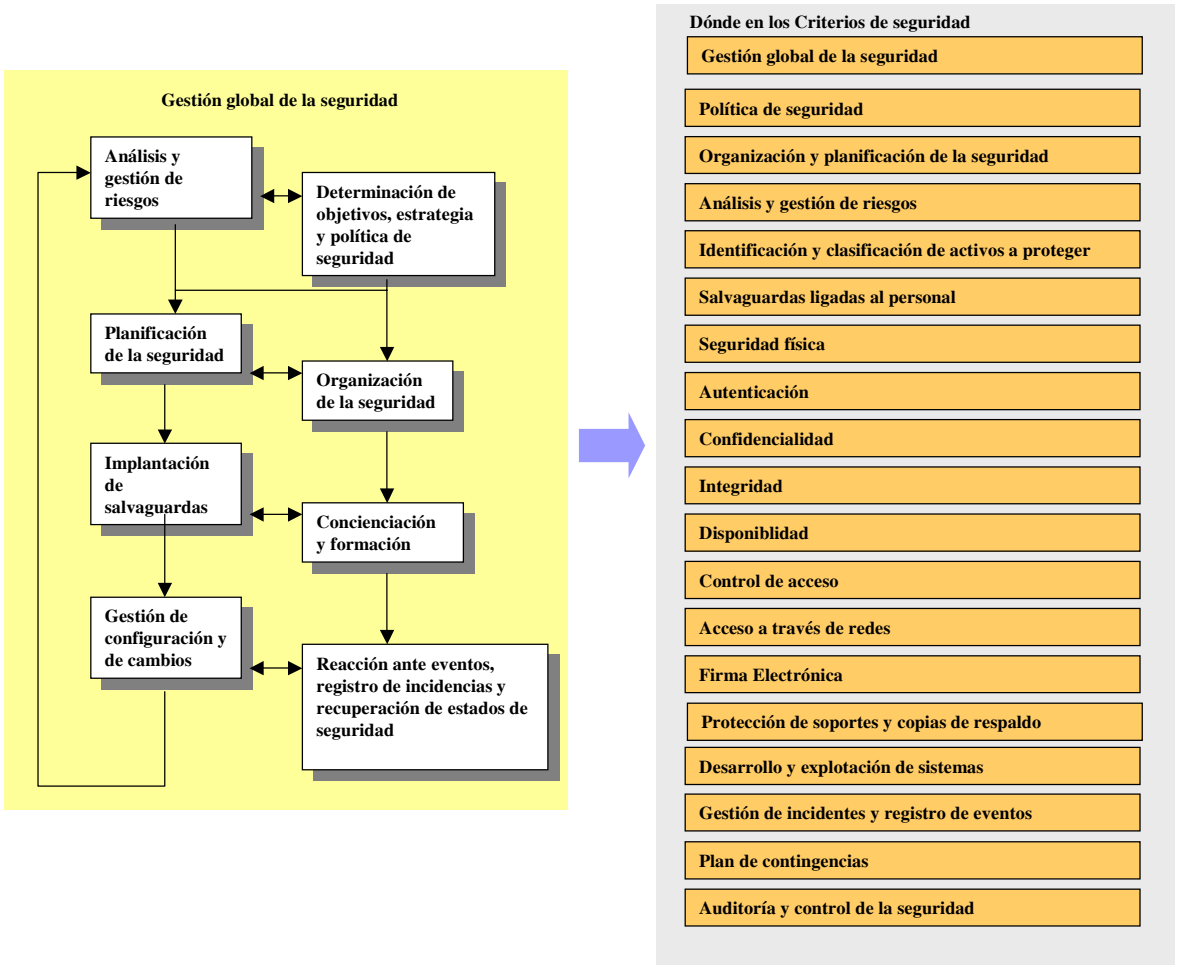
En relación con la protección de los datos de carácter personal:

- 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. (LO 15/1999, art. 9.1)

RECOMENDACIONES:

Se debe realizar y mantener la gestión global de la seguridad de la aplicación como acción permanente, cíclica y recurrente.

Para realizar la gestión global de seguridad se han de emprender los siguientes procesos:



- El análisis y gestión de riesgos se encarga de estudiar los activos, amenazas, vulnerabilidades, impactos, y riesgos que una seguridad insuficiente puede tener para la organización, así como de las salvaguardas necesarias.
- La determinación de objetivos, estrategia y política de seguridad se alimenta de la anterior para definir que hay que proteger y por qué, y sirven de guía y respaldo para la implementación de las medidas necesarias de protección.
- La planificación de la seguridad es la consecuencia funcional del análisis y gestión de riesgos.
- La organización de la seguridad establecerá los medios organizativos y recursos dedicados a la seguridad de la información.
- La implantación de las salvaguardas se realizará de acuerdo a la planificación y a la organización de la seguridad.
- La concienciación y formación tiene un papel fundamental para el éxito de la política de seguridad.
- La gestión de configuración y de cambios tiene un carácter de mantenimiento adaptado al ámbito de la seguridad.
- La fase de reacción a cada evento, registro de incidencias y recuperación de estados de seguridad tiene un carácter básicamente operacional.

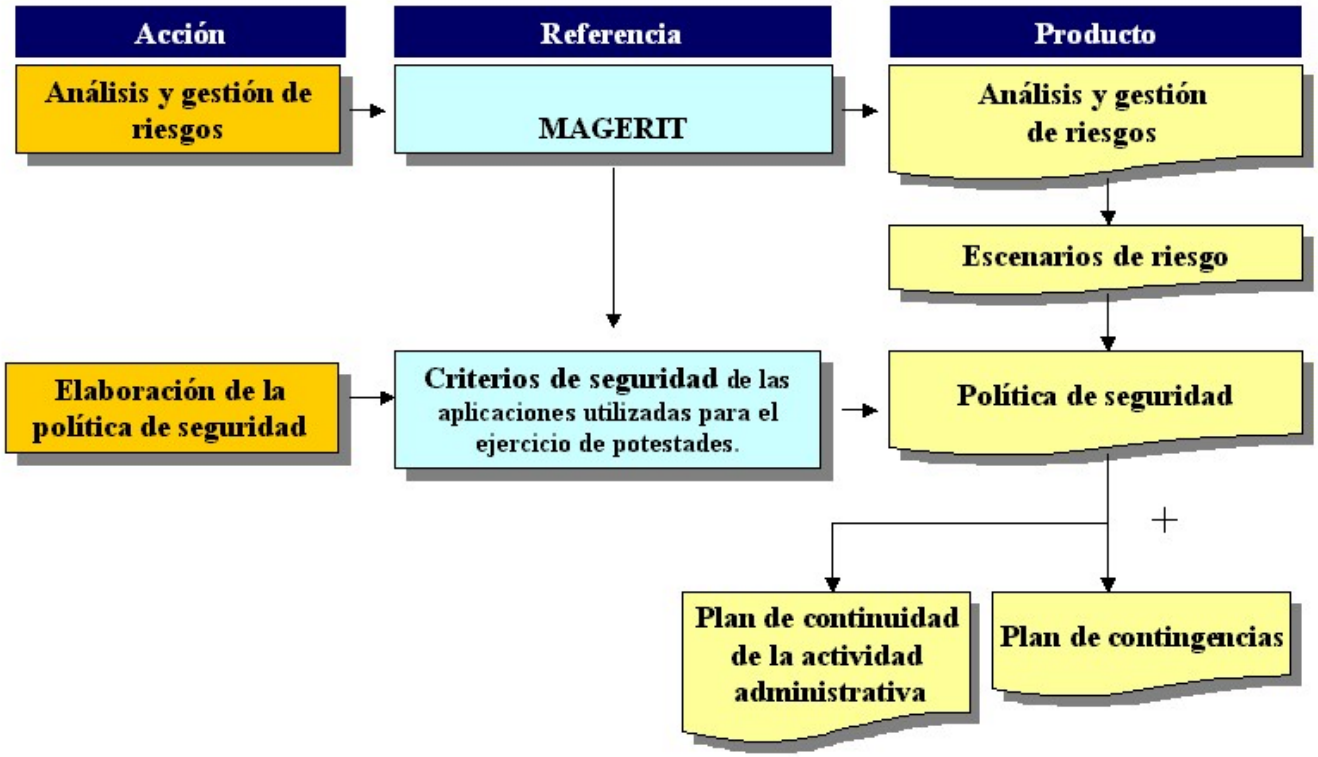
AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT); Guía de aproximación a la seguridad de los sistemas de información; capítulo 2; http://www.map.es/csi/pg5m20.htm
- UNE ISO/IEC IS 17799 – Tecnologías de la información – Código de buenas prácticas para la gestión de la seguridad de la información *(Information technology – Code of practice for information security managment)*
- *INFORMATION TECHNOLOGY Baseline Protection Manual*; capítulos 2 y 3; http://www.bsi.bund.de/gshb/english/etc/inhalt.htm
- ISO/IEC TR 13335 – Tecnologías de la información (TI) – Guía para la gestión de la seguridad de TI.
- Guía de seguridad informática (SEDISI), http://www.sedisi.es/ 05_index.htm
- Comunicación de la Comisión al Consejo, al Parlamento Europeo al Comité Económico y Social y al Comité de las Regiones, Seguridad de las redes y de la información: propuesta para un enfoque político europeo (6 de junio de 2001), http://www.map.es/csi/pdf/com2001_0298es01.pdf

3 Política de seguridad

CONSIDERACIONES:

La política de seguridad de la aplicación debe estar englobada dentro de la política general de seguridad de la información de la organización.



CONCEPTOS:

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.

MARCO LEGAL:

En relación con las Aplicaciones 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. (RD 263/1996, arts. 4.2 y 4.3)

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

Preparar un "Documento de Seguridad" y comunicarlo a los usuarios (RD 994/1999, arts. 8 y 15):

- 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 (RD 994/1999, arts. 8.1, 8.2). 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. (RD 994/1999, art.8.3)
- Adecuar el contenido del documento, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal. (RD 994/1999, art.8.4)
- 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 (RD 994/1999, arts. 9.1 y 9.2)
- Implantar salvaguardas: medidas organizativas y técnicas (RD 994/1999, artículos diversos reflejados en otros capítulos del presente volumen).
- Reaccionar ante eventos y registrar incidentes. (RD 994/1999, art. 10).

CRITERIOS:

3.1 Se deben definir y documentar los requisitos y los objetivos de seguridad de la aplicación.

3.2 Se deben definir y documentar las estrategias, normas, pautas y procedimientos para satisfacer los requisitos de seguridad y alcanzar los mencionados objetivos.

3.3 Se debe basar la política de seguridad en los resultados del análisis y gestión de riesgos.

RECOMENDACIONES:

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.
- Auditorias y controles periódicos.

Caso de que los documentos ya existan, basta una referencia exacta, garantizando que se encuentran en todo momento localizados y debidamente utilizados.

AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT); Guía de aproximación a la seguridad de los sistemas de información; capítulo 3; http://www.map.es/csi/pg5m20.htm
- UNE ISO/IEC IS 17799 – Tecnologías de la información – Código de buenas prácticas para la gestión de la seguridad de la información *(Information technology – Code of practice for information security managment)*; capítulo 3.
- *Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook;* capítulo 5; http://csrc.nist.gov/publications/nistpubs/800-12/
- ISO/IEC TR 13335 – Tecnologías de la información (TI) - Guía para la gestión de la seguridad de TI; Parte 1; capítulo 7.2.

4 Organización y planificación de la seguridad

CONSIDERACIONES:

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 de 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 a y desde las redes de comunicaciones externas;
  - las diferentes herramientas aplicables a todo lo anterior.

MARCO LEGAL:

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. (RD 263/1996, art. 4.2)

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

- Adoptar las medidas de índole organizativas necesarias que garanticen la seguridad de los datos de carácter personal. (LO 15/1999, art. 9.1)

CRITERIOS:

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

- *Propietario del activo,* 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.

4.2 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 cuales son los niveles de protección de cada activo, absteniéndose de utilizarlo en forma diferente a la prevista.

4.3 Se deben definir y documentar procedimientos de seguridad.

RECOMENDACIONES:

- 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 contempla en la planificación, gestión y operación de las aplicaciones).

AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT); Guía de aproximación a la seguridad de los sistemas de información; capítulo 4; http://www.map.es/csi/pg5m20.htm
- ISO/IEC IS 17799 - Tecnologías de la información - Código de buenas prácticas para la gestión de la seguridad de la información *(Information technology – Code of practice for information security managment)*; capítulo 4.
- ISO/IEC TR 13335 - Tecnologías de la información - Guía para la gestión de la seguridad de TI; Parte 4; capítulo 8.1.
- *Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook;* capítulo 3; http://csrc.nist.gov/publications/nistpubs/800-12/
- *INFORMATION TECHNOLOGY Baseline Protection Manual*; capítulo 3.1; http://www.bsi.bund.de/gshb/english/etc/inhalt.htm
- Resolución de 29 de noviembre de 1996, por la que se dictan instrucciones relativas a los accesos a las bases de datos de la Agencia Estatal de Administración Tributaria. (BOE 20-12-96) .

EJEMPLO DE SOLUCIÓN:

Se incluye una propuesta de actores y de actividades partiendo del supuesto de que 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 auditoria 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.

5 Análisis y gestión de riesgos

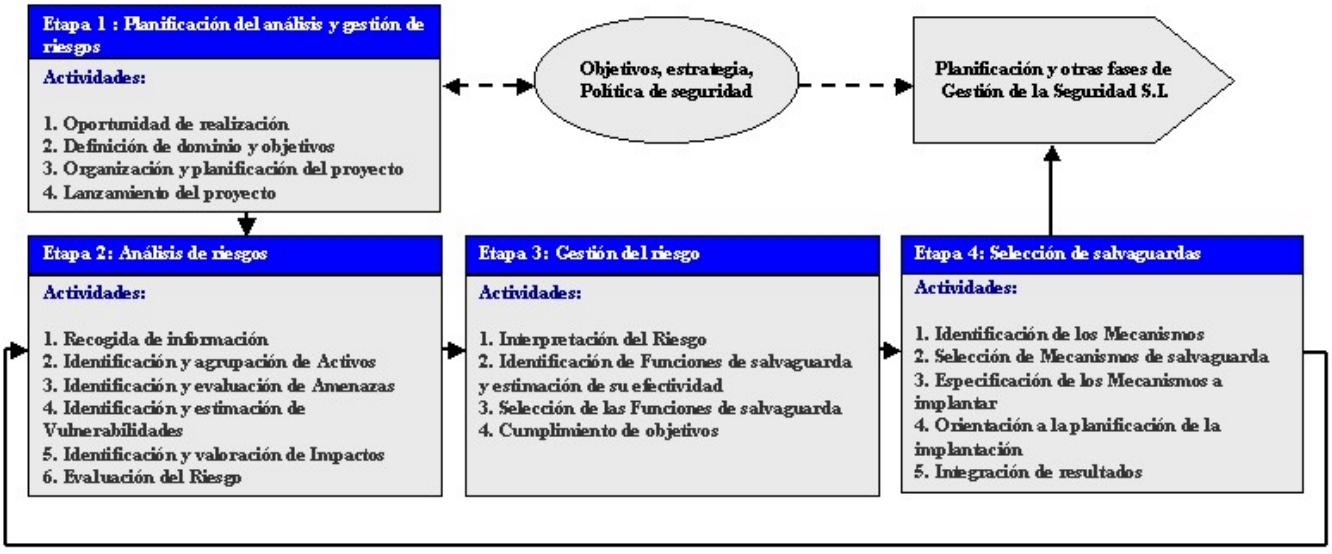
CONCEPTOS:

El proceso de análisis y gestión de riesgos constituye la tarea primera y a la vez esencial de toda actuación organizada en materia de seguridad. Permite conocer de manera rigurosa el estado de seguridad y determinar la valoración del riesgo. Es adecuado en las fases y actividades de carácter general (gestión global y política de seguridad con la implicación de la dirección) y en las de carácter específico de un determinado sistema de información (planificación, organización, implantación de salvaguardas, sensibilización, operación y mantenimiento).

