MINISTERIO
DE ADMINISTRACIONES
PÚBLICAS

SECRETARIA GENERAL
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,

NORMALIZACIÓN Y CONSERVACIÓN

24 de junio de 2004

Madrid, junio de 2004

NIPO 326-04-044-9

Catálogo general de publicaciones oficiales

http://publicaciones.administracion.es/

Índice

I) ACUERDO DEL 236º PLENO DE LA COMISIÓN INTERMINISTERIAL DE ADQUISICIÓN DE BIENES Y SERVICIOS INFORMÁTICOS

La Comisión Interministerial de Adquisición de Bienes y Servicios Informáticos, en el 236º Pleno, celebrado el 24 de junio de 2004, ACORDÓ:

Aprobación de la actualización de los "Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades" del Consejo Superior de Informática y para el impulso de la Administración Electrónica (CSI).

Publicación de los "Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades" del CSI en el sitio web del CSI, principalmente

II) RESOLUCIÓN DE 26 DE MAYO DE 2003, DE LA SECRETARÍA DE ESTADO PARA LA ADMINISTRACIÓN PÚBLICA

Resolución de 26 de mayo de 2003, de la Secretaría de Estado para la Administración Pública por la que se dispone la publicación del Acuerdo del Pleno de la Comisión Interministerial de Adquisición de Bienes y Servicios Informáticos (CIABSI) de 18 de diciembre de 2002 por el que se aprueban los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas por la Administración General del Estado en el ejercicio de sus potestades

---

El Pleno de la Comisión Interministerial de Adquisición de Bienes y Servicios Informáticos (CIABSI), en su reunión del día 18 de diciembre de 2002, adoptó el Acuerdo que figura a continuación de la presente Resolución, por el que se aprueban los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas por la Administración General del Estado en el ejercicio de sus potestades.

Para general conocimiento, se dispone la publicación de dicho Acuerdo como anexo a la presente Resolución.

Madrid, 26 de junio de 2003

El Secretario de Estado para la Administración Pública

JULIO GÓMEZ POMAR RODRÍGUEZ

ANEXO

Acuerdo del Pleno de la Comisión Interministerial de Adquisición de Bienes y Servicios Informáticos (CIABSI) de 18 de diciembre de 2002 por el que se aprueban los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas por la Administración General del Estado en el ejercicio de sus potestades.

El día 18 de diciembre de 2001, la Comisión Interministerial de Adquisición de Bienes y Servicios Informáticos (CIABSI), acordó la adopción de los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas por la Administración General del Estado en el ejercicio de sus potestades. En dicho acuerdo se estableció que durante un año tales criterios tendrían carácter de recomendación, salvo que una norma del Consejo Superior de Informática y para el impulso de la Administración Electrónica dispusiera otra cosa.

En el año transcurrido, los Criterios de seguridad, normalización y conservación se han difundido de manera general en el ámbito de la Administración General del Estado. Han probado su utilidad, facilitando a los órganos y Organismos Públicos un conjunto común, riguroso y fundado de criterios, normas y protocolos en la utilización de los medios electrónicos, informáticos y telemáticos para el ejercicio de sus potestades, de acuerdo con lo dispuesto en 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.

Los Criterios de seguridad, normalización y conservación están basados en un conjunto riguroso y fundado de normas técnicas de amplia aceptación por el mercado, garantizando la necesaria interoperabilidad entre los órganos de la Administración General del Estado y los Organismos Públicos vinculados o dependientes de aquella y la de éstos con los ciudadanos.

Así mismo, durante el año transcurrido, los Criterios se han actualizado incorporado las observaciones realizadas por los Departamentos ministeriales.

El Pleno de la Comisión Interministerial de Adquisición de Bienes y Servicios Informáticos (CIABSI), en su reunión del día 18 de diciembre de 2002,

ACUERDA

Primero.- Aprobar los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades.

Segundo.- Acordar la publicación de los Criterios de seguridad, normalización y conservación en la página web del Consejo Superior de Informática y para el impulso de la Administración Electrónica.

Tercero.- Encomendar a la Unidad de Apoyo del Consejo Superior de Informática y para el impulso de la Administración Electrónica el control sobre la actualización de los Criterios de seguridad, normalización y conservación. Dicha actualización se aprobará de conformidad con 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.

III) ACUERDO DEL 205º PLENO DE LA COMISIÓN INTERMINISTERIAL DE ADQUISICIÓN DE BIENES Y SERVICIOS INFORMÁTICOS

La Comisión Interministerial de Adquisición de Bienes y Servicios Informáticos, en el 205º Pleno, celebrado el 18 de diciembre de 2001, ACORDÓ:

Aprobación de los "Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades" del Consejo Superior de Informática y para el impulso de la Administración Electrónica (CSI).

Publicación de los "Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades" del CSI en el sitio web del CSI, principalmente

Los "Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades" del CSI tendrá carácter de recomendación durante un año, excepto cuando la legislación lo demande o lo acuerde el Pleno del CSI, en cuyo caso serán prescriptivos

Se encarga a la Unidad de Apoyo del CSI la actualización de los "Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades" del CSI, atendiendo a cambios en el marco normativo, estado de la tecnología y propuestas de mejora. Las nuevas versiones deberán ser aprobadas por el Pleno del CSI

Traducción y publicación en lengua inglesa

IV) ACUERDO DEL 218º PLENO DE LA COMISIÓN INTERMINISTERIAL DE ADQUISICIÓN DE BIENES Y SERVICIOS INFORMÁTICOS

La Comisión Interministerial de Adquisición de Bienes y Servicios Informáticos, en el 218º Pleno, celebrado el 18 de diciembre de 2002, ACORDÓ:

La aprobación de los "Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades", del Consejo Superior de Informática y para el impulso de la Administración Electrónica.

La publicación en el Boletín Oficial del Estado de los "Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades".

La publicación de los "Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades" en el sitio web del CSI.

V) PRESENTACIÓN

Los criterios de seguridad de las aplicaciones, de normalización y de conservación de la información tienen tres finalidades principales:

Facilitar la adopción generalizada por parte de la Administración General del Estado de medidas organizativas y técnicas que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información en las aplicaciones que ésta utiliza para el ejercicio de sus potestades.

Proporcionar el conjunto de medidas organizativas y técnicas de seguridad, normalización y conservación 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.

Promover el máximo aprovechamiento de las tecnologías de la información y las comunicaciones en la actividad administrativa, a la vez que se asegura la protección de la información de los ciudadanos en sus relaciones con la Administración.

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, normalización y conservación 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.

Consta de tres libros:

Criterios de seguridad. 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 citadas aplicaciones para ejercicio de potestades.

Criterios de normalización. Expone las pautas para facilitar la compatibilidad técnica y la interoperabilidad de las aplicaciones.

Criterios de conservación. Expone los requisitos, criterios y recomendaciones para la conservación de la información en soporte electrónico en las citadas aplicaciones.

Asimismo, los criterios, en particular los de seguridad y los de conservación, contemplan 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 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.

En todos los casos los criterios y recomendaciones se han seleccionado atendiendo a normas o estándares técnicos nacionales de reconocida autoridad. En este sentido conviene aclarar que el libro de Criterios de Normalización es complementario de los otros dos libros, en el sentido de que no se

repiten en él las normas técnicas nacionales o internacionales en las que se sustentan los criterios y las recomendaciones.

