



CENTRO DE ESTUDIOS FINANCIEROS

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

www.cef.es

info@cef.es

Índice Tema 11

1. Seguridad lógica de un sistema de información.
2. Riesgos, amenazas y vulnerabilidades. Medidas de protección y aseguramiento.
3. Auditoría y control de seguridad.





CENTRO DE ESTUDIOS FINANCIEROS

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

www.cef.es

info@cef.es

TEMA 11

Seguridad lógica de un sistema de información. Riesgos, amenazas y vulnerabilidades. Medidas de protección y aseguramiento. Auditoría de seguridad lógica.

1. SEGURIDAD LÓGICA DE UN SISTEMA DE INFORMACIÓN.

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.
- Autorización de derechos de acceso a distintos recursos del sistema.
- Acceso a redes, sistemas, aplicaciones, datos.
- Control y auditoría de acceso.

Se entiende 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.



Definiciones de control de acceso:

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

Desde el punto de vista legal hay que tener en cuenta:

En relación con las aplicaciones para el ejercicio de potestades (Real Decreto 263/1996):

- Adoptar medidas técnicas y de organización necesarias que aseguren la autenticidad, confidencialidad, integridad y disponibilidad.
- Proteger códigos o sistemas de forma que sólo puedan ser utilizados por las personas autorizadas por razón de sus competencias o funciones.
- Implantar las medidas de seguridad tendentes a evitar la interceptación y alteración de las comunicaciones así como los accesos no autorizados.
- 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.

En relación con la protección de los datos de carácter personal (Ley Orgánica 15/1999 y Real Decreto 994/1999):

- Almacenar los datos de carácter personal de forma que permita el ejercicio del derecho de acceso.
- Prohibir la recogida (acceso) de datos por medios fraudulentos, desleales o ilícitos.
- 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.
- Garantizar el acceso a través de redes de comunicaciones con una seguridad equivalente al acceso en modo local.
- Permitir el acceso de los usuarios únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- 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.
- Identificar a los usuarios que tengan acceso autorizado.
- 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.

En medidas de nivel medio (Real Decreto 994/1999):

- 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.
- Limitar la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

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.
- En el caso que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
- 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.
- Conservar los datos registrados durante un período mínimo de dos años.
- Revisar por parte del responsable de seguridad competente de forma periódica la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

Los criterios para realizar estas tareas son:

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 incluidos en el apartado «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.
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.
 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.
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 deben comprobar regularmente las asignaciones de accesos privilegiados para asegurarse de que éstas no han dado lugar a accesos no autorizados.
 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.).
 6. Se deben adoptar medidas en relación con el trabajo desde fuera de las instalaciones de la organización.
 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.

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.

Es básico tener en cuenta las siguientes recomendaciones:

- Interrumpir automáticamente la sesión después de un período de tiempo en el que el usuario no ha realizado ninguna acción. Este período 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.

2. RIESGOS, AMENAZAS Y VULNERABILIDADES. MEDIDAS DE PROTECCIÓN Y ASEGURAMIENTO.

Acceso a través de redes.

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?

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 «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.

Desde el punto de vista legal hay que tener en cuenta:

- 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 (Real Decreto 263/1996).
- En relación con la protección de los datos de carácter personal.

Datos de carácter personal a los que se ha de aplicar medidas de seguridad de nivel básico y medio (Real Decreto 994/1999).

- 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.

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.

Se deben utilizar los siguientes criterios:

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 deben 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.
2. Se deben proteger los sistemas o servidores de la aplicación mediante cortafuegos que restrinjan los accesos a los estrictamente necesarios.
 - Los dispositivos 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 de aplicaciones o protocolos, en la medida de lo posible.
 - Configurar de forma adecuada los dispositivos cortafuegos. En la configuración hay que tener en cuenta que puedan dejar pasar protocolos seguros, como, por ejemplo, SSL v3. No se ubicarán los servicios cortafuegos en las mismas máquinas donde residan los datos o aplicaciones.
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.
4. Se debe autenticar el acceso del usuario a los distintos recursos de la red.

5. Se deben 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 cortafuegos. En otro caso el módem deberá permanecer desconectado, conectándose bajo petición autenticada, y vigilando el acceso.
- Controlar el acceso a puertos de diagnóstico remotos.

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

Es básico tener en cuenta las siguientes 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.

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.

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 «Proxies», que funcionan como intermediarios a nivel de aplicación. Todas las peticiones a sistemas externos se realizan a través del «proxy». De la misma manera las respuestas recibidas de sistemas externos son devueltas al «proxy» para su entrega al emisor original. La utilización de «proxies» permite la no-facilitación de información sobre recursos internos de cara al exterior y, por tanto, limita la posible vulnerabilidad de éstos.