Análisis de los riesgos: Identificación de las amenazas que acechan a los activos (componentes pertenecientes o relacionados con el sistema de información) y determinación de la vulnerabilidad de los activos ante esas amenazas. Con lo anterior se estima el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización a partir del cual se calcula el riesgo que se corre.

Gestión de los riesgos Selección e implantación de las medidas de seguridad o 'salvaguardas' 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.

El análisis y la gestión de los riesgos tiene como objetivo proporcionar evidencias racionales que permitan tomar decisiones acerca de la seguridad imprescindible para que las organizaciones puedan cumplir su misión.



MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Adoptar las medidas técnicas y de organización necesarias que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información teniendo 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. (RD 263/1996, art. 4.2)

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

- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal, 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. (LO 15/1999, art. 9.1).

CRITERIOS:

5.1 Se debe realizar el análisis y la gestión de riesgos aplicando MAGERIT, Metodología de análisis y gestión de riesgos de los sistemas de información, para determinar las medidas organizativas y técnicas adecuadas que salvaguardan la autenticidad, confidencialidad, integridad y disponibilidad de acuerdo con la proporcionalidad entre la naturaleza de los datos y los tratamientos, los riesgos a que están expuestos y el estado de la tecnología.

5.2 Se debe informar al propietario de la aplicación y de los ficheros de los riesgos detectados al objeto de que pueda tomar decisiones sobre la política de seguridad a seguir.

5.3 Los riesgos y las salvaguardas de la aplicación se deben revisar periódicamente, así como siempre que las circunstancias lo aconsejen, como una parte más de la gestión de la seguridad.

RECOMENDACIONES:

- Realizar en primer lugar un análisis cualitativo de los riegos aplicando técnicas matriciales que aporta MAGERIT, fáciles de manejar y de interpretar, incluso cuando se vaya a realizar el análisis cuantitativo de los riesgos, para asegurar la consistencia y coherencia del mismo. Para este análisis cualitativo se puede hacer uso de una matriz tal como la siguiente:

Impacto	RIESGO				
Muy alto	Alto	Muy alto	Muy alto	Muy alto	Muy alto
Alto	Medio	Alto	Alto	Alto	Alto
Medio	Bajo	Bajo	Medio	Medio	Medio
Bajo	Bajo	Bajo	Bajo	Medio	Medio
Muy bajo	Muy bajo	Muy bajo	Muy bajo	Muy bajo	Bajo
Vulnerabilidad	Muy baja	Baja	Media	Alta	Muy alta

Si bien esta matriz tiene cinco niveles en cada elemento componente, cuando se tienen pocos elementos para discriminar las vulnerabilidades y los impactos puede ser suficiente y recomendable manejarla reducida a los tres niveles bajo, medio y alto. E incluso se puede utilizar para realizar una discriminación dicotómica de los riesgos, al objeto de distinguir entre dos grandes grupos de activos, el que incluye activos que implican 'riesgos mayores', y que requieren una atención más focalizada, y el que incluye activos que implican 'riesgos menores', a los que bastará aplicar medidas de seguridad básicas.

- Realizar a continuación el análisis cuantitativo, en el que se pueden tener en cuenta las siguientes consideraciones:
  - Realizar la valoración de las variables que intervienen en el análisis y gestión de riesgos [Vulnerabilidad (V), % de Degradación, Impacto (I) (valor del activo x % de Degradación), % de Disminución de Vulnerabilidad (DV), % de Disminución de Impacto (DI)] en escalones predefinidos, por ejemplo 3 (Alto, Medio y Bajo), que permitan discriminar y distinguir entre lo más favorable y lo más desfavorable.
  - La transición del análisis cualitativo al cuantitativo se facilita asignando valores a los escalones cualitativos, adaptados a las necesidades del escenario en cuestión. Por ejemplo: para valores que se expresan como un porcentaje (Degradación, DV, DI, etc.): A=90 / M=45 / B=10.
  - La relación entre los activos y las amenazas es matricial, de forma que para cada par activo-amenaza cabe determinar la vulnerabilidad (V), el impacto (I) y el riesgo (R) según el producto R=V x I.

Activos / Amenazas	Amenaza 1	Amenaza 2	...
Activo 1	V=V11 I=I11 R11=V11*I11	V=V12 I=I12 R12=V12*I12	
Activo 2	V=V21 I=I21 R21=V21*I21	V=V22 I=I22 R22=V22*I22	
…			

Ejemplo:
I={A,M,B}
V ={A,M,B}
R ={A,M,B}

  - La relación entre las funciones de salvaguarda y las amenazas es asimismo matricial, de forma que para cada par función de salvaguarda-amenaza cabe determinar la disminución de vulnerabilidad (DV), la disminución de impacto (DI) y, consecuentemente, el riesgo residual:

    $Rr=V\ (1-DV)\ x\ I\ (1-DI)$

Funciones / Amenazas	Amenaza 1	Amenaza 2	...
Función 1	DV11=[A,M,B] DI11=[A,M,B]	DV12=[A,M,B] DI12=[A,M,B]	
Función 2	DV21=[A,M,B] DI21=[A,M,B]	DV22=[A,M,B] DI22=[A,M,B]	
…			

  - En la valoración de la Vulnerabilidad y el Impacto, en las relaciones Amenazas-Activos y Amenazas-Salvaguardas cabe trabajar con las siguientes hipótesis:
    - Dado un activo, suponer un mismo % de Degradación para todas las amenazas que actúan sobre él.

- Dada una amenaza, suponer una misma Vulnerabilidad con independencia de los activos sobre los que actúa.
- Dado un activo, suponer una misma Vulnerabilidad y % de Degradación para todas las amenazas que le afectan.
- Dada una amenaza, suponer una misma Vulnerabilidad y % de Degradación para todos los activos afectados.
- En las relaciones Funciones-Amenazas, dada una Función suponer una misma DV y DI para todas las amenazas sobre las que actúa; etc. En una segunda etapa realizar un ajuste fino sobre determinadas relaciones *Amenazas-Activos, Funciones-Amenazas*.

- En escenarios donde el nivel de abstracción dificulta una valoración precisa de los Activos cabe plantear asimismo varios escalones de magnitud con una hipótesis de cuantificación y asociar los activos a cada escalón en función del criterio por el que se les atribuye mayor o menor valor.

En un ciclo posterior se realiza un análisis y gestión de los riesgos más detallados y profundos, según lo demanda el proyecto de seguridad concreta, siguiendo las pautas de Magerit.

AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT); http://www.map.es/csi/pg5m20.htm
- ISO/IEC IS 17799 – Tecnologías de la información - Código de buenas prácticas para la gestión de la seguridad de la información *(Information technology – Code of practice for information security managment).*
- *INFORMATION TECHNOLOGY Baseline Protection Manual*; capítulo 3.2; http://www.bsi.bund.de/gshb/english/etc/inhalt.htm .
- ISO/IEC TR 13335 – Tecnologías de la información (TI) - Guía para la gestión de la seguridad de TI- Partes 1, 2, y 3.

6 Identificación y clasificación de activos a proteger

CRITERIOS:

6.1 Se debe realizar y mantener un inventario de los activos a proteger (información, equipamiento del sistema, soportes e información, otros equipos –climatización, alimentación, etc.-).

6.2 Para cada activo se debe identificar a su propietario, así como su valor e importancia en términos cuantitativos o cualitativos, en función de los requisitos de autenticidad, integridad, confidencialidad y disponibilidad que le son aplicables. Esta información es crucial, pues facilita el análisis y gestión de riesgos y, por tanto sirve, para determinar las medidas de seguridad proporcionadas.

6.3 En relación con los activos de tipo información, se debe documentar a qué usuarios se autoriza el acceso y los atributos relacionados con el referido acceso.

RECOMENDACIONES:

- Definir procedimientos de etiquetado y manipulación de la información para cada uno de los distintos niveles con los que se clasifica la información y las diferentes actividades: acceso, modificación, copia, almacenamiento, transmisión, y destrucción.

En el ámbito de la Administración General del Estado no existe, a la fecha, una norma común para la 'clasificación' de la información, al margen de las disposiciones relativas a los secretos oficiales. No obstante, a partir de los tres niveles de medidas de seguridad identificados por el RD 994/1999 (básico, medio y alto) y de su relación con los subestados de seguridad de autenticación, confidencialidad, integridad y sus escalas de valoración definidas en la Metodología de análisis y gestión de riesgos de los sistemas de información, MAGERIT (la disponibilidad tiene unas consideraciones especiales que se recogen en los capítulos '12. Disponibilidad', '16. Protección de soportes de información y copias de respaldo' en parte y '19. Plan de contingencias'), reflejados a su vez en la 'función' o 'necesidad de conocer', se recomienda la tabla siguiente.

Tipos de datos	Nivel	Autenticación	Confidencialidad	Integridad
Según función / Datos de carácter NO personal	-	Baja	Libre	Baja
Según función / Datos de carácter personal; ficheros que deben reunir las medidas de seguridad calificadas de nivel básico: • Todos los ficheros que contengan datos de carácter personal.	Básico	Normal	Restringida	Normal
Según función / Datos de carácter personal; ficheros que deben reunir las medidas de seguridad calificadas de nivel medio: • Comisión de infracciones administrativas o penales. • Hacienda Pública. • Servicios financieros. • Ficheros cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999. • Datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.	Medio	Alta	Protegida	Alta
Según función / Datos de carácter personal; ficheros que deben reunir las medidas de seguridad calificadas de nivel alto: • Datos de ideología, religión, creencias, origen racial, salud o vida sexual. • Datos recabados para fines policiales sin consentimiento de las personas afectadas.	Alto	Crítica	Confidencial	Crítica

Los Organismos que hayan de manejar documentos oficiales de la Unión Europea clasificados deberán ceñirse a lo dispuesto en:

- La Decisión del Consejo 2001/264/CE, de 19 de marzo de 2001, por la que se adoptan las normas de seguridad del Consejo, en vigor desde el 1 de diciembre de 2001.
- La Decisión de la Comisión, de 29 de noviembre de 2001, por la que se modifica su Reglamento interno; Anexo 'Disposiciones de la Comisión en materia de seguridad.

7 Salvaguardas ligadas al personal

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Se adoptarán las medidas de organización necesarias que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información. (RD 263/1996, art. 4.2)

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

- Informar al interesado respecto identidad y dirección del responsable del tratamiento. (LO 15/1999, art. 5.1)
- Definir medidas técnicas y organizativas. (LO 15/1999, art. 9.1)
- Establecer los requisitos de las personas que intervengan en el proceso de datos. (LO 15/1999, art. 9.3)
- El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo. (LO 15/1999, art. 10)
- Responsabilizar al encargado del tratamiento de los datos a utilizarlos de forma exclusiva a su finalidad, respondiendo de las infracciones en que hubiera incurrido. (LO 15/1999, art. 12.4)
- Garantizar el nivel de seguridad al fichero tratado cuando el tratamiento de datos de carácter personal se realiza fuera de los locales de la ubicación del fichero. (RD 994/1999, art. 6)
- Definir y documentar las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal. (RD 994/1999, art. 9.1)
- Adoptar las medidas necesarias, por parte del responsable del fichero, para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento. (RD 994/1999, art. 9.2)
- Designar uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. (RD 994/1999, art. 16)
- Limitar el acceso a los locales donde se encuentran ubicados los sistemas de información con datos de carácter personal, al personal autorizado en el documento de seguridad. (RD 994/1999, art. 19).

CRITERIOS:

7.1 Se deben definir y documentar las funciones y obligaciones del personal (Véase '*Organización y planificación de la seguridad*').

- Definir y documentar las funciones y obligaciones del personal, en particular en relación con el acceso y utilización de los sistemas de información y, en particular, en relación con el acceso a los datos de carácter personal.
- Definir las responsabilidades relacionadas con la seguridad en cada puesto de trabajo. Aplicar el principio de segregación de funciones.

7.2 Dar a conocer al personal las medidas de seguridad que afecten al desarrollo de sus funciones y que en su caso deban aplicar, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

- Se debe formar y concienciar al personal respecto sus obligaciones en materia de seguridad.

7.3 Dependiendo de los requisitos de la aplicación, se deben tener en cuenta los aspectos de seguridad en el proceso de asignación de puestos.

7.4 Se debe suministrar al personal que maneje datos de carácter personal u otra información cuya protección sea necesaria, el mobiliario adecuado para guardar la información (en soporte papel o electrónico).

7.5 Se debe controlar periódicamente la forma en que el personal que disponga algún tipo de obligación en relación con la seguridad de la información de la Organización, cumple este tipo de obligaciones.

7.6 Firmar acuerdos de confidencialidad en los casos de personal con contratos temporales o personal perteneciente a otras empresas subcontratadas, cuando la información que puedan manejar en el desempeño de sus obligaciones temporales sean datos de carácter personal.

RECOMENDACIONES:

- Garantizar que el usuario de con datos de carácter personal, esté sensibilizado respecto de los riesgos que puede implicar un tratamiento incorrecto de esta información. Asimismo, conviene instruir a los usuarios acerca de los detalles de la Política de Seguridad de la Organización que les afecten.

AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT); Guía de aproximación a la seguridad de los sistemas de información; capítulo 6; http://www.map.es/csi/pg5m20.htm
- ISO/IEC IS 17799 - Tecnologías de la información - Código de buenas prácticas para la gestión de la seguridad de la información *(Information technology – Code of practice for information security managment)*; capítulo 6.
- *INFORMATION TECHNOLOGY Baseline Protection Manual*; capítulo 3.2; http://www.bsi.bund.de/gshb/english/etc/inhalt.htm

- *Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook;* capítulo 10; http://csrc.nist.gov/publications/nistpubs/800-12/
- ISO/IEC TR 13335 - Tecnologías de la información (TI) - Guía para la gestión de la seguridad de TI; Partes 3 y 4.

8 Seguridad física

CONCEPTOS:

La seguridad física proporciona protección ante accesos no autorizados, daños e interferencias a las instalaciones de la organización y a la información.

Los requisitos sobre seguridad física varían considerablemente según las organizaciones y *dependen de la escala y de la organización de los sistemas de información*. Pero son aplicables a nivel general los conceptos de asegurar la protección de ciertas áreas, controlar perímetros, controlar las entradas físicas e implantar equipamientos de seguridad.

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Adoptar las medidas técnicas y de organización necesarias que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información. (RD 263/1996, art. 4.2)

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

- Autorizar la ejecución del tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero, por el responsable del fichero. (RD 994/1999, art. 6)
- Autorizar el acceso físico de forma exclusiva al personal autorizado en el documento de seguridad. (RD 994/1999, art. 19).