VI) MODO DE UTILIZACIÓN

Es importante advertir de la estrecha interdependencia de unos libros con los demás o de los capítulos entre sí, como consecuencia de la naturaleza compleja de la información, de los sistemas que la manejan y de la utilización que de ellos se hace. Esto es, en la generalidad de los casos reales será necesario recurrir a la aplicación conjunta de los libros y capítulos de los Criterios de Seguridad, Normalización y Conservación.

Como ilustración de lo que se dice, considérese la aplicación de lo dispuesto en La Disposición final Primera del Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

Entre los requisitos técnicos de los registros y notificaciones telemáticas y prestación del servicio de dirección electrónica única, se mencionan expresamente los de "autenticidad, integridad, disponibilidad y confidencialidad de los dispositivos y aplicaciones de registro y notificación, así como los protocolos y criterios técnicos a los que deben sujetarse". Su ejecución práctica afecta a

- Los Criterios de seguridad en su conjunto, ya que la seguridad se consigue esencialmente protegiendo la autenticidad, integridad, disponibilidad y la confidencialidad, lo cual reclama un conjunto de medidas técnicas y organizativas, en las que intervienen entrelazadamente los diferentes capítulos. En efecto, 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 con 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. En general unos y otros vendrán determinados por la identificación y clasificación de activos a proteger y las salvaguardas ligadas al personal, que serán a su vez resultado de la gestión global de la seguridad de la información y la política de seguridad. Así mismo, su implementación en el seno de los departamentos administrativos deberá tener en cuenta: el análisis y gestión de riesgos, la seguridad física y la continuidad de los servicios exigirá el Plan de contingencias. Finalmente, la verificación del cumplimiento del conjunto de los Criterios se realizará gracias a la auditoría y control de la seguridad.)
- Los Criterios de normalización, por ejemplo en lo relativo a los servicios básicos de telecomunicaciones, la presentación de los datos o los requisitos para el acceso de personas con discapacidad.
- Los Criterios de Conservación, que intervienen en todo el ciclo de vida de las comunicaciones administrativas utilizadas en el ejercicio de potestades.

Por otra parte, "*los protocolos y criterios técnicos para la solicitud y recepción de los certificados telemáticos y las transmisiones de datos regulados en los artículos 13, 14 y 15 del Real Decreto 263/1996, de 16 de febrero, serán los establecidos en cada caso por el órgano certificante o titular de los correspondientes datos por medio de las correspondientes Resoluciones o Instrucciones*". Ahora bien, estos no pueden seleccionarse de manera arbitraria sino que habrán de establecerse *"en el marco de los criterios de seguridad, normalización y conservación a los que se refiere el citado Real*

Decreto." La voluntad del legislador de promover la racionalidad y la economía y de evitar las situaciones de aislamiento tecnológico queda subrayada cuando establece la preferencia de que *"Siempre que sea técnicamente posible, las remisiones o accesos a certificados telemáticos se realizarán a través de la Intranet administrativa."* En definitiva se vuelve al mismo conjunto de pautas que ha de guiar cualquier desarrollo tecnológico.

Razonamiento similar puede hacerse respecto de las condiciones que ha de reunir el órgano, organismo o entidad habilitado para la prestación del servicio de dirección electrónica única así como las condiciones de su prestación..

En definitiva , las normas técnicas ajenas a las que se recogen en los presentes Criterios únicamente pueden utilizarse cuando sean complementarias, no alternativas a las que a continuación se recogen.

MINISTERIO
DE ADMINISTRACIONES
PÚBLICAS

SECRETARÍA GENERAL
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

24 de junio de 2004

Madrid, junio de 2004

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.
Versión 2.2. Aprobada por la Sesión plenaria de la CIABSI de 24 de junio de 2004.	Actualización programada: Actualización de contenidos, revisión de las referencias al RD 994/1999, revisión editorial.

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 ISO/IEC 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)

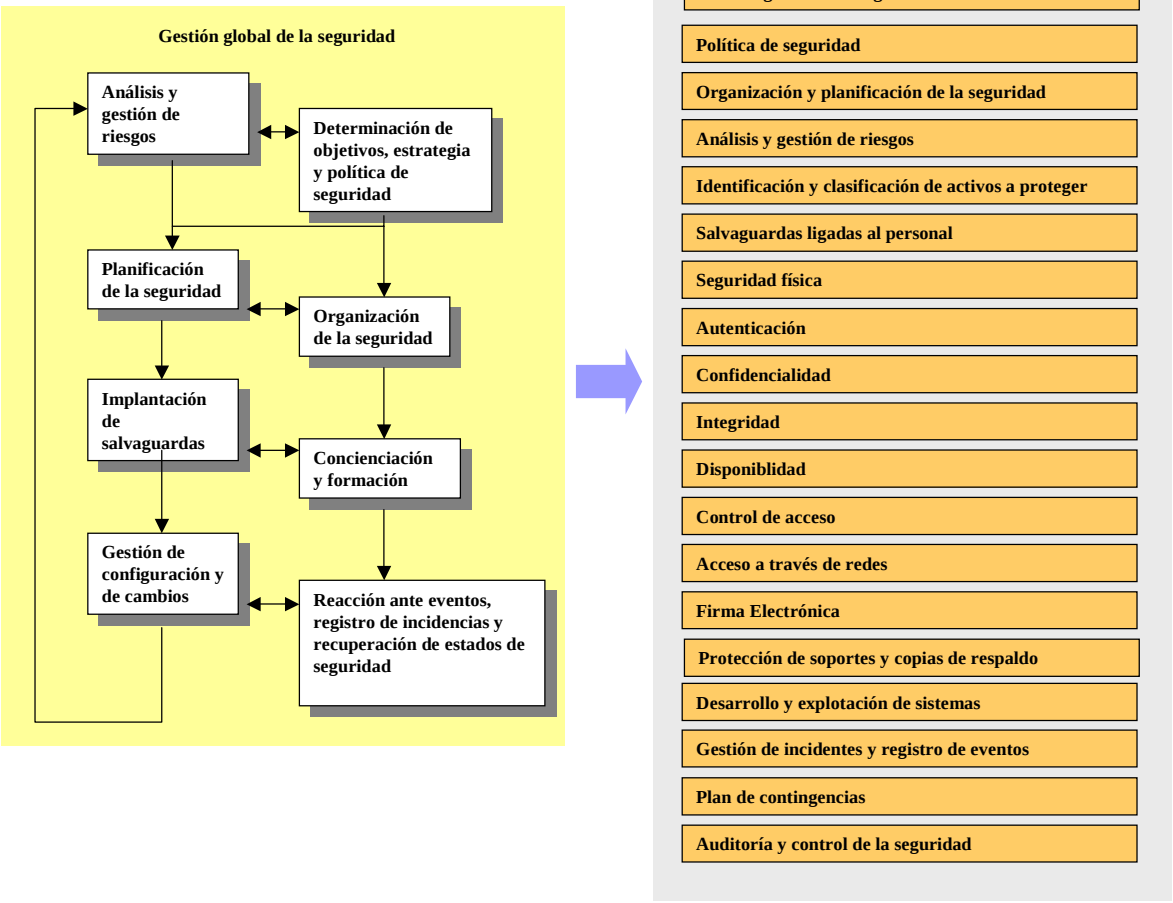
En relación con la protección de los datos de carácter personal:

- 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.