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.

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).

Desde el punto de vista legal hay que tener en cuenta:

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 (Real Decreto 263/1996).

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 (Real Decreto 994/1999).

En relación con la firma electrónica:

- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999.

Los criterios para realizar estas tareas son:

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.
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.
3. Se deben emplear listas de revocación del tipo CRL V2.
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 referentes a estructura física y eléctrica de las tarjetas, mensajes, estructura de ficheros y de órdenes.
5. Los servicios de sellado de tiempo proporcionados por la autoridad de certificación cumplirán los estándares definidos para este tipo de servicios [RFC3161].
6. Los protocolos de acceso a las listas de revocación serán del tipo HTTP u OCSP.
7. Los módulos criptográficos habrán de ser compatibles con la norma FIPS 140-2.

Es básico tener en cuenta las siguientes 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.

Desarrollo y explotación de sistemas.

Desde el punto de vista legal hay que tener en cuenta:

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 (Real Decreto 263/1996).

En relación con la protección de los datos de carácter personal (Real Decreto 994/1999):

- Garantizar los niveles de seguridad que les corresponda a los ficheros temporales con arreglo a los criterios establecidos.
- Borrar todo fichero temporal una vez haya dejado de ser necesario para los fines por los que fue creado.
- Identificar, inventariar y almacenar en lugar con acceso restringido cualquier soporte informático con información que contenga datos de carácter personal.
- 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.
- Realizar pruebas anteriores a la implantación o modificación de aplicaciones con datos no reales.

Los criterios para realizar estas tareas son:

1. Se deben adoptar procedimientos de explotación adecuados para salvaguardar la disponibilidad, integridad y confidencialidad de la información.
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 éstas deben cumplir y las pruebas a realizar antes de su aceptación.
3. Se debe 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.

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.
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.
6. Se debe formar a los usuarios en el uso adecuado de la aplicación y en los procedimientos de reacción ante incidentes.
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.
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 incorporar las funciones de salvaguarda antes de su puesta en explotación.

Es básico tener en cuenta las siguientes 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.

Gestión y registro de incidencias.

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 éstos ya se han producido, para tratar de averiguar las causas, los autores y los daños que han conllevado.

Desde el punto de vista legal hay que tener en cuenta:

En relación con las aplicaciones para el ejercicio de potestades (Real Decreto 263/1996):

- Se adoptarán las medidas técnicas y de organización necesarias que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información.
- 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.
- En relación con la protección de los datos de carácter personal (Real Decreto 994/1999):

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.

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.
- Autorizar por escrito del responsable del fichero para ejecutar los procedimientos para recuperar los datos.

Los criterios para realizar estas tareas son:

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.
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.
3. Se debe implantar un registro de 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.
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.

Es básico tener en cuenta las siguientes 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.

Medidas de protección en Autenticación, Confidencialidad, Integridad y Disponibilidad:

En este apartado 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.

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).

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.

Definiciones de autenticación:

- Procedimiento de comprobación de la identidad de un usuario (Real Decreto 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 (ISO7498-2).
- 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.

Desde el punto de vista legal hay que tener en cuenta:

En relación con las aplicaciones para el ejercicio de potestades (Real Decreto 263/1996):

- 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.
- 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.

En relación con la protección de datos de carácter personal (Real Decreto 994/1999):

Datos de carácter personal a los que se ha 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.
- Definir un procedimiento de asignación, distribución y almacenamiento de contraseñas.
- Actualizar contraseñas y almacenarlas de forma ininteligible.

Datos de carácter personal a los que se ha 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.
- Limitar el número de intentos de conexión fallidos.

Los criterios para realizar estas tareas son:

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.
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.
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.
4. El sistema debe exigir que cada usuario se identifique y autentique 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.).
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.
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, tres) 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.

Es básico tener en cuenta las siguientes recomendaciones:

La identificación y la autenticación basada en certificados sobre tarjeta inteligente criptográfica son recomendables:

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, tres) 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.

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.

Confidencialidad.

En este apartado 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.

La confidencialidad de los datos exige medidas específicas también en su eliminación o de los soportes en los que hubieran estado almacenados. 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.

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.
- 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.

Desde el punto de vista legal hay que tener en cuenta:

En relación con las aplicaciones para el ejercicio de potestades, el Real Decreto 263/1996.

- Adoptar las medidas técnicas y de organización necesarias que aseguren la confidencialidad de la información.
- 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.

En relación con la protección de los datos de carácter personal (Ley Orgánica 15/1999 y Real Decreto 994/1999):

- 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.
- 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 aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.
- 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.