CRITERIOS:

8.1 Se debe situar el equipamiento que soporta a la aplicación así como los soportes de información en áreas seguras y protegidas adecuadamente.

8.2 Se debe definir de forma proporcionada las medidas que garanticen la seguridad de los locales a proteger en relación con los requisitos de seguridad de la información que se almacene o procese.

8.3 Se debe construir barreras físicas del suelo al techo para prevenir entradas no autorizadas o contaminación del entorno. Las ventanas y puertas de las áreas seguras deben estar cerradas y controlarse periódicamente. Las ventanas deben protegerse externamente. Se pueden necesitar barreras adicionales y perimetrales entre áreas con diferentes requisitos de seguridad dentro del perímetro global de seguridad.

8.4 Se debe construir las instalaciones de forma discreta y minimizar las indicaciones sobre su propósito, evitando signos obvios (fuera o dentro del edificio) que identifiquen la presencia de las actividades cuya seguridad se desea. No informar al personal que no esté directamente implicado de las actividades que se hacen dentro de las áreas seguras.

8.5 No se debe identificar en directorios telefónicos y de los vestíbulos de la organización las localizaciones informáticas (excepto las oficinas y áreas de recepción).

8.6 Se debe proteger los locales de amenazas potenciales:

- Eléctricas: realización de un proyecto eléctrico para la instalación, que asegure la independencia de las líneas eléctricas de los equipos de las líneas de fuerza (motores, alumbrado, etc.) del edificio, la seguridad de las personas y de los equipos mediante un adecuado diseño de los cuadros eléctricos y de las protecciones diferenciales ,magneto-térmicas y filtros, la disponibilidad mediante sistemas de alimentación ininterrumpida, equipos electrógenos, etc., el correcto estado del sistema de puesta a tierra del edificio, una correcta instalación de la malla de tomas a tierra en el falso suelo, una correcta canalización y protección de los cables, etc. La instalación de un suelo técnico adecuado, en sus características antiestáticas y conductoras, a los equipos y los riesgos de las labores que se realizan en la sala. La instalación de sistemas de alarmas efectivos ante contingencias.
- Incendios: cumplimiento de las normas relativas a protección de incendios, vigilando la señalización, prohibiciones de fumar, no acumulación de papel y la no ocupación de las vías de salida de emergencia. Instalación de sistemas de detección, alarma, y extinción de incendios, y su revisión periódica. Disponibilidad de armarios ignífugos para el almacenamiento de las copias de respaldo.
- Clima: instalar sistemas de control de la temperatura y de la humedad.
- Agua: instalar sistemas de detección y evacuación de agua. Elegir ubicación sin canalizaciones cercanas de agua.
- Interferencias: evitar interferencias electromagnéticas, como las provenientes de los dispositivos móviles, cebadores de los fluorescentes, etc.
- Agentes químicos: considerar el uso de protecciones especiales para equipamientos situados en ambientes particularmente agresivos
- Otros: elegir la ubicación evitando excesivas vibraciones. Control del polvo mediante limpieza regular y pinturas especiales para el suelo de la sala que evite su acumulación.

8.7 Se debe documentar debidamente los procedimientos de emergencia y revisar esta documentación de forma regular.

8.8 Se debe formar al personal en el funcionamiento de todos los sistemas instalados, realizando simulaciones de contingencias.

8.9 Se deben implantar medidas para proteger los cables de líneas de datos contra escuchas no autorizadas, contra daños (por ejemplo, evitando rutas a través de áreas públicas o fácilmente accesibles), o interferencias (por ejemplo, evitando recorridos paralelos y cercanos a líneas eléctricas). Instalar las líneas de suministro y telecomunicaciones para servicios de los sistemas de información en instalaciones comunes, subterráneas cuando sea posible, o tener medidas alternativas de protección adecuada.

8.10 Se debe ubicar los terminales que manejen información y datos sensibles en lugares donde se reduzca el riesgo de que aquellos estén a la vista.

8.11 Se debe almacenar los materiales peligrosos y/o combustibles a una distancia de seguridad del emplazamiento de los ordenadores. Por ejemplo, los suministros informáticos como el papel no se deben almacenar en la sala de ordenadores (hasta que se necesiten). Inspeccionar el material entrante, para evitar amenazas potenciales, antes de llevarlo al punto de uso o almacenamiento.

8.12 Se debe ubicar el equipamiento alternativo y copias de respaldo en sitios diferentes y a una distancia conveniente de seguridad. Estas copias de respaldo se almacenarán en armarios ignífugos (véase el Capítulo "Protección de soportes de información y copias de respaldo").

8.13 Se debe controlar la entrada en exclusiva al personal autorizado a las áreas que se hayan definido como áreas a ser protegidas. Autorizar sólo con propósitos específicos y controlados los accesos a estas áreas, registrando los datos y tiempos de entrada y salida. Obligar a todo el personal que lleve una identificación visible dentro del área segura y que observe e informe de la presencia de personal extraño al área. En éstas se deben prohibir los trabajos no autorizados en solitario para evitar la oportunidad de acción maliciosa. Cerrar la puerta externa del área, cuando la interna esté abierta.

8.14 Se debe restringir el acceso a las áreas seguras del personal de los proveedores o de mantenimiento a los casos en que sea requerido y autorizado. Aun con acceso autorizado deben restringirse sus accesos y controlarse sus actividades (especialmente en zonas de datos sensibles).

8.15 Se deben definir normas y controles relativos a la posible salida/entrada física de soportes de información (impresos, cintas y disquetes, CDs, etc.), así como de los responsables de cada operación.

RECOMENDACIONES:

En relación con la adecuación de locales:

- Separar las áreas de carga y descarga de material de las áreas a proteger. En caso de que esto no sea posible, se deberán establecer los controles adecuados para impedir accesos no autorizados. Restringir los accesos al área de carga y descarga desde fuera del edificio, al personal autorizado y debidamente identificado.

En relación con la instalación de líneas de telecomunicaciones:

- Considerar medidas adicionales para sistemas sensibles o críticos, como:
  - Instalación de conductos blindados, salas cerradas, etc.
  - Uso de rutas o medios de transmisión alternativos.

En relación con la ubicación de equipamiento, materiales y copias de respaldo:

- Situar en áreas seguras los equipos a proteger donde se minimicen los accesos innecesarios a las áreas de trabajo, distanciadas de las zonas de acceso público y de las zonas con aproximación directa de vehículos públicos. Definir perímetros de seguridad con las correspondientes barreras y controles de entrada. Su protección física debe impedir accesos no autorizados, daños y cualquier otro tipo de interferencias.

AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT); Guía de aproximación a la seguridad de los sistemas de información; capítulo 7; http://www.map.es/csi/pg5m20.htm
- ISO/IEC IS 17799 – Tecnologías de la información - Código de buenas prácticas para la gestión de la seguridad de la información *(Information technology – Code of practice for information security managment)*; capítulo 7.
- *INFORMATION TECHNOLOGY Baseline Protection Manual;* capítulo 4; http://www.bsi.bund.de/gshb/english/etc/inhalt.htm
- *Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook;* capítulo 15; http://csrc.nist.gov/publications/nistpubs/800-12/
- ISO/IEC TR 13335 – Tecnologías de la información (TI) - Guía para la gestión de la seguridad de TI; Partes 3 y 4.

9 Autenticación

CONSIDERACIONES:

En este capítulo se tratan los aspectos más estrechamente relacionados con la protección de la autenticación, sin perjuicio de que dicha protección reclama en general tener en cuenta al mismo tiempo a los otros tres subestados de la seguridad (autenticación, integridad o la disponibilidad). En cualquier caso, las medidas de protección han de ser proporcionadas a la naturaleza de los datos y de los tratamientos, los riesgos a los que están expuestos y el estado de la tecnología. En general será precisa la aplicación conjunta de parte o de todos los 'Criterios de seguridad'.

La *autenticación* se refiere a la capacidad de verificar que un usuario, convenientemente identificado, que accede a un sistema o aplicación es quien dice ser; o que un usuario que ha generado un documento o información es quien dice ser (mediante la firma electrónica, que tiene su propio capítulo aparte).

La identificación de los usuarios y la verificación de la autenticidad de la misma es un requisito previo a la *autorización* del acceso a los recursos del sistema.

Es conveniente apuntar que el proceso de autenticación de la identidad de las personas lleva asociado, de forma implícita, la manifestación de la voluntad de la misma, que se extiende a todas y a cada una de las operaciones que realice a partir de haberse identificado y autenticado su identidad, hasta que mediante una acción bien determinada, por ejemplo desconectándose de la sesión de trabajo, manifiesta su voluntad de no continuar.

Los criterios y recomendaciones que se exponen en este capítulo se refieren a los procedimientos genéricos de autenticación; para la firma electrónica véase el capítulo correspondiente.

CONCEPTOS:

Definiciones de autenticación:

- Procedimiento de comprobación de la identidad de un usuario. (RD 994/1999)
- Función para el establecimiento de la validez de la supuesta identidad de un usuario, dispositivo u otra entidad en un sistema de información o comunicaciones. (Directrices de la OCDE para una Política Criptográfica)
- Servicio de seguridad que se puede referir al origen de los datos o a una entidad homóloga. Garantiza que el origen de datos, o entidad homóloga, son quienes afirman ser. (ISO 7498-2)
- 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)
- Autenticación fuerte: autenticación basada en la utilización de técnicas de criptografía asimétrica y en el uso de certificados electrónicos. También suele referirse a la combinación de algo que el usuario posee (por ejemplo una tarjeta electrónica) con algo que el usuario conoce (como las claves conocidas como "PIN").
- Autenticación simple: autenticación basada en mecanismos tradicionales de usuario y contraseña.
- **Certificado reconocido**: los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en la Ley de Firma Electrónica, en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

NIVELES DE SEGURIDAD:

Su escala de cuatro niveles está ligada a la menor o mayor necesidad de formalización, de autorización y de responsabilización probatoria en el conocimiento o la comunicación de los activos:

- ***Baja***, si no se requiere conocer autor ni responsable / datos de carácter NO personal.
- ***Normal,*** si se requiere conocer autor para por ejemplo evitar el repudio de origen / datos a los que se aplican las medidas denominadas de nivel básico.
- ***Alta***, si se requiere además evitar el repudio en destino / datos a los que se aplican las medidas denominadas de nivel medio.
- ***Crítica***, si se requiere la certificación de autor y de contenido / datos a los que se aplican las medidas denominadas de nivel alto.

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades.

- Las medidas de seguridad deberán garantizar la restricción de su utilización y del acceso a los datos e informaciones en ellos contenidos a las personas autorizadas. (RD 263/1996, art.4.3)
- Las comunicaciones y notificaciones efectuadas en los soportes o a través de los medios y aplicaciones referidos en el apartado anterior serán válidas siempre que se identifique fidedignamente al remitente y al destinatario de la comunicación. (RD 263/1996, art.7.2)

En relación con la protección de datos de carácter personal:

Datos de carácter personal a los que se han de aplicar las medidas de nivel básico:

- Preparar una relación actualizada de usuarios que pueden acceder a un sistema de información y procedimientos de identificación y de autenticación. (RD 994/1999, art. 11.1)
- Definir un procedimiento de asignación, distribución y almacenamiento de contraseñas. (RD 994/1999, art. 11.2)
- Actualizar contraseñas y almacenarlas de forma ininteligible. (RD 994/1999, art. 11.3)

Datos de carácter personal a los que se han de aplicar las medidas de nivel medio y de nivel alto:

- Implantar un mecanismo que permita identificación de forma inequívoca y personalizada de cualquier usuario que intente acceder al sistema de información. (RD 994/1999, art. 18.1)
- Limitar el número de intentos de conexión fallidos. (RD 994/1999, art. 18.2)

CRITERIOS:

9.1 Se deben adoptar medidas de identificación y autenticación *proporcionadas* a la naturaleza de la información y de los tratamientos, de los riesgos a los que están expuestos y del estado del arte de la tecnología.

9.2 Se debe elaborar y mantener una lista de usuarios autorizados; éstos deben tener un conjunto de atributos de seguridad que puedan ser mantenidos individualmente.

9.3 Se debe asignar a cada usuario un identificador único para su uso exclusivo y personal, de forma que cualquier actuación suya pueda ser trazada. Con el identificador de usuario el administrador de seguridad debe poder identificar al usuario específico.

9.4 El sistema debe exigir que cada usuario se identifique y autentifique su identidad, antes de que se le permita realizar cualquier acción, para acceder a la aplicación y a otros recursos (también al puesto local, al servidor, al dominio de red, etc.).

9.5 La identificación y autenticación fuerte, se realizará mediante al menos un par de claves complementarias, una pública y otra privada, generadas con algoritmos de cifrado asimétrico RSA o equivalente, con una longitud mínima de clave de 1024 bits, acompañadas del correspondiente certificado reconocido de autenticidad que cumplirá las especificaciones x.509 v3 o superiores.

9.6 La autenticación basada en identificador de usuario y contraseña fija sólo es adecuada en el ámbito donde haya datos a los que haya que aplicar las medidas denominadas de nivel básico.

- El sistema debe permitir que los usuarios seleccionen sus contraseñas.
- La longitud de la contraseña no debe ser inferior a seis caracteres. El sistema debe exigir para la contraseña un determinado número de caracteres alfabéticos y otros numéricos.
- El sistema debe forzar el uso de contraseñas individuales.
- El sistema debe mantener registro de las últimas contraseñas para impedir que los usuarios las vuelvan a utilizar.
- El sistema debe obligar a cambiar las contraseñas temporales (dadas por la administración de seguridad) en la primera conexión válida que realice el usuario.
- El sistema almacenará las contraseñas de forma cifrada.
- Después de un determinado número de intentos fallidos (por ejemplo, 3) el sistema debe bloquear nuevos intentos. Se deben registrar los intentos fallidos de acceso.

- En caso de ser necesario las contraseñas deberán transmitirse de forma cifrada y firmada o por un canal seguro.
- La contraseña debe ser cambiada regularmente (por ejemplo, dependiendo de los requisitos de seguridad, bien cada seis meses, bien cada noventa días o bien cada treinta días). En caso de no cambiar la contraseña en el plazo establecido se denegará el acceso al usuario.
- El sistema evitará mostrar las contraseñas en pantallas o en impresos.
- El usuario debe estar informado de que las contraseñas no deben tener información de fácil conjetura (por ejemplo, fechas asociadas con el usuario o series regulares, números de teléfono, matrículas de coche, nombres de familiares o amigos, direcciones, números o letras solamente, repetición de caracteres seguidos, palabras del diccionario, etc.); de que no deben ser compartidas o dadas a conocer a otros usuarios; y de que las contraseñas deben ser memorizadas y nunca deben quedar escritas en un lugar de fácil acceso.