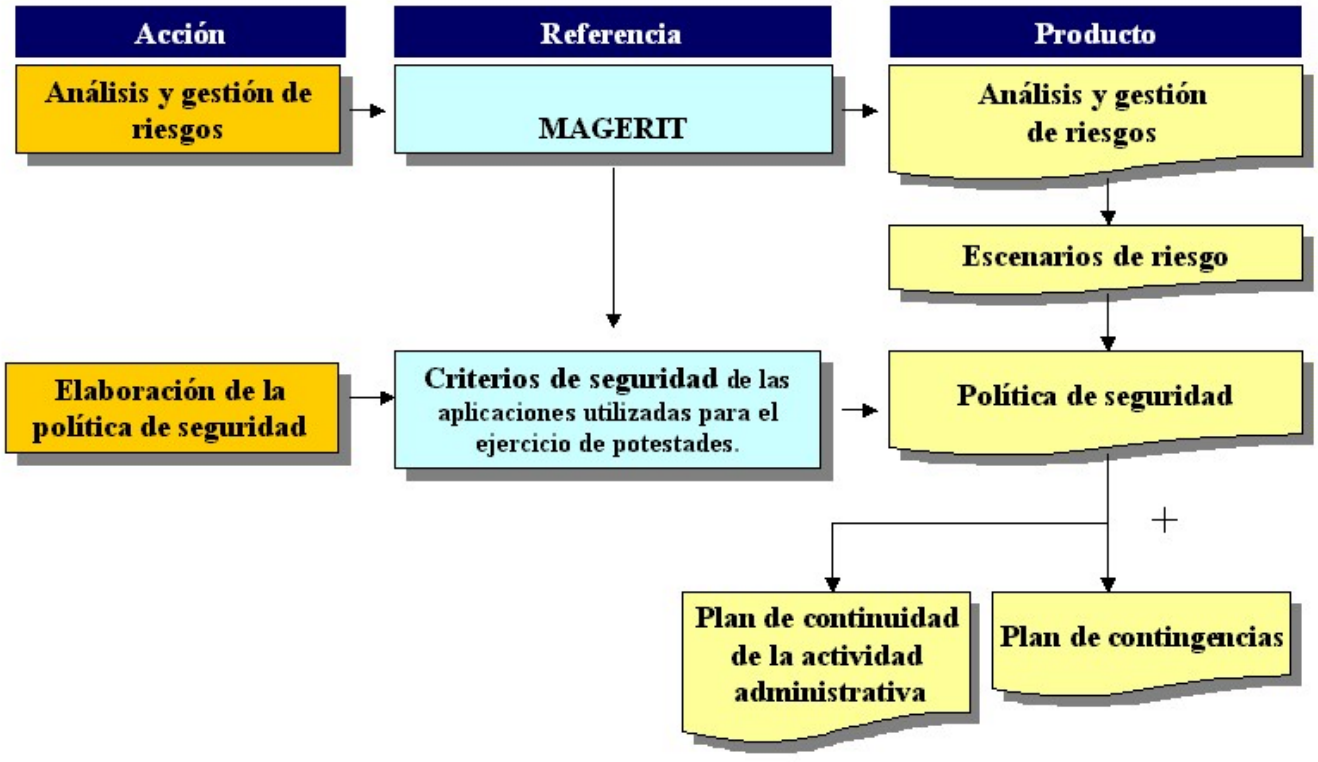
AMPLIACIÓN TÉCNICA:

- 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.csi.map.es/csi/pg5m20.htm
- UNE ISO/IEC 17799 – Tecnologías de la información – Código de buenas prácticas para la gestión de la seguridad de la información
- *INFORMATION TECHNOLOGY Baseline Protection Manual*; capítulos 2 y 3; http://www.bsi.bund.de/gshb/english/etc/inhalt.htm
- UNE 71501-1, -2, -3 IN Tecnología de la Información. Guía para la gestión de la seguridad de TI.
- Guía de seguridad informática (SEDISI), http://www.sedisi.es/05_Estudios/05_general.htm#seg
- 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.csi.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:

En medidas de seguridad de nivel básico:

- El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información. (RD 994/1999, arts. 8.1, 8.2). El documento deberá contener como mínimo 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.
- El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. (RD 994/1999, art.8.3)
- El contenido del documento deberá adecuarse a las disposiciones vigentes en materia de seguridad de los datos de carácter personal. (RD 994/1999, art.8.4)

En medidas de seguridad de nivel medio:

- El documento de seguridad deberá contener la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado. (RD 994/1999, art.15)

CRITERIOS:

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

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.csi.map.es/csi/pg5m20.htm
- UNE ISO/IEC 17799 – Tecnologías de la información – Código de buenas prácticas para la gestión de la seguridad de la información; capítulo 3.
- *Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook;* capítulo 5; http://csrc.nist.gov/publications/nistpubs/800-12/
- UNE 71501-1 IN Tecnología de la Información. Guía para la gestión de la seguridad de TI. Conceptos y modelos para la seguridad de TI; 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.csi.map.es/csi/pg5m20.htm
- UNE ISO/IEC 17799 - Tecnologías de la información - Código de buenas prácticas para la gestión de la seguridad de la información; 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

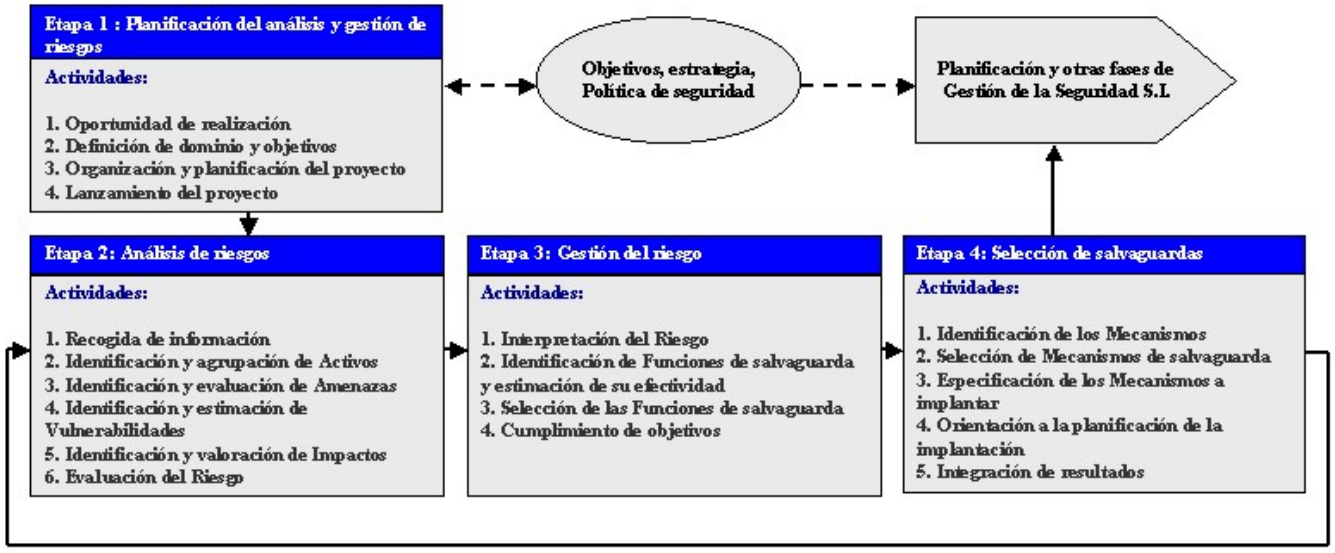
CONCEPTOS:

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.csi.map.es/csi/pg5m20.htm
- UNE ISO/IEC 17799 – Tecnologías de la información - Código de buenas prácticas para la gestión de la seguridad de la información.
- *INFORMATION TECHNOLOGY Baseline Protection Manual*; capítulo 3.2; http://www.bsi.bund.de/gshb/english/etc/inhalt.htm .
- UNE 71501-1, -2, -3 IN Tecnología de la Información. Guía para la gestión de la seguridad de TI..