Los criterios para realizar estas tareas son:

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.
2. Los algoritmos deben permitir una longitud mínima de claves de 128 bits y se utilizarán preferentemente 3DES, IDEA, RC4, RC5, AES, o equivalentes.
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.
4. En correo electrónico seguro se debe utilizar el estándar S/MIME v2 o superior.
5. En sesiones de administración remota se debe utilizar SSH.
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.
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.
8. Para salvaguarda de la confidencialidad se debe tener en cuenta también lo previsto en los apartados «Seguridad física», «Autenticación», «Control de acceso», «Acceso a través de redes» y «Protección de los soportes de información y copias de respaldo».
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, ha de ser independiente del utilizado 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.

Es básico tener en cuenta las siguientes 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.

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.

Integridad:

En este apartado 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.

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 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 de 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.

Desde el punto de vista legal hay que tener en cuenta:

En relación con las aplicaciones para el ejercicio de potestades el Real Decreto 263/1996.

Adoptar las medidas técnicas y de organización necesarias que aseguren integridad de la información.

- 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.
- 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.

En relación con la protección de los datos de carácter personal (Ley Orgánica 15/1999 y Real Decreto 994/1999):

- 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.
- Cumplir las condiciones con respecto a su integridad para registrar los datos de carácter personal.
- Identificar al usuario con acceso autorizado.
- Crear un mecanismo basado en contraseñas que garantice integridad de los datos de carácter personal.
- Cambiar las contraseñas para proteger integridad de los datos de carácter personal.

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.

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.

- En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
- 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.
- El período mínimo de conservación de los datos registrados será de dos años.
- 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.
- 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.

Los criterios para realizar estas tareas son:

1. Se deben implantar procedimientos de explotación de la aplicación y de los sistemas adecuados a la protección de la integridad.
2. Se deben implantar procedimientos de copias de respaldo de ficheros y bases de datos, y de protección y conservación de soportes de información.
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.
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.
5. Se deben proteger los archivos de información mediante el atributo de sólo lectura.
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.
7. Se debe realizar un análisis periódico de los accesos y de los recursos utilizados.
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.

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 deberán 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.

Es básico tener en cuenta las siguientes 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 apartados «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.

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.

Disponibilidad:

En este apartado 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.

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.

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 período 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.

Desde el punto de vista legal hay que tener en cuenta:

En relación con las aplicaciones para el ejercicio de potestades (Real Decreto 263/1996):

- Adoptar las medidas técnicas y de organización necesarias que aseguren disponibilidad de la información.

En relación con la disponibilidad de los datos de carácter personal la Ley Orgánica 15/1999:

- Registro de datos de carácter personal en ficheros que no reúnan las condiciones de seguridad.
- 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.
- 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.
- 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.
- Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.
- 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.

Los criterios para realizar estas tareas son:

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.
 - 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.
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.
 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.
 4. Los equipos deben mantenerse de acuerdo con las especificaciones de los suministradores respectivos.
 5. Se deben adoptar las medidas apropiadas de seguridad física en el entorno donde se encuentren los equipos que den soporte a la aplicación.
 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.
 7. Se deben proteger los sistemas y las aplicaciones contra los ataques de denegación de servicio.
 8. Se deberá preparar y mantener operativo un plan de contingencias.

Es básico tener en cuenta las siguientes 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 apartados «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.

3. AUDITORÍA Y CONTROL DE LA SEGURIDAD.

Definición de auditoría: 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).

Es básico tener en cuenta las siguientes recomendaciones:

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 de los procesos informáticos.

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 auditoría interna o externa a los sistemas de información e instalaciones de tratamiento de datos; esta auditoría verificará el cumplimiento del Reglamento del Real Decreto 994/1999.
- Emitir un informe de auditoría 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.
- Analizar los informes de auditoría 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.

Los criterios para realizar estas tareas son:

1. La situación y actividades de seguridad se deben revisar de forma independiente (auditoría) y periódicamente para asegurar que las prácticas de la organización siguen estas normas y que además son efectivas.
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 auditoría los sistemas de información e instalaciones de tratamiento de datos al menos cada dos años.
3. La aplicación debe estar dotada de un registro de eventos o pista de auditoría 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.
4. Se deben proteger los ficheros de recogida de eventos así como las herramientas de auditoría 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.
5. Se deben sincronizar los relojes de los distintos sistemas para facilitar un archivo fiable de eventos.
6. Se debe controlar periódicamente la utilización de los distintos componentes del sistema.
7. Se debe asegurar que la función de auditoría accede en su caso a la información relativa a las medidas de seguridad, pero no a los datos.
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.

Es básico tener en cuenta las siguientes recomendaciones:

- Revisar periódicamente que los usuarios cumplen con los requisitos de seguridad que les son aplicables (por ejemplo, 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.