RECOMENDACIONES:

- La identificación y la autenticación basada en certificados sobre tarjeta inteligente criptográfica es recomendable: 1) para identificación y autenticación con efecto jurídico en las comunicaciones entre ciudadanos y Administración; 2) en el ámbito donde haya datos a los que haya que aplicar medidas de protección denominadas de nivel medio o alto.
- La autenticación basada en identificador de usuario y contraseña dinámica o de un solo uso puede ser recomendable en el ámbito donde haya datos a los que se hayan de aplicar medidas hasta las denominadas de nivel medio.
  - Las contraseñas generadas de forma aleatoria deben valer sólo para una vez.
  - La contraseña generada de forma dinámica debe ser superior a 6 caracteres.
- En caso de que se utilicen dispositivos de generación de contraseñas dinámicas:
  - Los dispositivos de generación de contraseñas dinámicas deben ser resistentes a accesos no autorizados y actuar al menos mediante la introducción por el usuario de un PIN de al menos de 4 caracteres. En circunstancias que así lo requieran puede ser de tipo biométrico (por ejemplo, huella dactilar,...).
  - El PIN debe ser siempre distinto al identificador de usuario.
  - Después de un número de intentos fallidos de entrada de PIN (por ejemplo, 3) el dispositivo de generación quedará bloqueado.
  - Debe existir un inventario de control de estos dispositivos y de los usuarios que los utilizan.
  - Cuando un usuario no requiere el acceso al sistema debe devolver el dispositivo de generación.
- La autenticación basada en certificados sobre soporte magneto/óptico puede darse en el ámbito de las medidas denominadas de nivel medio. En los diferentes tipos de soportes se requiere un mecanismo que asegure que sólo el usuario accede a su certificado, normalmente mediante la introducción de alguna clave (como PIN) que sólo él conoce.
- Evitar que el número de caracteres de la contraseña se pueda ver en la pantalla.

- Véase las mencionadas en el capítulo “Control de acceso”.
- Utilizar preferentemente sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido rigurosamente evaluados conforme a normas europeas o internacionales, como ISO/IEC 15408, y certificados por entidades independientes y de reconocida solvencia, como las recogidas en los acuerdos o arreglos internacionales de reconocimiento mutuo de los certificados de la seguridad de la tecnología de la información.

AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT); Guía de aproximación a la seguridad de los sistemas de información; capítulo 5.2; http://www.map.es/csi/pg5m20.htm
- ISO/IEC IS 17799 - Tecnologías de la información - Código de buenas prácticas para la gestión de la seguridad de la información *(Information technology – Code of practice for information security managment)*; capítulos 9.2 y 9.4.3.
- *Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook;* capítulo 16; http://csrc.nist.gov/publications/nistpubs/800-12/
- ISO/IEC TR 13335 - Guía para la gestión de la seguridad de TI.
- Páginas del Consejo Superior de Informática y para el impulso de la Administración Electrónica sobre evaluación y certificación: (http://www.map.es/csi/pg3410.htm)

SSLv3/TSL

- SSLv3 : http://home.netscape.com/eng/ssl3/index.html
- TSLv1: RFC 2246.

10 Confidencialidad

CONSIDERACIONES:

En este capítulo se tratan los aspectos más estrechamente relacionados con la protección de la confidencialidad, sin perjuicio de que dicha protección reclama en general tener en cuenta al mismo tiempo a los otros tres subestados de la seguridad (autenticación, integridad o la disponibilidad). En cualquier caso, las medidas de protección han de ser proporcionadas a la naturaleza de los datos y de los tratamientos, los riesgos a los que están expuestos y el estado de la tecnología. En general será precisa la aplicación conjunta de parte o de todos los ‘Criterios de seguridad’.

La confidencialidad de los datos exige medidas específicas también en su eliminación o de los soportes en los que hubieran estado almacenados, conforme a lo que se dice en el capítulo de “Medidas de almacenamiento y conservación”, de Criterios de Conservación. Sería el caso del cumplimiento de la obligación que tiene el servicio de dirección electrónica única de eliminar el contenido de las notificaciones una vez que venza el plazo de vigencia de las mismas.

CONCEPTOS:

Definiciones de confidencialidad:

- Condición que asegura que la información no puede estar disponible o ser descubierta por o para personas, entidades o procesos. La confidencialidad a menudo se relaciona con la intimidad cuando se refiere a personas físicas. (MAGERIT)
- Propiedad de la información que impide que ésta esté disponible o sea revelada a individuos, entidades o procesos no autorizados. (ISO 7498-2)
- Propiedad de que los datos o la información no estén disponibles, ni se revele, a personas, entidades o procesos no autorizados. (Directrices de la OCDE para una Política Criptográfica)
- El hecho de que los datos o informaciones estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada. (Directrices de la OCDE para la Seguridad de los Sistemas de Información)
- Prevención de la revelación no autorizada de información. (ITSEC)
- **Cifrado simétrico**: algoritmo de cifra tal que la clave para cifrar es igual a la de descifrar. La seguridad del proceso depende del secreto de la clave, no del secreto del algoritmo. El emisor y el receptor, deben compartir la misma clave utilizada para cifrar y descifrar, y ésta debe ser desconocida para cualquier otro individuo.
- **Cifrado asimétrico**: algoritmo de cifra tal que la clave utilizada para cifrar es distinta a la utilizada para descifrar. De estas dos claves una es conocida (clave pública), y otra parte permanece en secreto (clave privada).Lo fundamental de este sistema reside en la confianza de que una determinada clave pública corresponde realmente a quien proclama ser su propietario. Habitualmente se utilizan diferentes pares de claves para distintos fines (firma electrónica, autenticación electrónica, confidencialidad).
- **Definición de función resumen o *hash*:** función de un solo sentido que a partir de una cadena de bits de longitud arbitraria, calcula otra, aparentemente aleatoria, de longitud fija, normalmente un resumen. Se utiliza principalmente en la creación y verificación de la firma electrónica.
- **Certificado reconocido**: los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en la Ley de Firma Electrónica, en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

NIVELES DE SEGURIDAD:

Su escala usa los siguientes cuatro niveles:

- ***Libre***, sin restricciones en su difusión / datos de carácter NO personal.
- ***Restringida***, con restricciones normales / datos a los que se aplican las medidas denominadas de nivel básico.
- ***Protegida***, con restricciones altas / datos a los que se aplican las medidas denominadas de nivel medio.
- ***Confidencial***, no difundible por su carácter crítico / datos a los que se aplican las medidas denominadas de nivel alto.

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Adoptar las medidas técnicas y de organización necesarias que aseguren la confidencialidad de la información. (RD263/1996, art. 4.2)
- Los códigos o sistemas utilizados para garantizar la integridad y autenticidad de los documentos estarán protegidos de forma que únicamente puedan ser usados por las personas autorizadas por razón de sus competencias o funciones. (RD263/1996, art. 6.1)

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

- No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas. (LO 15/1999, art. 9.2)
- El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo. (LO 15/1999, art. 10)
- Se cifrarán los datos de carácter personal a los que deban aplicarse medidas de nivel alto en su transmisión a través de redes de telecomunicaciones. (RD 994/1999, art. 26).

CRITERIOS:

10.1 Se debe cifrar la información cuando la naturaleza de los datos y de los tratamientos y los riesgos a los que estén expuestos lo requiera, tanto en transacciones o comunicaciones como en almacenamiento, en particular cuando se trate de datos de carácter personal a los que haya que aplicar las medidas de nivel alto. *Información dinámica*: En los intercambios entre puestos, servidores y otros dispositivos, así como en transacciones electrónicas y transmisiones a través de redes de telecomunicaciones. *Información estática*: En servidores, en soportes electrónicos de información o en ordenadores personales o estaciones de trabajo de los usuarios.

10.2 Los algoritmos deben permitir una longitud mínima de claves de 128 bits, y se utilizarán preferentemente 3DES, IDEA, RC4, RC5, AES, o equivalentes.

10.3 Para el establecimiento de sesión web cifrada se debe utilizar el protocolo SSL v3/TLS v1 o superior con cifrado simétrico de, al menos, 128 bits.

10.4 En correo electrónico seguro se debe utilizar el estándar S/MIME v2 o superior.

10.5 En sesiones de administración remota se debe utilizar SSH.

10.6 Se deben implantar procedimientos de apoyo a los mecanismos de cifrado (control de acceso físico y lógico, autenticación, gestión de claves, etc.) para evitar la divulgación no autorizada de la información almacenada en dispositivos y soportes electrónicos o en tránsito a través de redes de telecomunicaciones.

10.7 El borrado de los datos debe realizarse mediante mecanismos adecuados, como por ejemplo los basados en ciclos de reescritura de los ficheros. El procedimiento de borrado tendrá en cuenta la naturaleza de los datos o al riesgo aparejado a su desvelamiento.

10.8 Para salvaguarda de la confidencialidad se debe tener en cuenta también lo previsto en los capítulos 'Seguridad física', 'Autenticación', 'Control de acceso', 'Acceso a través de redes' y 'Protección de los soportes de información y copias de respaldo'.

10.9 Cuando el mecanismo de protección de la confidencialidad en las comunicaciones de la Administración con el ciudadano utilice algoritmos de clave pública, además de los de clave simétrica, el par de claves complementarias, pública y privada han de ser independientes de los utilizados para autenticidad. Serán de RSA o equivalente, longitud mínima de clave de 1024 bits y certificado reconocido conforme con la norma UIT X.509 v3 o versiones posteriores.

La Administración deberá informar al ciudadano de las medidas que permitan descifrar la información.

RECOMENDACIONES:

- El intercambio de una clave simétrica de cifrado debe realizarse bien por un canal seguro o bien después de cifrarla con criptografía asimétrica.
- Un sistema de gestión de claves criptográficas debe basarse en un conjunto de estándares, procedimientos y métodos para:
  - Generar las claves en los distintos sistemas y aplicaciones.
  - Proteger físicamente los dispositivos de generación, almacenamiento y archivo de claves.
  - Proteger la confidencialidad de las claves privadas frente a su divulgación no deseada y su modificación o destrucción.
  - Proteger las claves públicas frente a su modificación o destrucción.
  - Generar y obtener certificados de clave pública.
  - Distribuir las claves a los distintos usuarios incluyendo la forma de activación de claves cuando se reciben.
  - Almacenar las claves incluyendo la forma en que los usuarios autorizados pueden acceder a ellas.
  - Cambiar y actualizar las claves incluyendo las normas relativas a la forma de realizar los cambios.
  - Actuar ante situaciones en las que se ha violado una clave privada.
  - Revocar las claves incluyendo su desactivación y anulación.
  - Recuperar de claves en caso de pérdida o corrupción.
  - Archivar las claves para la información respaldada en distintos medios de almacenamiento.
  - Destruir las claves.
  - Crear un diario de actividades relacionadas con la administración de claves, para su utilización con fines de auditoría.
- Aplicar cifrado integral del disco duro para la protección de la confidencialidad de la información contenida en equipos portátiles y en otros equipos que puedan contener información que requiera confidencialidad.

- Aplicar cifrado en los soportes removibles (por ejemplo, disquetes, CD-ROM, dispositivos SCSI) que puedan contener información que requiere salvaguarda de la confidencialidad.
- En circunstancias excepcionales, cabe recurrir a equipos de baja radiación electromagnética (con protección denominada *Tempest*).
- Utilizar preferentemente sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido rigurosamente evaluados conforme a normas europeas o internacionales, como ISO/IEC 15408, y certificados por entidades independientes y de reconocida solvencia, como las recogidas en los acuerdos o arreglos internacionales de reconocimiento mutuo de los certificados de la seguridad de la tecnología de la información.

AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT); Guía de aproximación a la seguridad de los sistemas de información y Guía de procedimientos; http://www.map.es/csi/pg5m20.htm
- ISO/IEC TR 13335 – Tecnologías de la información (TI) - Guía para la gestión de la seguridad de TI; Parte 4; capítulo 10.2.
- Páginas del Consejo Superior de Informática y para el impulso de la Administración Electrónica sobre evaluación y certificación: (http://www.map.es/csi/pg3410.htm).
- Algoritmos Criptográficos citados
- TSL/SSL
- SSH

EJEMPLOS DE SOLUCIÓN TÉCNICA PARA CONFIDENCIALIDAD:

Protección de la confidencialidad de información estática:

- El mercado ofrece soluciones hardware y software para el cifrado de información en soportes electrónicos utilizando diversas técnicas criptográficas, basadas o no en la utilización de una infraestructura de clave pública.
- Por otra parte, los archivos e información deben encontrarse en soportes protegidos ante accesos físicos y lógicos de personas no autorizadas. Esta protección se puede conseguir mediante salvaguardas que impiden el acceso físico a los soportes (discos duros y otros soportes electrónicos de la información), además de las salvaguardas consistentes en cifrar la información contenida en dichos soportes.

Protección de la confidencialidad de información dinámica (mensajes, transacciones, acceso a webs, etc.):

- Utilización de IPSec para comunicación autenticada y cifrada entre encaminadores, cortafuegos y en la combinación de ambos.
- El estándar IPsec se diseñó para dar seguridad en comunicaciones que utilicen protocolos de transmisión IP, tanto IPv4 como IPv6. Los servicios que suministra Ipsec se aplican en control de acceso, integridad en el tráfico "sin conexión", autenticación de origen, protección contra transmisión reiterativa y confidencialidad. Estos servicios son suministrados a nivel IP, por lo que

suministran protección para cualquier servicio realizado con la ayuda de protocolos de niveles superiores al nivel IP.

11 Integridad

CONSIDERACIONES:

En este capítulo se tratan los aspectos más estrechamente relacionados con la protección de la integridad, sin perjuicio de que dicha protección reclama en general tener en cuenta al mismo tiempo a los otros tres subestados de la seguridad (autenticación, integridad o la disponibilidad). En cualquier caso, las medidas de protección han de ser proporcionadas a la naturaleza de los datos y de los tratamientos, los riesgos a los que están expuestos y el estado de la tecnología. En general será precisa la aplicación conjunta de parte o de todos los 'Criterios de seguridad'.

La integridad se puede proteger mediante la firma electrónica, de la que se ocupa otro capítulo.

CONCEPTOS:

Definiciones de integridad:

- Condición de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado. La integridad está ligada a la fiabilidad funcional del sistema de información, a su eficacia para cumplir las funciones del sistema. (MAGERIT)
- Propiedad de que los datos o la información no hayan sido modificados o alterados de forma no autorizada. (Directrices de la OCDE para una Política Criptográfica)
- El hecho de que de los datos o informaciones sean exactos y completos y la preservación de este carácter exacto y completo. (Directrices de la OCDE para la Seguridad de los Sistemas de Información)
- Seguridad que la información, o los datos, están protegidos contra modificación o destrucción no autorizada, y certidumbre de que los datos no han cambiado de la creación a la recepción.
- Prevención de la modificación no autorizada de información. (ITSEC)
- Propiedad de los datos que garantiza que éstos no han sido alterados o destruidos de modo no autorizado. (ISO 7498-2).

Fechado electrónico

- Sirve de evidencia de la existencia de un documento y liga dicho documento a un instante temporal determinado.

NIVELES DE SEGURIDAD:

Su escala usa cuatro niveles referibles a la facilidad mayor o menor de reobtener el activo con calidad suficiente, o sea completo y no corrompido para el uso que se desea darle:

- ***Baja,*** si se puede reemplazar fácilmente con un activo de igual calidad / datos de carácter no personal.

- ***Normal,*** si se puede reemplazar con un activo de calidad semejante con una molestia razonable / datos a los que se aplican las medidas denominadas de nivel básico.
- ***Alta,*** si la calidad necesaria es reconstruible difícil y costosamente / datos a los que se aplican las medidas denominadas de nivel medio.
- ***Crítica,*** si no puede volver a obtenerse una calidad semejante / datos a los que se aplican las medidas denominadas de nivel alto.