6 Identificación y clasificación de activos a proteger

MARCO LEGAL:

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

- Las medidas de seguridad exigibles se clasifican en tres niveles: básico, medio y alto. Dichos niveles se establecen atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información. (RD 994/1999; art. 3)
- Aplicación de los niveles de seguridad (RD 994/1999; art. 4)
  - Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.
  - Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el artículo 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.
  - Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto.
  - Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20.
  - Cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes.

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)

En medidas de seguridad de nivel básico:

- Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas. (RD 994/1999, art. 9.1)
- El responsable del fichero adoptará las medidas necesarias 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)

En medidas de seguridad de nivel medio:

- El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. (RD 994/1999, art. 16)

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. Un ejemplo clásico es la separación entre explotación y desarrollo.

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 Establecer obligaciones de confidencialidad en los casos de personal con contratos temporales o personal perteneciente a empresas subcontratadas, cuando la información que puedan manejar en el desempeño de sus obligaciones temporales sean datos de carácter personal, u otra información sensible. El personal temporal o subcontratado deberá aceptar expresamente las prescripciones de confidencialidad.

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.csi.map.es/csi/pg5m20.htm
- UNE ISO/IEC 17799 - Tecnologías de la información - Código de buenas prácticas para la gestión de la seguridad de la información; 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/
- UNE 7150-3 IN Tecnología de la Información. Guía para la gestión de la seguridad de TI y ISO/IEC TR 13335-4 Tecnologías de la información (TI) - Guía para la gestión de la seguridad de TI.

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:

En medidas de seguridad de nivel básico:

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

En medidas de seguridad de nivel medio:

- Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal. (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.csi.map.es/csi/pg5m20.htm
- ISO/IEC 17799 – Tecnologías de la información - Código de buenas prácticas para la gestión de la seguridad de la información; 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/
- UNE 7150-3 IN Tecnología de la Información. Guía para la gestión de la seguridad de TI y ISO/IEC TR 13335-4 Tecnologías de la información (TI) - Guía para la gestión de la seguridad de TI..

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.

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:

- El responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso. (RD 994/1999, art. 11.1)
- Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. (RD 994/1999, art. 11.2)
- Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán 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:

- El responsable del fichero establecerá 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)
- Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información. (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-1024 o equivalente, 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.csi.map.es/csi/pg5m20.htm
- UNE ISO/IEC 17799 - Tecnologías de la información - Código de buenas prácticas para la gestión de la seguridad de la información; 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/
- UNE 71501-1, -2, -3 IN Tecnología de la Información. 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.csi.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. (RD 263/1996, 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. (RD 263/1996, 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)

En medidas de seguridad de nivel alto:

- La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.
- (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-1024 o equivalente 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.csi.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.csi.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)

En medidas de seguridad 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 seguridad de nivel alto:

- El período mínimo de conservación de los datos registrados será de dos años. (RD 994/1999, art. 24.4)
- 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.csi.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.csi.map.es/csi/pg3410.htm)
- Alerta-Antivirus. Página del Centro de Alerta Temprana sobre Virus y Seguridad Informática. Ministerio de Industria, Comercio y Turismo, Res; http://www.alerta-antivirus.es/index.html
- 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)

En medidas de seguridad de nivel básico:

- 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)

En medidas de seguridad seguridad de nivel alto:

- 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.csi.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.csi.map.es/csi/pg3410.htm)
- Alerta-Antivirus. Página del Centro de Alerta Temprana sobre Virus y Seguridad Informática. Ministerio de Industria, Comercio y Turismo. Red-es; http://www.alerta-antivirus.es/index.html

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 'A*utenticación*')
- 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)

En medidas de seguridad de nivel básico:

- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones. (RD 994/1999, art. 12.1)
- El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos a los autorizados. (RD 994/1999, art. 12.2)
- La relación de usuarios contendrá el acceso autorizado para cada uno de ellos (RD 994/1999, art. 12.3)
- Exclusivamente el personal autorizado para ello en el documento de seguridad podrán conceder, alterar o anular el acceso autorizado sobre datos o recursos, conforme los criterios establecidos por el responsable del fichero. (RD 994/1999, art. 12.4)

En medidas de seguridad de nivel medio:

- El responsable del fichero establecerá 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)
- Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información. (RD 994/1999, art. 18.1)

En medidas de seguridad de nivel alto:

- De cada acceso se guardarán como mínimo , 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)
- 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, 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 competente 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).

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 aplicables 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.csi.map.es/csi/pg5m20.htm
- UNE ISO/IEC 17799 – Tecnologías de la información - Código de buenas prácticas para la gestión de la seguridad de la información; 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.csi.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:

- Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de telecomunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local. (RD 994/1999; art. 5)

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

- La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros. (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.csi.map.es/csi/pg5m20.htm
- UNE ISO/IEC 17799 – Tecnologías de la información – Código de buenas prácticas para la gestión de la seguridad de la información; 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
- UNE 71501-1, -2, -3 IN Tecnología de la Información. 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.csi.map.es/csi/pg3410 .htm)
- 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:

Son de aplicación las siguientes definiciones de la Ley 59/2003, de 19 de diciembre, de firma electrónica:

Firma electrónica: La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Firma electrónica avanzada: La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

Firma electrónica reconocida: Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Documento electrónico: Se considera documento electrónico el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente. El documento electrónico será soporte de:

a) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.

b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.

c) Documentos privados.

Prestador de servicios de certificación: Se denomina prestador de servicios de certificación la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

Certificado electrónico: Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

Firmante: El firmante es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.

Certificado reconocido: Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley 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. Los certificados reconocidos incluirán, al menos, los siguientes datos

a) La indicación de que se expiden como tales.

b) El código identificativo único del certificado.

c) La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.

d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.

e) La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.

f) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.

g) El comienzo y el fin del período de validez del certificado.

h) Los límites de uso del certificado, si se establecen.

i) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite.

Documento nacional de identidad electrónico: El documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.

Declaración de prácticas de certificación: . Todos los prestadores de servicios de certificación formularán una declaración de prácticas de certificación en la que detallarán, en el marco de esta ley y de sus disposiciones de desarrollo, las obligaciones que se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados y, en su caso la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata

sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros.

Datos de creación de firma: Los datos de creación de firma son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.

Dispositivo de creación de firma: Un dispositivo de creación de firma es un programa o sistema informático que sirve para aplicar los datos de creación de firma.

Dispositivo seguro de creación de firma: Un dispositivo seguro de creación de firma es un dispositivo de creación de firma que ofrece, al menos, las siguientes garantías:

a) Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.

b) Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.

c) Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.

d) Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.

Datos de verificación de firma: Los datos de verificación de firma son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

Dispositivo de verificación de firma: Un dispositivo de verificación de firma es un programa o sistema informático que sirve para aplicar los datos de verificación de firma. Los dispositivos de verificación de firma electrónica garantizarán, siempre que sea técnicamente posible, que el proceso de verificación de una firma electrónica satisfaga, al menos, los siguientes requisitos:

a) Que los datos utilizados para verificar la firma correspondan a los datos mostrados a la persona que verifica la firma.

b) Que la firma se verifique de forma fiable y el resultado de esa verificación se presente correctamente.

c) Que la persona que verifica la firma electrónica pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.

d) Que se muestren correctamente tanto la identidad del firmante o, en su caso, conste claramente la utilización de un seudónimo, como el resultado de la verificación.

e) Que se verifiquen de forma fiable la autenticidad y la validez del certificado electrónico correspondiente.

f) Que pueda detectarse cualquier cambio relativo a su seguridad.