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Adoptar las medidas técnicas y de organización necesarias que aseguren integridad de la información. (RD263/1996, art. 4.2)
- Los documentos emitidos por los órganos y entidades del ámbito de la Administración General del Estado y por los particulares en sus relaciones con aquéllos, que hayan sido producidos por medios electrónicos, informáticos y telemáticos en soportes de cualquier naturaleza serán válidos siempre que quede acreditada su integridad, conservación y la identidad del autor, así como la autenticidad de su voluntad, mediante la constancia de códigos u otros sistemas de identificación.
- En los producidos por los órganos de la Administración General del Estado o por sus entidades vinculadas o dependientes, dichos códigos o sistemas estarán protegidos de forma que únicamente puedan ser utilizados por las personas autorizadas por razón de sus competencias o funciones. (RD263/1996, art. 6.1)
- Las copias de documentos originales almacenados por medios o en soportes electrónicos, informáticos o telemáticos, expedidas por los órganos de la Administración General del Estado o por sus entidades vinculadas o dependientes, tendrán la misma validez y eficacia del documento original siempre que quede garantizada su autenticidad, integridad y conservación. (RD263/1996, art. 6.2).

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

- Asegurar que los datos de carácter personal sean exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. (LO 15/1999, art. 4.3)
- Cumplir las condiciones con respecto a su integridad para registrar los datos de carácter personal. (LO 15/1999, art. 9.2)
- Identificar al usuario con acceso autorizado. (RD 994/1999, art. 11.1)
- Crear un mecanismo basado en contraseñas que garantice integridad de los datos de carácter personal. (RD 994/1999, art. 11.2)
- Cambiar las contraseñas para proteger integridad de los datos de carácter personal. (RD 994/1999, art.11.3)
- En medidas de nivel básico:

  Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. (RD 994/1999, art. 14.2)
- En medidas de nivel alto:

De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. (RD 994/1999, art. 24.1)

- En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido. (RD 994/1999, art. 24.2)
- Los mecanismos que permiten el registro de los datos detallados en los párrafos anteriores estarán bajo el control directo del responsable de seguridad competente sin que se deba permitir, en ningún caso, la desactivación de los mismos. (RD 994/1999, art. 24.3)
- El período mínimo de conservación de los datos registrados será de dos años. (RD 994/1999, art. 24.4)
- El responsable de seguridad se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes. (RD 994/1999, art. 24.5)
- Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en este Reglamento. (RD 994/1999, art. 25).

CRITERIOS:

11.1 Se deben implantar procedimientos de explotación de la aplicación y de los sistemas adecuados a la protección de la integridad.

11.2 Se deben implantar procedimientos de copias de respaldo de ficheros y bases de datos, y de protección y conservación de soportes de información.

11.3 Se deben generar copias de los documentos emitidos en soportes no reescribibles de tipo 'múltiple lectura única escritura' (WORM), como, por ejemplo, CD-ROM o DVD (Véase en '*Criterios de Conservación*', en el capítulo '*Soportes*' el apartado '*Tipos de soportes de almacenamiento de la información*').

11.4 Se deben aplicar técnicas de comprobación de la integridad de la información: funciones resumen o hash, firma electrónica, etc. (en particular a documentos y mensajes) para verificar la integridad de la misma y, en su caso, de fechado electrónico.

11.5 Se deben proteger los archivos de información mediante el atributo de solo lectura.

11.6 En las aplicaciones que ejecuten transacciones o procesos donde se produzcan múltiples actualizaciones de datos que se encuentren relacionados entre sí, se deben adoptar herramientas o procedimientos que aseguren la integridad de estos datos en el caso de que se produzca un fallo de proceso y no se pueda completar la transacción.

11.7 Se debe realizar un análisis periódico de los accesos y de los recursos utilizados.

11.8 Se deben adoptar medidas de protección frente a código dañino en los servidores de aplicación, en los equipos de los usuarios y en los soportes circulantes (disquetes, CD's, otros):

- Se deben instalar exploradores del software, con actualización periódica.
- Se deben aplicar procedimientos para evitar la instalación de software no autorizado por la organización, para evitar la utilización de programas no deseados, para control

de la navegación por internet, etc. Esto se puede implementar, por ejemplo, con software libre.

11.9 Se debe aplicar el fechado electrónico a los documentos o información cuya fecha y hora se desea acreditar. La sincronización de la fecha y la hora se deberá realizar con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992 de 23 de octubre y según las condiciones técnicas y protocolos que el citado Organismo establezca. En particular los registros telemáticos y los servicios de notificación electrónica deben adoptar servicios de fechado electrónico para la acreditación de fecha y hora.

RECOMENDACIONES:

En relación con la protección contra el código dañino cabe adoptar las siguientes medidas:

- Comprobadores de integridad del software. El punto más vulnerable de un sistema informático es la plataforma cliente. El sistema operativo más extendido en los puestos de trabajo puede ser fácilmente manipulado, por un virus, un caballo de Troya o una persona. Para comprobar que elementos tales como las DLL, *drivers* y ejecutables no han sido alterados cabe aplicar técnicas de comprobación de la integridad a las aplicaciones.

Recomendaciones de carácter general:

- Para salvaguarda de la integridad se debe tener en cuenta también lo previsto en los capítulos 'Seguridad física', 'Autenticación', 'Control de acceso', 'Acceso a través de redes' y 'Protección de los soportes de información y copias de respaldo'.
- Se deben aplicar procedimientos para evitar la instalación de software no autorizado por la organización, para evitar la utilización de programas no deseados, para control de la navegación por internet; etc.
- Utilizar preferentemente sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido rigurosamente evaluados conforme a normas europeas o internacionales, como ISO/IEC 15408, y certificados por entidades independientes y de reconocida solvencia, como las recogidas en los acuerdos o arreglos internacionales de reconocimiento mutuo de los certificados de la seguridad de la tecnología de la información.

AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT); distintos capítulos de la Guía de aproximación a la seguridad de los sistemas de información y de la Guía de procedimientos; http://www.map.es/csi/pg5m20.htm
- ISO/IEC TR 13335 Tecnologías de la información (TI) - Guía para la gestión de la seguridad de TI; Parte 4; capítulos 8.2.3, 10.3.
- *Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook;* capítulo 16; http://csrc.nist.gov/publications/nistpubs/800-12/
- Relación de productos certificados desde la constitución del Comité de Gestión del Acuerdo de Reconocimiento Mutuo de Certificados: (http://www.map.es/csi/pg3410.htm)

- Página del Consejo Superior de Informática y para el impulso de la Administración Electrónica dedicada a virus informáticos: http://www.map.es/csi/pg7060.htm
- Orden de 3 de diciembre de 1999, de la Consellería de Justicia y Administraciones Públicas, por la que se aprueba el Reglamento Técnico de Medidas de Seguridad para la Aprobación y Homologación de Aplicaciones y Medios de Tratamiento Automatizado de la Información. (Generalitat Valenciana).

EJEMPLO

La aplicación de la firma electrónica a la integridad viene del hecho de que está vinculada al firmante de manera única, permite la identificación del firmante y está vinculada a los datos a los que se refiere de modo que cualquier cambio ulterior sea detectable. Así, proporciona las siguientes características:

- *Autenticación del emisor u origen del documento*, de forma que no haya posibilidad de enviar información sustituyendo de forma fraudulenta al emisor u origen.
- Integridad del contenido.
- *No repudio del origen*, de forma que no se pueda denegar el haber enviado u originado una información dada.

Otros aspectos como:

- *Autenticación del receptor o destinatario del documento*, de forma que el emisor tenga certeza de que sólo recibe la información el receptor destinatario de la misma;
- *No repudio del destino*, de forma que no se pueda denegar el haber recibido una información dada;

Requieren además el archivo de la información intercambiada junto con la fecha, la firma electrónica del emisor o del receptor o de ambos posiblemente a su vez, bajo la firma electrónica de una tercera parte de confianza.

Para la aplicación de la huella electrónica a los documentos electrónicos se aplican funciones resumen o *hash* a partir de datos tales como el contenido del documento electrónico, la fecha y hora de generación del documento electrónico. Esta huella electrónica puede estar incluida en el propio documento, almacenarse en un campo de base de datos vinculado al documento, etc.

12 Disponibilidad

CONSIDERACIONES:

En este capítulo se tratan los aspectos más estrechamente relacionados con la protección de la disponibilidad, sin perjuicio de que dicha protección reclama en general tener en cuenta al mismo tiempo a los otros tres subestados de la seguridad (autenticación, integridad o la disponibilidad). En cualquier caso, las medidas de protección han de ser proporcionadas a la naturaleza de los datos y de los tratamientos, los riesgos a los que están expuestos y el estado de la tecnología. En general será precisa la aplicación conjunta de parte o de todos los 'Criterios de seguridad'.

Se ha de tener en cuenta que en la disponibilidad intervienen múltiples aspectos: unas adecuadas instalaciones y equipamiento físico, un adecuado dimensionamiento de la plataforma tecnológica que permita hacer frente a escenarios variables de carga de trabajo, o posibles fallos, procedimientos de explotación y de mantenimiento, protección contra código dañino y frente a intentos de intrusión o ataques de denegación de servicio, así como procedimientos relativos a la gestión de la información que pueda almacenarse cifrada o codificada que garanticen la gestión de claves. La eliminación de errores de codificación y la adopción de estándares y especificaciones públicas de programación pueden facilitar el control de la aplicación (software libre).

Las medidas para salvaguardar la disponibilidad pueden tener mayor rigor que el que con carácter general se recoge en los criterios. Sería el caso de los registros telemáticos y los sistemas de notificación electrónica única, los cuales han de implantar medidas organizativas y técnicas para salvaguarda de la disponibilidad que debe cubrir el servicio 7 días a la semana y 24 horas al día.

CONCEPTOS:

Definiciones de disponibilidad:

- Grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Situación que se produce cuando se puede acceder a un sistema de información en un periodo de tiempo considerado aceptable. La disponibilidad está asociada a la fiabilidad técnica de los componentes del sistema de información. (MAGERIT)
- Propiedad que requiere que los recursos de un sistema abierto sean accesibles y utilizables a petición de una entidad autorizada. (ISO 7498-2)
- Prevención de una negación ilícita de acceso a la información o a los recursos. (ITSEC).

NIVELES DE SEGURIDAD:

Su escala emplea cuatro niveles definidos por el período de ***tiempo máximo de carencia*** del activo. Por ejemplo, para los sistemas de gestión habituales la escala suele ser la siguiente:

- ***Menos de una hora***, considerado como fácilmente recuperable.
- ***Hasta un día laborable***, coincidente con un plazo habitual de recuperación con ayuda telefónica de especialistas externos o de reposición con existencia local.

- ***Hasta una semana,*** coincidente con un plazo normal de recuperación grave con ayuda presencial de especialistas externos, de reposición sin existencia local o con el arranque del centro alternativo.
- ***más de una semana,*** considerado como interrupción catastrófica.

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Adoptar las medidas técnicas y de organización necesarias que aseguren disponibilidad de la información. (RD263/1996, art. 4.2).

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

- Registro de datos de carácter personal en ficheros que no reúnan las condiciones de seguridad. (LO 15/1999, art. 9.2)
- El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos. (LO 15/1999, art. 15.1)
- La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. (LO 15/1999, art. 15.2)
- Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. (RD 994/1999, art. 14.2)
- Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. (RD 994/1999, art. 14.3)
- Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en este Reglamento. (RD 994/1999, art. 25).

CRITERIOS:

12.1 Se deben adoptar los procedimientos de explotación que garanticen la fiabilidad de la aplicación y de los soportes en los que resida la información.

- Se deben adoptar medidas de seguridad física (Véase capítulo '*Seguridad física*').
- Se deben adoptar medidas de protección física del cableado.
- Se deben mantener actualizadas las listas de vulnerabilidades del software instalado, consultando para ello las fuentes precisas.
- Se debe actualizar periódicamente o cuando sea necesario el software de base y aplicar las correcciones a debilidades de éste.

- Se deben diseñar de forma adecuada las redes (Véase capítulo 'Acceso a través de redes').

12.2 Los equipos que soporten la aplicación y cuya interrupción accidental pueda provocar alteración o pérdida de datos o documentos administrativos, deben estar protegidos contra fallos de suministro eléctrico mediante sistemas de alimentación ininterrumpida.

12.3 Si la naturaleza de los tratamientos y de los datos lo hacen apropiado, se deben implantar equipos dotados de mecanismos tolerantes a fallos.

- Se debe contar con suministro eléctrico duplicado.
- Se debe contar con hardware duplicado.

12.4 Los equipos deben mantenerse de acuerdo con las especificaciones de los suministradores respectivos.

12.5 Se deben adoptar las medidas apropiadas de seguridad física en el entorno donde se encuentren los equipos que den soporte a la aplicación. (Véase capítulo 'Seguridad física')

12.6 Se deben proteger los sistemas y las aplicaciones contra el código dañino. Cabe adoptar las siguientes medidas:

- Se han de instalar exploradores del software debidamente actualizados.
- Se deberán implantar medidas para el control de los soportes circulantes (disquetes, CD's, discos magneto ópticos o cualquier otro).
- Se han de implantar procedimientos de protección y vigilar su funcionamiento de mecanismos capaces de evitar la instalación de software no autorizado por la organización, o evitar la utilización de programas no deseados o para control de la navegación por internet, así como cualquier otro que la evolución de las amenazas o de la tecnología hagan necesarios.

12.7 Se deben proteger los sistemas y las aplicaciones contra los ataques de denegación de servicio.

12.8 Se deberá preparar y mantener operativo un plan de contingencias. (Véase capítulo 'Plan de contingencias').

RECOMENDACIONES:

En relación con procedimientos y mecanismos para salvaguarda de la disponibilidad:

- En función de la naturaleza de los datos y de los tratamientos recurrir a la redundancia de equipos y a los equipos tolerantes a fallos, teniendo en cuenta asimismo los aspectos relativos a la carga.
- En la medida en que el mercado los proporcione, conviene utilizar mecanismos que comprueben la integridad del software

Otras recomendaciones de carácter general:

- Para salvaguarda de la disponibilidad se debe tener en cuenta también lo previsto en los capítulos 'Seguridad física', 'Autenticación', 'Control de acceso', 'Acceso a través de redes', 'Protección de los soportes de información y copias de respaldo', 'Gestión y registro de incidencias' y 'Plan de contingencias'.
- Utilizar preferentemente sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido rigurosamente evaluados conforme a normas europeas o internacionales, como ISO/IEC 15408, y certificados por entidades independientes y de reconocida solvencia, como las

recogidas en los acuerdos o arreglos internacionales de reconocimiento mutuo de los certificados de la seguridad de la tecnología de la información.

AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT); distintos capítulos de la Guía de aproximación a la seguridad de los sistemas de información y de la Guía de procedimientos; http://www.map.es/csi/pg5m20.htm
- ISO/IEC TR 13335 – Tecnologías de la información (TI) - Guía para la gestión de la seguridad de TI; Parte 4; capítulo 10.4.
- Páginas del Consejo Superior de Informática y para el impulso de la Administración Electrónica sobre de la seguridad de la tecnología de la información: (http://www.map.es/csi/pg3410.htm)
- Página del Consejo Superior de Informática y para el impulso de la Administración Electrónica dedicada a virus informáticos: http://www.map.es/csi/pg7060.htm

13 Control de acceso

CONSIDERACIONES:

El control de acceso es una función de seguridad esencial para proteger los datos y los tratamientos de posibles manipulaciones no autorizadas. En el control de acceso intervienen diversos componentes:

- Identificación y autenticación de usuarios. (Véase '*Autenticación*')
- Autorización de derechos de acceso a distintos recursos del sistema.
- Acceso a redes, sistemas, aplicaciones, datos. (Véase '*Acceso a través de redes*')
- Control y auditoría de acceso. (Véase '*Auditoría y control de la seguridad*')

Se entienden por privilegios (de acceso) los mecanismos de salvaguarda que permiten a ciertos usuarios alterar los controles de seguridad del sistema o de las aplicaciones. La asignación de privilegios especiales innecesarios es una de las causas de vulnerabilidad más frecuentes en los sistemas que han sufrido ataques, por lo que se deberá controlar mediante un procedimiento formal de autorización de privilegios.

El acceso por usuarios externos a la organización da lugar a riesgos si el acceso se produce desde localizaciones con un nivel de seguridad inadecuado. En los casos en los que la organización tenga que permitir este acceso, por necesidad del servicio, debe llevar a cabo un análisis de riesgos específico para determinar las salvaguardas a implantar; salvaguardas que deberán acordarse con la otra parte y, en su caso, definirse mediante convenio o contrato.

El acceso por terceros no se autorizará hasta que no se hayan implantado las salvaguardas de protección específicas y firmado el contrato de acuerdo con los terceros estableciendo las características del acceso. El contrato debe especificar los requisitos de seguridad de tales accesos, contener los criterios y las condiciones de seguridad específicos.

CONCEPTOS:

Definiciones de control de acceso:

- Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos. (RD 994/1999)
- Servicio de seguridad que previene el uso de un recurso salvo en casos y de manera autorizada. (ISO 7498-2).

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Adoptar medidas técnicas y de organización necesarias que aseguren la autenticidad, confidencialidad, integridad y disponibilidad. (RD263/1996, art. 4.2)
- Proteger códigos o sistemas de forma que sólo puedan ser utilizados por las personas autorizadas por razón de sus competencias o funciones. (RD263/1996, art. 6.1)
- Implantar las medidas de seguridad tendentes a evitar la interceptación y alteración de las comunicaciones así como los accesos no autorizados. (RD263/1996, art. 7.1.c)
- Contar con las medidas de seguridad que garanticen la integridad, autenticidad, protección de los documentos almacenados. En particular asegurarán la identificación de los usuarios y el control de accesos. (RD263/1996, art. 8.4)

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

- Almacenar los datos de carácter personal de forma que permitan el ejercicio del derecho de acceso. (LO 15/1999, art. 4.6)
- Prohibir la recogida (acceso) de datos por medios fraudulentos, desleales, o ilícitos. (LO 15/1999, art. 4.7)
- Asegurar que los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. (LO 15/1999, art. 11)
- Garantizar el acceso a través de redes de comunicaciones con una seguridad equivalente al acceso en modo local. (RD 994/1999, art. 5)
- Permitir acceso de los usuarios únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones. (RD 994/1999, art. 12.1)
- Establecer mecanismos por parte del responsable del fichero para evitar que un usuario pueda acceder a datos o recursos con derechos distintos a los autorizados. (RD 994/1999, art. 12.2)
- Identificar los usuarios que tengan acceso autorizado. (RD 994/1999, art. 12.3)
- Identificar en el documento de seguridad al personal que pueda conceder, alterar o anular acceso a datos o recursos, conforme los criterios establecidos por el responsable del fichero. (RD 994/1999, art. 12.4)

En medidas de nivel medio:

- Establecer por parte del responsable del fichero, un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado. (RD 994/1999, art. 18.1)

- Limitar la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información. (RD 994/1999, art. 18.1)

En medidas de nivel alto:

- Guardar como mínimo para cada acceso, la identificación del usuario, la fecha y la hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. (RD 994/1999, art. 24.1)
- En el caso que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido. (RD 994/1999, art. 24.2)
- Poner bajo control directo del responsable de seguridad competente los mecanismos mencionados en los dos párrafos anteriores, sin que se deba permitir, en ningún caso, la desactivación de los mismos. (RD 994/1999, art. 24.3)
- Conservar los datos registrados durante un periodo mínimo de dos años. (RD 994/1999, art. 24.4)
- Revisar por parte del responsable de seguridad competente de forma periódica, la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes. (RD 994/1999, art. 24.5).

CRITERIOS:

13.1 Se deben adoptar procedimientos en relación con la identificación y autenticación de usuarios, la gestión y revisión de derechos y privilegios de acceso de los usuarios, la comprobación de los accesos .

- Se deben seguir los criterios incluidas en el capítulo 'Autenticación'.
- Se debe implantar un procedimiento formalizado de registro de altas y bajas de acceso de usuarios a todos los servicios de la aplicación y del sistema, de manera que se garantice que no se proporcione acceso al sistema hasta que se hayan completado los procedimientos de autorización y que se compruebe que el usuario tiene la autorización del responsable (propietario) del servicio para utilizarlo.
- Se debe verificar que el nivel de acceso asignado al usuario corresponde a necesidades de funcionamiento de la Organización y es consistente con la normativa de seguridad de la Organización y que no se contradice con el principio de segregación de funciones (según grupos de usuarios, servicios y sistemas de información).
- Se debe informar a cada usuario de todos sus derechos de acceso, los cuales ha de reconocer como conocidos de manera fehaciente, así como la comprensión y aceptación de las condiciones de acceso.
- Se debe mantener actualizado el registro de todas las personas con derechos de acceso al servicio, revisándolo de forma periódica para localizar y eliminar identificadores de usuarios redundantes (duplicados) o sobrantes (no utilizados).
- Se debe eliminar de forma inmediata las autorizaciones de acceso a los usuarios que dejen la Organización o cambien su función dentro de ella y comprobar que los identificadores eliminados no sean reasignados a otros usuarios.
- No se debe permitir la utilización de claves compartidas o multiusuario.

13.2 Se debe asociar el control de acceso con los requisitos de autenticidad, confidencialidad, integridad y disponibilidad exigidos por el recurso al cual se intenta acceder.

13.3 Se debe limitar el acceso a los recursos según la función o la necesidad de conocer.

- Se debe establecer un proceso de autorización que registre los privilegios asignados a los usuarios; hasta que no haya concluido completamente, no otorgar privilegios especiales.
- Se deben identificar los privilegios asociados a cada subsistema (el sistema operativo, el gestor de base de datos, la aplicación, etc.) y a cada categoría de usuarios que los necesiten.
- Se deben asignar privilegios a individuos (no a colectivos) considerando cada caso como un acceso eventual temporal y partiendo del principio de 'necesidad de uso' (que minimice el acceso para el estricto desempeño de sus funciones y sólo cuando es imprescindible).
- Se debe promover el desarrollo y uso de herramientas (procedimientos automáticos o rutinas) que permitan la asignación temporal de privilegios.

13.4 Se deben revisar periódicamente y mediante procedimiento formal los derechos de acceso de los usuarios

- Se debe revisar la capacidad de acceso de los usuarios (por ejemplo, cada seis meses).
- Se deben someter a revisión más frecuente los accesos privilegiados (por ejemplo, cada tres meses).
- Se debe comprobar regularmente las asignaciones de accesos privilegiados para asegurarse de que éstos no han dado lugar a accesos no autorizados.

13.5 Se debe formar a los usuarios en relación con el control de acceso a los recursos protegidos.

- Los usuarios deben cumplir con las recomendaciones relativas a elementos de identificación y autenticación (contraseñas, certificados, tarjetas, etc.) y a los equipos no atendidos (desconexión de sesiones, protección si procede con bloqueador de teclado o llave, etc.).

13.6 Se deben adoptar medidas en relación con el trabajo desde fuera de las instalaciones de la organización.

13.7 Se deben adoptar medidas adicionales específicas para los equipos portátiles.

- Se deben instalar controles de acceso que actúen con carácter previo a la carga del sistema operativo.
- Se deben instalar mecanismos que cifren la información de los soportes de almacenamiento.

13.8 Se deben adoptar medidas adicionales específicas para el control de acceso de terceras partes

- Se debe elaborar un documento que contenga las normas de seguridad en vigor para el acceso de terceras partes.
- Se deben establecer procedimientos de protección de los activos; medidas de protección física; medidas contra la introducción y propagación de virus o de otro código dañino.
- Se deben establecer procedimientos de autorización de acceso a cada recurso o activo.
- Se debe fijar el método de acceso permitido (control del identificador y de contraseñas de usuario o mediante certificados digitales).
- Se debe mantener permanentemente actualizada la lista de usuarios autorizados y de permisos de acceso a recursos o activos específicos.

- Horas y fechas de disponibilidad del servicio (características necesarias del plan de contingencias).
- Responsabilidades de cada parte: derecho de auditoría para cumplimentar las responsabilidades contractuales; derecho de la organización anfitriona para controlar (y suspender en su caso) la actividad de uno o varios usuarios; acuerdo para la investigación e informes de incidentes de seguridad.
- Responsabilidades derivadas de la normativa (protección de datos de carácter personal, entre otros).
- Restricciones contra la copia y la revelación no autorizada.
- Medidas para asegurar la devolución de documentación y activos de información al finalizar el contrato.
- Mecanismos para asegurar que las medidas de seguridad son conocidas, respetadas y aplicadas.
- Requisitos de formación de los terceros en los métodos y procedimientos de seguridad compatibles con los de la organización.

RECOMENDACIONES:

- Interrumpir automáticamente la sesión después de un periodo de tiempo en el que el usuario no ha realizado ninguna acción. Este periodo de tiempo dependerá de las características de la propia aplicación y del perfil del usuario que accede a la información.
- Limitar el tiempo máximo de conexión para aplicaciones que se considere conveniente, así como la franja horaria de acceso.
- Mantener un registro de eventos relativos al control de acceso.
- Controlar el acceso a los programas de utilidades.
- Bloquear las cuentas que no sean utilizadas durante un período de tiempo fijado.
- Utilizar preferentemente sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido rigurosamente evaluados conforme a normas europeas o internacionales, como ISO/IEC 15408, y certificados por entidades independientes y de reconocida solvencia, como las recogidas en los acuerdos o arreglos internacionales de reconocimiento mutuo de los certificados de la seguridad de la tecnología de la información.

AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT); Guía de aproximación a la seguridad de los sistemas de información, capítulo 5; Guía de procedimientos; http://www.map.es/csi/pg5m20.htm
- ISO/IEC IS 17799 – Tecnologías de la información - Código de buenas prácticas para la gestión de la seguridad de la información *(Information technology – Code of practice for information security managment)*; capítulo 9.
- INFORMATION TECHNOLOGY *Baseline Protection Manual* http://www.bsi.bund.de/gshb/english/etc/inhalt.htm

- *Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook;* capítulo 17; http://csrc.nist.gov/publications/nistpubs/800-12/
- ISO/IEC TR 13335 – Tecnologías de la información (TI) - Guía para la gestión de la seguridad de TI; Parte 4; capítulo 10.4.
- Páginas del Consejo Superior de Informática y para el impulso de la Administración Electrónica sobre evaluación y certificación: (http://www.map.es/csi/pg3410 .htm)
- Resolución de 29 de noviembre de 1996, por la que se dictan instrucciones relativas a los accesos a las bases de datos de la Agencia Estatal de Administración Tributaria. (BOE 20-12-96) .

14 Acceso a través de redes

CONSIDERACIONES:

Se entiende por acceso a través de redes cualquier tipo de comunicación, con los sistemas informáticos o de comunicaciones de una organización, realizada mediante enlaces de telecomunicaciones.

El enfoque de la seguridad en relación con el acceso a través de redes debe contemplar cuestiones como las siguientes:

- ¿En qué medida puede un intruso acceder a los recursos del sistema o de la aplicación desde la red?
- ¿En qué medida estas intrusiones pueden afectar a los datos y a los tratamientos?
- ¿Los datos son fáciles de ser modificados o leídos cuando son transmitidos?.

CONCEPTOS:

Se entiende por cortafuegos el conjunto de dispositivos que protegen a la red de una organización frente a Internet u otras redes externas a dicha organización.

Se entiende por filtros de paquetes un tipo de dispositivo que permite o deniega el paso de paquetes de una red a otra en función de su origen, destino, contenido, etc.

Se entiende por apoderados o "proxies" aquellos dispositivos que permiten realizar las comunicaciones indirectamente a través de ellos, sirviendo de intermediarios. De esta forma pueden aplicar filtros a las aplicaciones o protocolos que soportan, y dan mayor seguridad a la red interna, al no exponerla directamente a las comunicaciones con el exterior.

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- La existencia de medidas de seguridad tendentes a evitar la interceptación y alteración de las comunicaciones, así como los accesos no autorizados. (RD 263/1996, art. 7.1)

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

Datos de carácter personal a los que se han de aplicar medidas de seguridad de nivel básico y medio:

- Autorizar la ejecución de datos de carácter personal fuera de los locales de la ubicación del fichero por parte del responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado. (RD 994/1999, art. 6)

Datos de carácter personal a los que se han de aplicar medidas de seguridad de nivel alto:

- Realizar el cifrado de los datos o utilizar cualquier otro mecanismo que garantice que la información no es inteligible, cuando los datos de carácter personal, se transmiten a través de redes de telecomunicaciones. (RD 994/1999, art. 26).

CRITERIOS:

14.1 Se debe establecer un proceso de gestión de las redes para garantizar la seguridad de la información transmitida y el acceso a la información remota. La responsabilidad de la gestión y explotación de la red debe ser explícita.

- Se debe segregar redes cuando existan aplicaciones con requisitos de seguridad diferentes y controlar el acceso a redes internas y externas.
- Cuando la aplicación o aplicaciones lo requieran, se deben ubicar en una subred aislada con barreras.

14.2 Se deben proteger los sistemas o servidores de la aplicación mediante cortafuegos que restrinjan los accesos a los estrictamente necesarios.

- Los dispositivos del cortafuegos han de permitir la autenticación de la conexión, control de acceso, ocultación de la estructura interna de la red (direcciones), inspección del tráfico, y registro de eventos.
- Incluirán mecanismos de detección de intrusión, así como de análisis de vulnerabilidades.
- Incluirán el empleo de intermediarios o apoderados de aplicaciones o protocolos, en la medida de lo posible.
- Configurar de forma adecuada los dispositivos del cortafuegos. En la configuración tener en cuenta que puedan dejar pasar protocolos seguros, como, por ejemplo, SSL v3. No se ubicarán los servicios del cortafuegos en las mismas máquinas donde residan los datos o aplicaciones.

14.3 Se debe cifrar la información transmitida a través de redes, para evitar su modificación y divulgación no autorizadas.

- Implantar mecanismos que permitan conexiones seguras: autenticación mutua de los dos extremos, control de acceso, protección de la información intercambiada (cifrado) y registro de eventos.

14.4 Se debe autentificar el acceso del usuario a los distintos recursos de la red.

14.5 Se debe definir en cada sistema y aplicación los usuarios que pueden acceder a través de conexiones externas.

- Cuando resulte imprescindible utilizar módems se deben establecer los mecanismos que garanticen protección equivalente a los proporcionados por un cortafuegos. En otro caso el módem deberá permanecer desconectado, conectándose bajo petición autentificada, y vigilando el acceso.