Certificación de un prestador de servicios de certificación: La certificación de un prestador de servicios de certificación es el procedimiento voluntario por el que una entidad cualificada pública o privada emite una declaración a favor de un prestador de servicios de certificación, que implica un reconocimiento del cumplimiento de requisitos específicos en la prestación de los servicios que se ofrecen al público.

Certificación de dispositivos seguros de creación de firma electrónica: La certificación de dispositivos seguros de creación de firma electrónica es el procedimiento por el que se comprueba que un dispositivo

cumple los requisitos establecidos en esta ley para su consideración como dispositivo seguro de creación de firma.

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)
- Las disposiciones de creación de registros telemáticos tendrán entre sus contenidos mínimos el sistema o sistemas de firma electrónica reconocidos por el registro para la identificación del usuario y la admisión de la solicitud, escrito o comunicación. **(**RD 209/2003-RD 772/1999, art. 14)
- En relación con los *Certificados telemáticos**,*** *e*l certificado telemático contendrá los datos objeto de certificación y la firma electrónica de la autoridad competente para expedirlos.(RD 209/2003-RD 263/1996, art. 14)
- Los Requisitos de autenticidad de los dispositivos y aplicaciones de registro y notificación contemplan que los dispositivos y las aplicaciones de registro y notificación sólo admitirán la firma electrónica avanzada basada en un certificado reconocido que cumpla la recomendación UIT X.509 versión 3 o superiores (ISO/IEC 9594-8 de 1997) de acuerdo con lo previsto en la legislación de firma electrónica. (Orden PRE/1551/2003, Tercero)
- Asimismo, la aceptación de una firma electrónica estará condicionada a que la utilización del servicio de consulta sobre la vigencia de los certificados en los que se basen dicha firma electrónica no suponga un coste específico adicional para los órganos, organismos o entidades incluidas en el ámbito de aplicación de la presente Orden. (Orden PRE/1551/2003, Tercero)
- En relación con los requisitos de integridad de los dispositivos y aplicaciones de registro y notificación, los órganos de la Administración General del Estado y los Organismos Públicos vinculados o dependientes de aquélla que pongan en marcha dispositivos y aplicaciones de registro y notificación, deberán contar con medidas organizativas y técnicas para garantizar la integridad de la información. Entre las medidas a establecer figura la aplicación de técnicas de comprobación de la integridad de la información, como firma electrónica (con los requisitos señalados en el apartado tercero), funciones resumen o «hash», y en su caso, de fechado electrónico. (Orden PRE/1551/2003, Cuarto).

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:

- Ley 59/2003, de 19 de diciembre, de firma electrónica
- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999.
- 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, cuyos requisitos mínimos son:

- Un par de claves complementarias, una pública y otra privada, generadas con algoritmos de cifrado asimétrico RSA-1024 o equivalente.
- Una función resumen o hash, preferiblemente SHA-1 (longitud 160 bits) o MD5 (128 bits) o mejores.
- 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, o versiones posteriores.

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, en particular, la norma ISO/IEC 18014 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 conformes 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:

- 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.csi.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.csi.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)
- 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 perdida o destrucción. (RD 994/1999, art. 14.2)
- Deberán realizarse 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:

- Deberá establecerse 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)
- Se dispondrá 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)
- Deberá conservarse una copia de respaldo y de 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.

16.11 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.

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.csi.map.es/csi/pg5m20.htm
- UNE ISO/IEC 17799 Tecnologías de la información - Código de buenas prácticas para la gestión de la seguridad de la información; capítulos 8.4.1.
- *INFORMATION TECHNOLOGY Baseline Protection Manual*; capítulo 3.4; http://www.bsi.bund.de/gshb/english/etc/inhalt.htm
- UNE 71501-1, -2, -3 IN Tecnología de la Información. Guía para la gestión de la seguridad de TI..

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:

- La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado. (RD 994/1999, art. 6)
- Los ficheros temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios establecidos en el Reglamento. (RD 994/1999, art. 7.1)
- Todo fichero temporal será borrado una vez haya dejado de ser necesario para los fines que motivaron su creación. (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)
- Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado. (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.csi.map.es/csi/pg5m20.htm
- UNE ISO/IEC 17799 – Tecnologías de la información – Código de buenas prácticas para la gestión de la seguridad de la informacións*)*; 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
- UNE 71501-1, -2, -3 IN Tecnología de la Información. Guía para la gestión de la seguridad de TI..
- ISO/IEC WD 15446, *Guide on the production of protection profiles and security targets* http://www.commoncriteria.org/protection_profiles/pp.html

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:

- El procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar 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:

- En el registro deberán consignarse además, los procedimientos realizados de recuperación de 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)
- Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de 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 superior o 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.csi.map.es/csi/pg5m20.htm
- UNE ISO/IEC 17799 – Tecnologías de la información – Código de buenas prácticas para la gestión de la seguridad de la información; 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

- UNE 71501-1, -2, -3 IN Tecnología de la Información. 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.csi.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:

- UNE ISO/IEC 17799 – Tecnologías de la información – Código de buenas prácticas para la gestión de la seguridad de la información; 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 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).

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:

- Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoria interna o externa que verifique el cumplimiento del Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años. (RD 994/1999, art. 17.1)
- El informe de auditoria deberá dictaminar sobre la adecuación de las medidas y controles al 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)
- Los informes de auditoría serán analizados 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).
- Registro de accesos (RD 994/1999; art. 24)
  - 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 competente 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.

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.csi.map.es/csi/pg5m20.htm)
- UNE ISO/IEC 17799 – Tecnologías de la información – Código de buenas prácticas para la gestión de la seguridad de la información; 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
- *COBIT: Control Objectives for Information and related Technology*; http://www.itgi.org

MINISTERIO
DE ADMINISTRACIONES
PÚBLICAS

SECRETARÍA GENERAL
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 NORMALIZACIÓN

24 de junio de 2004

Madrid, junio de 2004

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. Presentada al Pleno de CIABSI de 18 de 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.
Versión 2.2. Aprobada por la Sesión plenaria de la CIABSI de 24 de junio de 2004.	Actualización programada: actualización de contenidos, revisión editorial.

1 Presentación

Introducción

Este documento elaborado por el Consejo Superior de Informática y para el impulso de la Administración Electrónica, expone las pautas para la normalización en los servicios electrónicos prestados por los órganos y entidades del ámbito de la Administración General del Estado con el objeto de facilitar la compatibilidad técnica, la disponibilidad y la interoperabilidad.

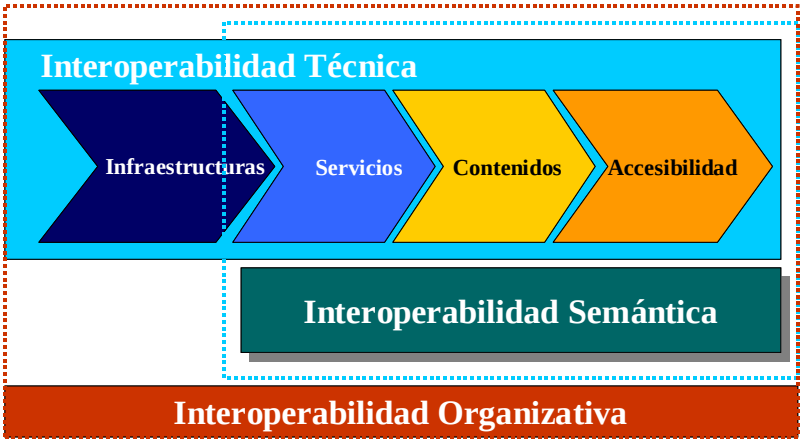
El Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado encomienda al Consejo Superior de Informática y para el Impulso de la Administración Electrónica la aprobación y difusión de los criterios de normalización 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.

Adopción de medidas de interoperabilidad

Las aplicaciones utilizadas para el ejercicio de potestades deben poder desplegarse en un entorno que facilite la interoperabilidad de los siguientes elementos:

- Infraestructuras
- Servicios
- Contenidos
- Accesibilidad

Es habitual presentar estos elementos según un modelo conceptual de pirámide; sin embargo, la experiencia demuestra que su comportamiento práctico responde al principio de la cadena, de forma que cualquier obstáculo a la interoperabilidad, en cualquiera de los eslabones, afecta negativamente a la posibilidad de despliegue de la aplicación y de la prestación del servicio correspondiente.



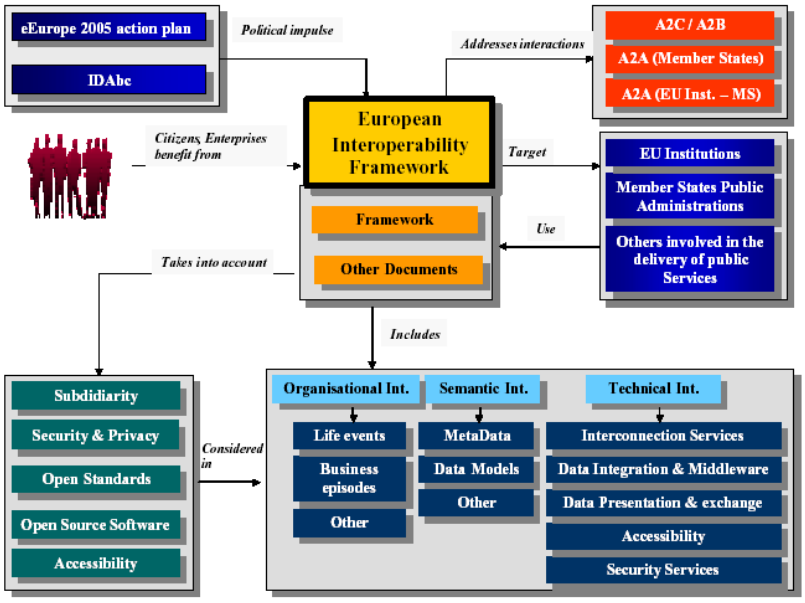
La cadena de interoperabilidad

Aunque el ámbito de las cuestiones que afectan a la interoperabilidad es muy extenso, el acuerdo sobre un conjunto de normas facilita la interoperabilidad y se configura como el elemento clave de la racionalidad técnica y económica ya que su presencia es la que permite que el despliegue de las

aplicaciones se pueda realizar de forma más rápida, más flexible y con menor coste. Es evidente, no obstante, que las normas por sí solas no garantizan que los procesos sean completamente independientes de las plataformas tecnológicas, pero al mismo tiempo la referencia a normas de autoridad es condición necesaria para la interoperabilidad. El reconocimiento de este hecho, se manifiesta en que diversos países de nuestro entorno (Reino Unido, Francia y Alemania) vienen desarrollando las denominadas infraestructuras de interoperabilidad para facilitar el establecimiento de los servicios Administración-Ciudadano, Administración-empresa y Administración-Administración.

En particular, el **documento de trabajo de la Comisión sobre interoperabilidad** (*Linking up Europe: the importance of interoperability for e-government services*) recoge el carácter estratégico de la interoperabilidad, desde los puntos de vista económico y técnico, como elemento esencial para el desarrollo de los servicios de Administración Electrónica a los niveles paneuropeo y nacional (central, regional y local); expone que no es posible la ejecución de las diversas políticas (mercado interior, crecimiento sostenido, seguridad, etc.) en un escenario donde no sea posible la interoperabilidad de los servicios de Administración electrónica, donde se produzcan 'islas' en la prestación de los servicios por la fragmentación de los esfuerzos a todos los niveles de la Administración; e identifica la interoperabilidad como clave para compartir y reutilizar la información y para la prestación de los servicios de Administración Electrónica y difusión de la información administrativa a través de múltiples canales.

Asimismo, el Plan de Acción eEurope 2005 encomienda a la Comisión Europea la elaboración del Marco Europeo de Interoperabilidad, tarea de la cual se encarga el Programa IDA (Intercambio de Datos entre Administraciones). Este Marco Europeo de interoperabilidad debe abordar los contenidos de información y las políticas y especificaciones técnicas recomendadas para combinar los sistemas de información de la administración pública de toda la UE; se debe basar en normas abiertas y fomentará el uso de programas de fuente abierta; y contempla que los Estados miembros dispongan en su ámbito de un marco de interoperabilidad propio o de un instrumento equivalente, que en nuestro caso corresponde con los presentes Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades.



Marco Europeo de Interoperabilidad (Fuente: *European Interoperability Framework for Pan-European eGovernment Services – Framework*), Programa IDA, Comisión Europea.

Objetivos

Este documento tiene por objetivo facilitar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones en la actividad administrativa en condiciones de racionalidad y economía, mediante la adopción de normas que asegurar la interoperabilidad de los sistemas informáticos y telemáticos.

Estructura y contenidos

Este documento se estructura en los siguientes capítulos:

- Presentación.
- Interoperabilidad.
- Metadatos.
- Desarrollo de sistemas de información.
- Requisitos de diseño de páginas *web* y de accesibilidad para personas con discapacidad.
- Software libre y de fuente abierta.

En relación con las cuestiones que se tratan se recogen *criterios* que señalan las normas que se deben adoptar y que se numeran para facilitar su localización y referencia; las ***normas aplicables*** remiten a referencias concretas; asimismo, se incluyen ***consideraciones*** con alguna explicación o matización del alcance o contenidos y un apartado de ***ampliación técnica*** con referencias para ampliar y profundizar en las normas y conceptos técnicos.

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".

En este documento se han utilizado con carácter equivalente los términos *norma* y *estándar*; el primero se ha utilizado para referencias genéricas mientras que el término *estándar* se ha utilizado para referencias más especificas.

Modo de utilización

Es importante hacer notar que las normas técnicas relativas a la seguridad y a la conservación figuran en los libros correspondientes, por lo que no se repiten aquí. Se remite al lector interesado a *Criterios de Seguridad* y a *Criterios de Conservación*, respectivamente.

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.

Actualizaciones

Por la naturaleza de su contenido, 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.

2 Intranet Administrativa

Interconexión de redes

CONSIDERACIONES:

En primer lugar, hay que resaltar que las normas y recomendaciones que aquí se recogen están basadas y deben estar ligadas a la Intranet Administrativa.

La Intranet Administrativa es la infraestructura básica de comunicaciones y de servicios telemáticos comunes, para el intercambio electrónico seguro de información entre departamentos de la Administración General del Estado, y entre esta y las Administraciones de Comunidades Autónomas, Corporaciones locales y Unión Europea.

Es importante el compromiso con la Intranet Administrativa debido a que sienta las bases para el desarrollo de la Administración electrónica y debido a la racionalización de las comunicaciones que conlleva.