– Controlar el acceso a puertos de diagnóstico remotos.

14.6 El acceso a los sistemas de forma remota se debe realizar, siempre que sea técnicamente factible, mediante redes privadas virtuales.

RECOMENDACIONES:

- Definir sistemas de control de ruta, para requisitos de confidencialidad muy exigentes.
- Utilizar preferentemente sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido rigurosamente evaluados conforme a normas europeas o internacionales, como ISO/IEC 15408, y certificados por entidades independientes y de reconocida solvencia, como las recogidas en los acuerdos o arreglos internacionales de reconocimiento mutuo de los certificados de la seguridad de la tecnología de la información.

AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT); Guía de aproximación a la seguridad de los sistemas de información; capítulos 9.4 y 9.5; http://www.map.es/csi/pg5m20.htm
- ISO/IEC IS 17799 – Tecnologías de la información – Código de buenas prácticas para la gestión de la seguridad de la información *(Information technology – Code of practice for information security managment)*; capítulo 9.4.
- Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook; capítulo 5.
- *INFORMATION TECHNOLOGY Baseline Protection Manual*; capítulo 1; http://www.bsi.bund.de/gshb/english/etc/inhalt.htm
- ISO/IEC TR 13335 – Tecnologías de la información (TI) - Guía para la gestión de la seguridad de TI; Parte 1; capítulo 7.2.
- Páginas del Consejo Superior de Informática y para el impulso de la Administración Electrónica sobre evaluación y certificación: (http://www.map.es/csi/pg3410 .htm)
- http://csrc.nist.gov/cc/pp/pplist.htm#FIREWALL
- ITU-T **M.3400**: Funciones de gestión TMN.

EJEMPLO:

La gestión de redes significa la puesta en marcha de un conjunto de procesos y la implantación de una serie de herramientas. Los componentes más importantes de una gestión de red adecuada son:

- **Gestión de fallos:**.detección, informe, diagnóstico y corrección de problemas.
- **Gestión de la configuración:** control de la configuración de los elementos hardware y software, inventarios, licencias, configuración de los servicios, etc.
- **Gestión de la seguridad:** medidas para asegurar la autenticidad, confidencialidad, integridad y disponibilidad.
- **Gestión del rendimiento:** control de la ocupación de los enlaces, y de los recursos de los equipos empleados.
- **Gestión de la contabilidad**: control del coste de los servicios.

Es muy interesante instalar herramientas software de gestión de redes que faciliten la ejecución de los procesos mencionados anteriormente.

En relación con las barreras basadas en el concepto de cortafuegos se pueden distinguir básicamente dos tipos de estrategias:

- Filtrado de Paquetes. En función de la dirección IP origen, destino, puertos y tipos de servicios. Protegen el sistema del tráfico no autorizado proveniente del exterior.
- Filtrado de Aplicaciones. Soportado habitualmente por paquetes denominados *apoderados ("Proxies")*, que funcionan como intermediarios a nivel de aplicación. Todas las peticiones a sistemas externos se realizan a través del apoderado ("*proxy*"). De la misma manera las respuestas recibidas de sistemas externos son devueltas al apoderado ("*proxy*") para su entrega al emisor original. La utilización de apoderados ("proxies") permite la no-facilitación de información sobre recursos internos de cara al exterior y por tanto limita la posible vulnerabilidad de éstos.

15 Firma electrónica

CONSIDERACIONES:

- El empleo de sistemas basados en criptografía de clave pública ha demostrado ser una de las mejores alternativas para asegurar la autenticidad, integridad y confidencialidad de los sistemas. Su uso cada vez es más extendido en las diversas áreas de las tecnologías de la información y las comunicaciones.
- Las normas técnicas aplicables a los productos de firma electrónica y a los dispositivos de creación de la firma estarán a lo que disponga la legislación en la materia. Los criterios y recomendaciones de este capítulo se han de entender en ausencia de la publicación de dichas normas.
- La aplicación de los criterios o la toma en consideración de las recomendaciones del presente capítulo persiguen garantizar la interoperabilidad técnica en las comunicaciones de la Administración y de ésta con los ciudadanos, lo que resulta imprescindible para que puedan funcionar con éxito los mecanismos de verificación de la firma electrónica, sin perjuicio de que hayan de ser conformes con la legislación sobre firma electrónica.

CONCEPTOS:

Firma electrónica: los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación. (Directiva 1999/93/CE)

Firma electrónica avanzada: la firma electrónica que cumple los requisitos siguientes: a) estar vinculada al firmante de manera única; b) permitir la identificación del firmante; c) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control; d) estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable. (Directiva 1999/93/CE)

Certificado: documento electrónico, firmado electrónicamente por el proveedor de servicios de certificación (para hacerlo infalsificable), que proporciona confirmación independiente de la vinculación entre una clave pública y una persona y confirma la identidad de ésta.

Por ejemplo, el certificado de usuario Clase 2CA, emitido por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (Véase http://www.cert.fnmt.es/clase2/main.htm).

Certificado reconocido: los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en la Ley de Firma Electrónica, en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

Proveedor de servicios de certificación: la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica. (Directiva 1999/93/CE).

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Se adoptarán las medidas de organización necesarias que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información. (RD 263/1996, art. 4.2)

En relación con la protección de datos de carácter personal:

- Se cifrarán los datos de carácter personal a los que deban aplicarse medidas de nivel alto en su transmisión a través de redes de telecomunicaciones. (RD 994/1999, art. 26)

En relación con la firma electrónica:

- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999.
- Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica.
- Real Decreto 1317/2001, de 30 de noviembre, por el que se desarrolla el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas fiscales, administrativas y del orden social, en materia de prestación de servicios de seguridad, por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, en las comunicaciones a través de medios electrónicos, informáticos y telemáticos con las Administraciones Públicas.

CRITERIOS:

15.1 La firma electrónica en las comunicaciones administrativas será al menos firma electrónica avanzada, con certificado reconocido, cuyos requisitos mínimos son:

- Un par de claves complementarias, una pública y otra privada, generadas con algoritmos de cifrado asimétrico RSA o equivalente, con una longitud mínima de clave de 1024 bits o equivalente.
- Una función resumen o hash, preferiblemente SHA-1 (longitud 160 bits) o MD5 (128 bits) o equivalente.
- Los algoritmos de firma, generación de claves, métodos de relleno y funciones resumen deberán garantizar la seguridad criptológica.
- El correspondiente certificado de firma electrónica cumplirá las especificaciones UIT X.509 v3, o versiones posteriores.

15.2 La creación de la firma debe contar con mecanismos de protección que únicamente conozca o estén en posesión del firmante, por ejemplo mediante una contraseña.

15.3 Se deben emplear listas de revocación del tipo CRL V2.

15.4 Las tarjetas criptográficas y los lectores de tarjetas se ajustarán a los siguientes estándares:

- PC/SC de interoperabilidad de tarjetas y dispositivos lectores de tarjetas con sistemas operativos.
- ISO 7816 en los apartados 1,2,3 y 4 referentes a estructura física y eléctrica de las tarjetas, mensajes, estructura de ficheros y de órdenes.

15.5 Los servicios de sellado de tiempo proporcionados por la autoridad de certificación cumplirán los estándares definidos para este tipo de servicios [RFC3161].

15.6 Los protocolos de acceso a las listas de revocación serán del tipo HTTP u OCSP

15.7 Los módulos criptográficos habrán de ser compatibles con la norma FIPS 140-2.

RECOMENDACIONES:

- La firma electrónica avanzada basada en certificados reconocidos o los dispositivos seguros de creación de la firma electrónica se utilizarán cuando el correspondiente análisis y gestión de los riesgos así lo aconseje.
- Utilizar preferentemente sistemas productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido rigurosamente evaluados conforme a normas europeas o internacionales, como ISO/IEC 15408, y certificados por entidades independientes y de reconocida solvencia, como las recogidas en los acuerdos o arreglos internacionales de reconocimiento mutuo de los certificados de la seguridad de la tecnología de la información

NORMAS APLICABLES:

- RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- RFC 2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
- ITU-T X.509: Public key and attribute certificate frameworks.
- RFC 3039: Internet X.509 Public Key Infrastructure Qualified Certificates Profile.
- ETSI TS 101 862: Qualified certificate profile.
- NIST FIPS 140-2. Security Requirements For Cryptographic Modules.
- RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
- RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- PC/SC. Personal Computer/Smart Card.
- ISO 7816: Identification cards -- Integrated circuit(s) cards with contacts.

AMPLIACIÓN TÉCNICA:

- *IST Programme; Diffuse Standards and Specifications List - Information Security Standards* http://www.diffuse.org/secure.html#help
- Revista independiente sobre criptografía, seguridad y privacidad en Internet http://www.kriptopolis.com

- Páginas del Consejo Superior de Informática y para el impulso de la Administración Electrónica sobre evaluación y certificación: (http://www.map.es/csi/pg3410 .htm)
- Comunicación de la Comisión al Consejo, al Parlamento Europeo al Comité Económico y Social y al Comité de las Regiones, Seguridad de las redes y de la información: propuesta para un enfoque político europeo (6 de junio de 2001) http://www.map.es/csi/pdf/com2001_0298es01.pdf

16 Protección de soportes de información y copias de respaldo

CONCEPTOS:

La protección de los soportes de información (discos duros, disquetes, cd-rom, cintas, ordenadores portátiles, etc.) debe incluir un conjunto equilibrado de medidas proporcionado a la naturaleza de los datos y documentos que contengan.

En la preparación de los procedimientos de protección de los soportes de información ha de tenerse en cuenta que los ordenadores personales, incluyendo los portátiles, agendas electrónicas, etc., con discos fijos u otros dispositivos de almacenamiento no volátiles, operando de forma aislada o conectados en red, deben ser considerados como dispositivos de almacenamiento de información en el mismo sentido que otros soportes electrónicos de almacenamiento de información extraíbles.

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Los documentos que contengan actos administrativos que afecten a derechos o intereses de los particulares podrán conservarse en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. (RD 263/1996, art. 8)
- Deberán existir medidas de seguridad que garanticen la integridad, autenticidad, calidad, protección y conservación de los documentos almacenados. (RD 263/1996, art. 8)

En relación con la protección de datos de carácter personal:

Datos de carácter personal a los que se han de aplicar medidas de seguridad de nivel básico:

- Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad. (RD 994/1999, art. 13.1)
- La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del fichero. (RD 994/1999, art. 13.2)
- El responsable del fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de datos. (RD 994/1999, art. 14.1)

- Establecer procedimientos para la realización de copias de respaldo y para la recuperación de datos que garanticen su reconstrucción en el estado en que se encontraban al tiempo de producirse la perdida o destrucción. (RD 994/1999, art. 14.2)
- Realizar copias de respaldo, al menos semanalmente, salvo que en dicho periodo no se hubiera producido ninguna actualización de los datos. (RD 994/1999, art. 14.3)

Datos de carácter personal a los que se han de aplicar medidas de seguridad de nivel medio:

- Disponer de un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada. (RD 994/1999, art. 20.1)
- Disponer de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada. (RD 994/1999, art. 20.2)
- Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario. (RD 994/1999, art. 20.3)
- Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos. (RD 994/1999, art. 20.4)

Datos de carácter personal a los que se han de aplicar medidas de seguridad de nivel alto:

- La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte. (RD 994/1999, art. 23)
- Conservar una copia de respaldo y los procedimientos de recuperación de los datos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas exigidas en este reglamento. (RD 994/1999, art. 25) **.**

CRITERIOS:

16.1 Se debe aplicar lo previsto en el documento 'Criterios de Conservación' en los capítulos de 'Seguridad de la información' y 'Protección frente al deterioro físico' (Desarrollar y aplicar procedimientos de seguridad que contemplen la autenticidad, confidencialidad, integridad y disponibilidad, el tratamiento de datos de carácter personal, la gestión de soportes removibles, la eliminación y destrucción de soportes y la documentación del sistema de conservación.).

16.2 Se deben establecer procedimientos de realización, recuperación y pruebas de las copias de respaldo que contemplen copias de los programas, aplicaciones, documentación, bases de datos, sistemas operativos, logs, etc.; debe definirse la periodicidad con que se realizan las copias (diaria, semanal, mensual), número de copias que se realizan y versiones distintas que se conservan. Los procedimientos de realización de copias serán automáticos y periódicos.

16.3 Se debe elegir un lugar de almacenamiento adecuado para los soportes de información. Se debe tener en cuenta lo previsto en el capítulo 'Seguridad física'.

16.4 Para ficheros a los que haya que aplicar medidas de nivel alto se debe recurrir a dos copias distintas una de las cuales debe guardarse en una ubicación diferente de donde se encuentren los equipos informáticos que las tratan.

16.5 Se debe mantener un registro de entrada y salida de los soportes de información. Permitirá conocer: el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada. Cabe recoger asimismo el número de serie del soporte y marca de clasificación.

16.6 Los soportes de información enviados o distribuidos al exterior que contengan datos de nivel alto deberán ser cifrados.

16.7 Verificar la definición y correcta aplicación de las medidas de protección de los soportes de información.

16.8 Se debe incluir entre las prácticas de protección de los soportes de información medidas básicas como las siguientes, dentro y fuera del horario normal de trabajo, para evitar su pérdida o destrucción:

- Los documentos, disquetes y otros soportes de información deben guardarse en armarios cuando no se usen y, especialmente, fuera del horario normal de trabajo.
- La información crítica o sensible debe encerrarse bajo llave cuando no se requiera especialmente o la oficina esté vacía.
- Los ordenadores personales y los terminales deben estar protegidos por llave, contraseñas u otras salvaguardas cuando no se usen.

16.9 Se debe verificar que los usuarios cumplen las recomendaciones relativas a que los equipos no atendidos queden convenientemente protegidos.

16.10 Realizar periódicamente pruebas para verificar que la recuperación de la información a partir de las copias de respaldo funciona correctamente. Estas pruebas se pueden basar en inspecciones periódicas de forma aleatoria o exhaustiva para comprobar su presencia física y contenido.

RECOMENDACIONES:

- Proteger la entrada y salida de correo, así como los puntos de fax desatendidos.
- Considerar que la denominación del nivel de seguridad aplicable (Véase capítulo 'Identificación y clasificación de activos a proteger') aparezca señalada de forma inequívoca en todos sus soportes:
  - Reflejar el nivel de seguridad aplicable en todas y cada una de las páginas de los impresos, incluyendo la carátula; opcionalmente el nivel de seguridad puede figurar en la cabecera o en el pie de página, siempre que resulte fácilmente legible.
  - Reflejar el nivel de seguridad aplicable en todas y cada una de las pantallas que aparezcan en los terminales o puestos del usuario, o estar permanentemente en la cabecera de la pantalla.
  - Etiquetar cada soporte electrónico transportable (cintas, cartuchos, disquetes, etc.) con el máximo nivel de seguridad de la información que contenga.

- Si la información (por ejemplo, datos de carácter personal a los que se han de aplicar medidas de nivel medio o alto) se envía al exterior o por correo externo a la organización, el sobre cerrado y marcado con el citado nivel de seguridad deberá introducirse en un contenedor NO marcado.