CRITERIOS:

2.1 La interconexión desde los organismos de la Administración General del Estado se realiza utilizando las Áreas de Conexión en cada Departamento Ministerial. Se parte de la existencia de una Unidad en cada uno de ellos que tiene las competencias para procurar estos servicios a todos sus centros directivos y organismos autónomos.

2.2 Igualmente por racionalidad técnica y económica, el acceso de la Administración a los servicios paneuropeos de Administración Electrónica se canaliza a través del enlace entre la Intranet Administrativa con TESTA II y, en particular, el tráfico se canaliza a través de las respectivas conexiones de los Departamentos Ministeriales con la Intranet Administrativa.

2.3 Siempre que sea posible, los sistemas de la Administración utilizarán los servicios de infraestructura (Intranet Administrativa y servicios conexos) y proporcionarán los datos requeridos para desarrollar dichos servicios con arreglo a los requisitos de los citados sistemas.

Protocolos de nivel bajo

CONSIDERACIONES:

Se han tenido en cuenta aquellos protocolos más cercanos al nivel físico que pudieran tener relación con la interoperabilidad de los servicios:

- Transmisión en redes troncales: JDS (Jerarquía Digital Síncrona), WDM (*Wavelenght Division Multiplexing)*
- Transporte sobre redes troncales: ATM (*Asyncronous Transfer Mode).*

- De acceso remoto: Frame Relay, DSL (*Digital Subscriber Line*).
- Interconexión de PBX: QSIG.

RECOMENDACIONES:

- Utilizar tecnologías JDS o WDM en las redes troncales.
- Usar ATM como transporte en la redes troncales.
- Usar tecnologías Frame Relay o DSL para los servicios de acceso remoto.
- Permitir la interconexión de PBX mediante señalización QSIG.

NORMAS APLICABLES:

Jerarquía Digital Síncrona:

- ITU-T G.707: Network Node Interface for the Synchronous Digital Hierarchy (SDH).
- ITU-T G.783: Characteristics of Synchronous Digital Hierarchy (SDH) Equipment Functional Blocks.
- ITU-T G.803: Architecture of Transport Networks Based on the Synchronous Digital Hierarchy (SDH).

WDM:

- ITU-T G.983: A broadband optical access system with increased service capability by wavelength allocation.

ATM:

- ITU-T I.121: Broadband aspects of ISDN.
- ITU-T I.731 y siguientes: Types and general characteristics of ATM equipment.

QSIG:

- ITU-T Q.93x y Q.95x.

Frame Relay:

- ITU-T Q.922: ISDN data link layer specification for frame mode bearer services.

DSL:

- ITU-T G991-997.

AMPLIACIÓN TÉCNICA:

- http://www.itu.int/; ATM: http://www.atmforum.com/.

Protocolos de nivel medio

CONSIDERACIONES:

Se han considerado aquellos protocolos de soporte a las aplicaciones que mayor importancia tienen en la interconexión de servicios: IP, TCP/UDP, Ipsec, MPLS, H.323.

CRITERIOS:

2.4 Se debe utilizar IP v4 en las comunicaciones de datos, excepto en los sistemas propietarios ya existentes.

2.5 Se debe cumplir el Plan de Direccionamiento e interconexión de redes de área local en la Administración (INTERRAL).

2.6 Se debe emplear SSLv3/TLS para las aplicaciones web que requieran confidencialidad en las comunicaciones.

RECOMENDACIONES:

- La utilización de IPv6 se recomienda en la medida que esté disponible.
- Usar tecnologías de conectividad extremo a extremo basadas en IPsec (redes privadas virtuales).
- Basar en H.323 los sistemas de Voz sobre IP, videoconferencia, y otros de transmisión audio/vídeo.

NORMAS APLICABLES:

Protocolos relativos al direccionamiento IP

- RFC 1219 – Sugiere un procedimiento de asignación de direcciones a subredes basado en la utilización de máscaras.
- RFC 1918 – Define los rangos de direcciones IP a utilizar en redes privadas. Reserva para redes privadas una dirección clase A, que puede contener hasta 64.516 subredes con 256 maquinas cada una.

Protocolos de interconexión LAN-WAN

- Protocolo Internet v4 (Ipv.4)
- RFC 791 (Estándar STD5) - IP es un protocolo de nivel 3 utilizado para la interconexión de ordenadores situados en la misma o en distintas redes de paquetes. La dirección de cada uno de los ordenadores que están en la red tiene una longitud de 32 bits, distribuidos en 4 palabras de 8 bits, que identifican de forma universal la red y el ordenador a la que pertenece.
- **Plan de Direccionamiento e interconexión de redes de área local en la Administración (INTERRAL)** Especifica el plan de direccionamiento de la Administración, aprobado por el Grupo de Usuarios de Telecomunicaciones de la Administración, para protocolos TCP/IP definiendo un espacio privado de direcciones común para todos los Centros de la Administración. www.csi.map.es/csi/pg3305.htm

Protocolo del nivel de trasporte

- RFC 793 (Estándar STD7) - TCP es un protocolo de nivel de transporte orientado a conexión que proporciona una conexión fiable extremo a extremo entre aplicaciones que se ejecutan en máquinas situadas en la misma o en distintas redes interconectadas.
- El protocolo TCP, junto con el protocolo de nivel de red IP es uno de los principales responsables del desarrollo de internet.
- RFC 768 (Estándar STD6) - UDP define los mecanismos para transmitir información entre aplicaciones utilizando un número mínimo de elementos. UDP no está orientado a conexión.

IPSEC

- RFC 2401: Security Architecture for the Internet Protocol

H.323

- ITU-T H.323

SSLv3/TSL

- http://home.netscape.com/eng/ssl3/index.html
- RFC 2246: "TSL 1.0"

AMPLIACIÓN TÉCNICA:

- ftp://ftp.isi.edu/in-notes/rfc791.txt
- ftp://ftp.rfc-editor.org/in-notes/rfc1918.txt
- ftp://ftp.rfc-editor.org/in-notes/rfc1219.txt
- ftp://ftp.isi.edu/in-notes/rfc793.txt
- ftp://ftp.isi.edu/in-notes/rfc768.txt

Servicios básicos
Servicios de nombres de dominio

CONSIDERACIONES:

El servicio de nombres de dominio permite la traducción de un nombre sencillo de recordar a la dirección IP asociada, que es utilizada por las máquinas para comunicarse bajo ese protocolo. Este servicio dispone de una estructura distribuida y jerárquica representable fácilmente en forma de árbol.

CRITERIOS:

2.7 Se debe emplear el servicio de nombres de dominio en la publicación de servicios, siguiendo las reglas al respecto marcadas por la Intranet Administrativa.

RECOMENDACIONES:

- Los servidores DNS deberán tener una funcionalidad de BIND 9.2.1 o superior.

NORMAS APLICABLES:

Protocolos relativos a la especificación e implantación de nombres de dominio

- RFC 1034 (Estándar STD13) - El objeto de RFC 1034 es especificar los nombres de dominios de los servicios web y las direcciones de correo electrónico.
- RFC 1035 (Estándar STD13) - El objeto de RFC 1035 es proporcionar el mecanismo para asignar nombres a los recursos de red.
- BIND 8.2.4 (Estándar ISC) – *Berkeley Internet Name Domain* es una implementación del DNS especificada por ISC que se encarga de traducir las direcciones a formato numérico, para que los sistemas puedan establecer la conexión.