- Incluir en las copias de respaldo los ficheros de registros de eventos (trazas de *audit*, *logs*) y diario de incidencias.
- Emplear en las copias de respaldo formatos no propietarios que garanticen su accesibilidad en el tiempo.

NIVELES DE SEGURIDAD:

La naturaleza de los datos manejados determina las medidas de seguridad a aplicar. (Véase capítulo 'Identificación y clasificación de activos a proteger').

AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT); Guía de aproximación a la seguridad de los sistemas de información; capítulos 8.4, 8.5 y 8.6; http://www.map.es/csi/pg5m20.htm
- ISO/IEC IS 17799 Tecnologías de la información - Código de buenas prácticas para la gestión de la seguridad de la información *(Information technology – Code of practice for information security managment)*; capítulos 8.4.1.
- *INFORMATION TECHNOLOGY Baseline Protection Manual*; capítulo 3.4; http://www.bsi.bund.de/gshb/english/etc/inhalt.htm
- ISO/IEC TR 13335 – Tecnologías de la información (TI) - Guía para la gestión de la seguridad de TI; Parte 1; capítulo 7.2.

17 Desarrollo y explotación de sistemas

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Se adoptarán las medidas técnicas y de organización necesarias que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información. (RD 263/1996, art. 4.2).

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

- Garantizar los niveles de seguridad que les corresponda a los ficheros temporales con arreglo a los criterios establecidos. (RD 994/1999, art. 7.1)
- Borrar todo fichero temporal una vez haya dejado de ser necesario para los fines por los que fue creado. (RD 994/1999, art. 7.2)

- Identificar, inventariar y almacenar en lugar con acceso restringido cualquier soporte informático con información que contiene datos de carácter personal. (RD 994/1999, art. 13.1)
- Autorizar por parte del responsable, la salida fuera de los locales en los que esté ubicado el fichero, de cualquier soporte informático con información que contiene datos de carácter personal. (RD 994/1999, art. 13.2)
- Realizar pruebas anteriores a la implantación o modificación de aplicaciones con datos no reales. (RD 994/1999, art. 22).

CRITERIOS:

17.1 Se deben adoptar procedimientos de explotación adecuados para salvaguardar la disponibilidad, integridad y confidencialidad de la información.

17.2 Se deben definir procedimientos para el paso de aplicaciones a explotación, ya sean nuevas o actualizaciones de las existentes, que recojan los requisitos que estas deben cumplir y las pruebas a realizar antes de su aceptación.

17.3 Se deben asegurar por medio de la gestión de configuración y de cambios que las modificaciones en el sistema no reducen la efectividad de las salvaguardas ni la seguridad general del mismo, que se identifican nuevos requisitos de seguridad o impacto en la seguridad de los posibles cambios y que los mismos tienen reflejo en el plan de contingencias.

17.4 Se deben realizar mantenimientos preventivos, como la instalación de las actualizaciones de seguridad recomendadas por los fabricantes, o el aumento de capacidad para evitar saturaciones.

17.5 Se debe documentar en la política de seguridad los requisitos con relación a licencias de programas y la prohibición de uso e instalación de software no autorizado. Establecer controles periódicos que revisen el software instalado e implantar mecanismos de protección para evitar la instalación de software no autorizado.

17.6 Se debe formar a los usuarios en el uso adecuado de la aplicación y en los procedimientos de reacción ante incidentes.

17.7 Se debe aplicar el análisis y gestión de riesgos para determinar las necesidades de seguridad de la aplicación antes de su desarrollo e incorporar las funciones de salvaguarda antes de completarla (más barato y efectivo).

17.8 Se deben tener en cuenta los aspectos de seguridad de la aplicación en todas las fases de su ciclo de desarrollo, desde la planificación hasta la implantación y el mantenimiento e incorporando las funciones de salvaguarda antes de su puesta en explotación.

RECOMENDACIONES:

En relación con el desarrollo:

- Establecer criterios de aceptación para nuevos sistemas, así como en los desarrollos de nuevas versiones y funciones.
- Para la realización de las pruebas previas a la puesta en explotación (relativas a la seguridad, rendimientos, diseño, etc.) es conveniente la disposición de un entorno de pruebas independiente de los entornos de desarrollo y de explotación.

- En condiciones de determinados requisitos de seguridad cabe desarrollar un Perfil de Protección conforme con los Criterios Comunes de evaluación de la seguridad de las tecnologías de la información.

En relación con la explotación:

- Implantar y mantener actualizado el software de detección y protección ante código dañino y de detección de intrusiones.
- Formar a los usuarios en la utilización adecuada de la aplicación, del software antivirus y en la notificación de incidencias relacionadas con los ataques de este tipo y todo lo relativo a la gestión y responsabilidades relacionadas con el código dañino.

AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT); Guía de aproximación a la seguridad de los sistemas de información; capítulos 8 y 9; http://www.map.es/csi/pg5m20.htm
- ISO/IEC IS 17799 – Tecnologías de la información – Código de buenas prácticas para la gestión de la seguridad de la información *(Information technology – Code of practice for information security managment)*; capítulo 10.
- *Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook;* capítulo 14; http://csrc.nist.gov/publications/nistpubs/800-12/
- *INFORMATION TECHNOLOGY Baseline Protection Manual;* capítulo 3.6; http://www.bsi.bund.de/gshb/english/etc/inhalt.htm
- ISO/IEC TR 13335 – Tecnologías de la información (TI) – Guía para la gestión de la seguridad de TI; Parte 1; capítulo 7.2.
- ISO/IEC WD 15446, *Guide on the production of protection profiles and security targets* http://www.commoncriteria.org/protection_profiles/pp.html
- Http://csrc.nist.gov/cc/pp/pplist.htm.

18 Gestión y registro de incidencias

CONCEPTOS:

Se trata de una función esencial para el análisis de los problemas informáticos y en especial de los incidentes de seguridad.

Se entiende la 'informática forense' como aquella que se ocupa de investigar los incidentes o intrusiones, una vez que estos ya se han producido, para tratar de averiguar las causas, a los autores y los daños que han conllevado.

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Se adoptarán las medidas técnicas y de organización necesarias que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información. (RD 263/1996, art. 4.2)
- Las medidas de seguridad deberán garantizar la prevención de alteraciones o pérdidas de los datos e informaciones y la protección de los procesos informáticos frente a manipulaciones no autorizadas. (RD 263/1996, art. 4.3)

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

Datos de carácter personal a los que se han de aplicar las medidas denominadas de nivel básico:

- Notificar y gestionar las incidencias utilizando un registro en el que conste el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién lo comunica y los efectos que se hubieran derivado de la misma. (RD 994/1999, art. 10)

Datos de carácter personal a los que se han de aplicar las medidas denominadas de nivel medio y alto:

- Consignar además de los datos mencionados en el punto anterior, los procedimientos realizados para recuperar los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación. (RD 994/1999, art. 21.1)
- Autorizar por escrito del responsable del fichero para ejecutar los procedimientos para recuperar los datos. (RD 994/1999, art. 21.2)

CRITERIOS:

18.1 Se debe definir el procedimiento de gestión de incidencias, que establezca las formas de comunicación, el diagrama de estados por los que pasará hasta su conclusión, la clasificación según su gravedad, las condiciones para el escalado de la incidencia a los responsables de la organización, la forma de comunicación a proveedores externos, consulta del estado de las incidencias, etc.

18.2 Se debe formar y concienciar a los usuarios en relación con los procedimientos de comunicación, consulta y reacción ante incidencias. Se deben establecer canales para informar lo más rápidamente posible de las incidencias y el mal funcionamiento de los sistemas.

18.3 Se debe implantar un registro incidencias acorde al procedimiento y a los datos manejados con el tipo de incidencia, momento, persona que realiza la notificación, a quién lo notifica y los efectos de la misma. Esta información junto con otra relativa a la seguridad se debe conservar para aprender de estas experiencias, con objeto de minimizar los posibles daños y consecuencias, para investigaciones futuras y para el control de los accesos.

18.4 Si sospecha que el mal funcionamiento es debido a problemas de software (por ejemplo un virus), el usuario debe:

- Observar los síntomas y mensajes que aparezcan en pantalla.
- Dejar de usar el sistema (aislarlo si es posible, pero no apagarlo) e informar de inmediato a la unidad de soporte informático.
- Informar inmediatamente a su mando responsable por el canal determinado.
- La organización informará a los usuarios que ellos no deben, en ninguna circunstancia, intentar retirar el software sospechoso. Esto debe realizarse por un experto debidamente entrenado y con experiencia. Si el experto va a realizar las pruebas en la máquina del

usuario, ésta se desconectará de las redes de la organización antes de volver a arrancarla.

RECOMENDACIONES:

- Los actores implicados conocerán los procedimientos para realizar y remitir informes sobre los diferentes tipos de incidencias, las amenazas, vulnerabilidades o simplemente el mal funcionamiento de la aplicación o del sistema; a quién deben ir dirigidos, así como la respuesta con las acciones a ejecutar.
- Controlar y cuantificar los distintos tipos de incidentes, causa u origen e impacto causado.
- La organización debe pedir a los usuarios que observen e informen sobre toda aplicación o programa que parezca que no está funcionando bien (es decir de acuerdo con las especificaciones).
- Es conveniente el desarrollo de planes de informática forense, y la implantación de herramientas para su ejecución, que permitan aclarar incidencias ocurridas.

AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT); Guía de aproximación a la seguridad de los sistemas de información; capítulo 6.5; http://www.map.es/csi/pg5m20.htm
- ISO/IEC IS 17799 – Tecnologías de la información – Código de buenas prácticas para la gestión de la seguridad de la información *(Information technology – Code of practice for information security managment)*; capítulo 6.3.
- *Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook;* capítulo 12; http://csrc.nist.gov/publications/nistpubs/800-12/
- *INFORMATION TECHNOLOGY Baseline Protection Manual*; capítulo 1; http://www.bsi.bund.de/gshb/english/etc/inhalt.htm
- ISO/IEC TR 13335 Tecnologías de la información (TI) – Guía para la gestión de la seguridad de TI; Parte 1; capítulo 7.2.
- Páginas del Consejo Superior de Informática y para el impulso de la Administración Electrónica sobre evaluación y certificación: (http://www.map.es/csi/pg3410 .htm).

19 Plan de contingencias

CONSIDERACIONES:

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, debe preverse 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 e 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.

MARCO LEGAL:

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. (RD 263/1996, arts. 4.2, 4.3)

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. (LO 15/1999, art. 9.1).

CRITERIOS:

19.1 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.

19.2 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.

19.3 Se debe activar el plan de contingencias como reacción ante un incidente que afecte a la continuidad del servicio proporcionado por la aplicación.

RECOMENDACIONES:

- 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:
    - Sustitución de elementos,
    - servicio degradado,
    - servicio simplificado,
    - sin servicio,
    - 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.

AMPLIACIÓN TÉCNICA:

- ISO/IEC IS 17799 – Tecnologías de la información – Código de buenas prácticas para la gestión de la seguridad de la información *(Information technology – Code of practice for information security managment)*; capítulo 11.
- ISO/IEC TR 13335 – Tecnologías de la información (TI) - Guía para la gestión de la seguridad de TI; Parte 4; capítulo 8.1.6.
- *Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook;* capítulo 11; http://csrc.nist.gov/publications/nistpubs/800-12/
- *INFORMATION TECHNOLOGY Baseline Protection Manual*; capítulo 3.3; http://www.bsi.bund.de/gshb/english/etc/inhalt.htm

20 Auditoria y control de la seguridad

CONCEPTOS:

Definición de auditoria:

Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar el alcance al que se cumplen los procedimientos o requisitos contra los que se compara la evidencia. (ISO 9000: 2000).

MARCO LEGAL:

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. (RD 263/1996, arts. 4.2 y 4.3)

En relación con la protección de los datos de carácter personal a los que se han de aplicar las medidas de nivel medio y alto:

- Someter a una auditoria interna o externa a los sistemas de información e instalaciones de tratamiento de datos, esta auditoria verificará el cumplimiento del Reglamento del RD 994/1999, de 11 de Junio/1999 de medidas de seguridad, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años. (RD 994/1999, art. 17.1)
- Emitir un informe de auditoria que deberá dictaminar sobre la adecuación de las medidas y controles del mencionado 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, art. 17.2)

- Analizar los informes de auditoria por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos. (RD 994/1999, art. 17.3).

CRITERIOS:

20.1 La situación y actividades de seguridad se deben revisar de forma independiente (auditoria) y periódicamente para asegurar que las prácticas de la organización siguen estas normas y que además son efectivas.

20.2 En relación con la protección de datos de carácter personal a los que haya que aplicar las denominadas medidas de nivel medio o alto, se deben someter a auditoria los sistemas de información e instalaciones de tratamiento de datos al menos cada dos años.

20.3 La aplicación debe estar dotada de un registro de eventos o pista de auditoria que registre al menos el identificador de usuario, fecha, hora, y proceso mediante el que se ha realizado un alta, modificación o baja de cualquier información que substancie el ejercicio de una potestad, afecte a datos de carácter personal o pueda ser considerada como sensible.

20.4 Se deben proteger los ficheros de recogida de eventos así como las herramientas de auditoria y control, a fin de evitar su alteración o destrucción por medios no autorizados y para salvaguardar su integridad y su disponibilidad, especialmente los del registro telemático y el servicio de dirección electrónica única.

20.5 Se deben sincronizar los relojes de los distintos sistemas para facilitar un archivo fiable de eventos.

20.6 Se debe controlar periódicamente la utilización de los distintos componentes del sistema.

20.7 Se debe asegurar que la función de auditoria accede en su caso a la información relativa a las medidas de seguridad, pero no a los datos.

20.8 En las aplicaciones que se citan a continuación, el registro de eventos guardará al menos traza:

- En el servicio de dirección electrónica única, se guardará traza de la fecha y la hora del acceso del interesado al contenido de la notificación y traza de la fecha y hora de remisión del aviso de notificación al interesado.
- En el registro telemático se guardará traza de la fecha y hora de recepción en el registro de la solicitud, escrito o comunicación.

RECOMENDACIONES:

- Revisar periódicamente que los usuarios cumplen con los requisitos de seguridad que les son aplicables (Ej. Actualización de contraseñas, conservación de la información en el puesto de trabajo, etc.).
- Revisar periódicamente las medidas organizativas y técnicas de seguridad para mejorarlas y aumentar su eficacia.
- Realizar periódicamente los denominados análisis de vulnerabilidades, con ayuda de herramientas disponibles en el mercado, para detectar y poder corregir los posibles agujeros de seguridad en los sistemas.

AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT); Guía de aproximación a la seguridad de los sistemas de información; capítulo 9.7 (http://www.map.es/csi/pg5m20.htm)
- ISO/IEC IS 17799 – Tecnologías de la información – Código de buenas prácticas para la gestión de la seguridad de la información *(Information technology – Code of practice for information security managment)*; capítulo 12.3.
- *Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook;* capítulo 18. http://csrc.nist.gov/publications/nistpubs/800-12/
- ISO/IEC TR 13335 - Tecnologías de la información (TI) - Guía para la gestión de la seguridad de TI; Parte 4; capítulo 8.1.6.
- *INFORMATION TECHNOLOGY Baseline Protection Manual*; capítulo 3.3; http://www.bsi.bund.de/gshb/english/etc/inhalt.htm
- The Information Systems Audit and Control Association & Foundation; http://www.isaca.org