AMPLIACIÓN TÉCNICA:

- ftp://ftp.rfc-editor.org/in-notes/rfc1034.txt
- ftp://ftp.rfc-editor.org/in-notes/rfc1035.txt

Directorio

CONSIDERACIONES:

El servicio de directorio responde a la necesidad de compartir y administrar de modo consistente, con acceso integrado y distribuido, la información sobre servicios, recursos, usuarios y objetos.

RECOMENDACIONES:

- Los sistemas de directorio soportarán el conjunto de protocolos X.500 y LDAPv3.
- Los sistemas de acceso a los directorios emplearán LDAPv3.

NORMAS APLICABLES:

- X.500**:** Serie X.500 del ITU-T
- Protocolos de acceso a directorios (*Lightweight Directory Access Protocol* v3 - LDAP v3)
- RFC 2251 - LDAP está concebido para proporcionar acceso a los directorios X.500 utilizando menos recursos. Los elementos del protocolo son transportados directamente sobre el protocolo de Transporte (TCP u otros), saltándose gran parte de los niveles superiores de sesión/presentación.

AMPLIACIÓN TÉCNICA:

- ftp://ftp.rfc-editor.org/in-notes/rfc2251.txt

Protocolos de transferencia de ficheros

CONSIDERACIONES:

FTP es un protocolo ampliamente utilizado y disponible en la totalidad de plataformas existentes.

RECOMENDACIONES:

- Aplicar FTP para las transferencias de ficheros.

NORMAS APLICABLES:

Protocolo FTP

- RFC 959 (Estándar 13) – especifica la última versión del protocolo de transferencia de ficheros FTP.

AMPLIACIÓN TÉCNICA:

- ftp://ftp.rfc-editor.org/in-notes/rfc959.txt
- ftp://ftp.rfc-editor.org/in-notes/rfc2228.txt
- ftp://ftp.rfc-editor.org/in-notes/rfc2640.txt

Correo electrónico

CONSIDERACIONES:

El correo electrónico se ha convertido en una herramienta básica de comunicación a la que se le exigen nuevas funcionalidades como el soporte del cifrado y de la firma electrónica.

CRITERIOS:

2.8 Se debe emplear correo electrónico basado en el protocolo SMTP. No obstante, se permite la continuidad de los sistemas de correo X.400 existentes.

2.9 Los sistemas SMTP deben soportar **ESMTP** (*Extended Simple Mail Transport Protocol*, incluidos los servicios Delivery Status Notifications y Message Disposition Notifications), así como **MIME**.

2.10 Los clientes y servidores SMTP deben soportar **POP3 e IMAP4**.

2.11 El intercambio de correo seguro se realizará mediante **S/MIME 3.0**.

NORMAS APLICABLES:

- RFC 821 SMTP *Simple Mail Transfer Protocol* (Estándar STD10). ftp://ftp.isi.edu/in-notes/rfc821.txt

- RFC 822 *Standard for the format of ARPA Internet text messages* (Estándar STD11) - Especifica con detalle la sintaxis de las cabeceras de los mensajes de texto que intercambian los usuarios de correo electrónico. El cuerpo de los mensajes es texto plano en formato US-ASCII. ftp://ftp.isi.edu/in-notes/rfc822.txt
- RFC 2045 *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies* - La serie de RFCs MIME redefine el formato especificado en RFC 822 para permitir ampliar los tipos de mensajes a intercambiar por SMTP y poder incluir ficheros tipo MIME. ftp://ftp.rfc-editor.org/in-notes/rfc2045.txt
- RFC 2046 *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types* - especifica los contenidos del campo "content-type" para identificar la naturaleza de los datos incluido en el cuerpo de la entidad MIME. El campo "content-type" incluye información del tipo y subtipo e información auxiliar. ftp://ftp.rfc-editor.org/in-notes/rfc2046.txt
- RFC 2047 MIME *Multipurpose Internet Mail Extensions Part Three: Message Header Extensions for Non-ASCII Text* - permite resolver las dificultades que tienen algunos clientes de correo para interpretar correctamente las ciertas cabeceras definidas por RFC 2045. ftp://ftp.rfc-editor.org/in-notes/rfc2047.txt
- RFC 2049 *Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples* - especifica los requisitos de conformidad que debe cumplir un agente para interpretar correctamente las especificaciones MIME. ftp://ftp.rfc-editor.org/in-notes/rfc2049.txt
- ESMTP. RFC: 1869,1652,1891-94
- S/MIME. RFC 2311 *S/MIME V2 message specification*; 2312 *S/MIME v2 certificate handling*. ftp://ftp.rfc-editor.org/in-notes/rfc2311.txt; ftp://ftp.rfc-editor.org/in-notes/rfc2312.txt
- POP3. RFC:1939,2249
- IMAP4. RFC 2060
- SMTP/SSL. RFC2487 *SMTP Service Extension for Secure SMTP over TLS*

Protocolos de transferencia de hipertexto

CONSIDERACIONES:

Los protocolos de transferencia de hipertexto, en particular http v1.1, permiten publicar y compartir contenidos de una manera sencilla, posibilitando que los usuarios dispongan de un sistema genérico de acceso a los mismos.

CRITERIOS:

2.12 Los servidores Web deben soportar http 1.1.

2.13 La comunicación entre navegadores y servidores Web debe usar http 1.0. o http 1.1.

NORMAS APLICABLES:

Protocolo HTTP 1.1

- RFC 2616 - HTTP es un protocolo de del nivel de aplicación del tipo petición /respuesta, orientado a objetos y que puede utilizarse para múltiples tareas. Una característica de HTTP es que puede definir y negociar los tipos de datos permitiendo la independencia de los sistemas en relación con los tipos de datos.

AMPLIACIÓN TÉCNICA:

- ftp://ftp.isi.edu/in-notes/rfc2616.txt

Servicios de noticias

CONSIDERACIONES:

Se trata de un sistema para facilitar el trabajo de equipos de proyectos, y como herramienta para la difusión del conocimiento.

CRITERIOS:

2.14 Emplear sistemas de noticias que utilicen el protocolo NNTP.

NORMAS APLICABLES:

Protocolos NNTP

- RFC 977 - especifica el protocolo para la distribución, petición, recuperación y publicación de artículos relacionados con el servicio de noticias.

AMPLIACIÓN TÉCNICA:

- ftp://ftp.isi.edu/in-notes/rfc977.txt

Presentación e intercambio de datos

CONSIDERACIONES:

Dada la importancia de garantizar el acceso a los servicios desde cualquier tipo de dispositivo o plataforma y de simplificar el desarrollo y explotación de los sistemas hay que revisar las normas de las interfaces.

RECOMENDACIONES:

- Para formatos de ficheros e intercambio de datos véase en los *Criterios de Conservación* el capítulo "*Formato de la información en soporte electrónico*".
- Otras recomendaciones son las siguientes:
  - Emplear la especificación de SMS para mensajes cortos a teléfonos móviles.
  - Emplear la especificación de WAP 2.0 para los servicios dirigidos a teléfonos móviles.

- Emplear la especificación de XSL v1.0 para la conversión y muestra de documentos XML en HTML.
- Emplear la especificación MIME para indicar el formato de un fichero o la parte de un fichero, en servicios Web y de correo.
- Emplear bases de datos relacionales compatibles con SQL ANSI X3.135-1992/ISO 9075-1992.

AMPLIACIÓN TÉCNICA:

- www.wapforum.org.
- www.w3.org.
- www.unicode.org.

Integración de datos y aplicaciones

CONSIDERACIONES:

La utilización de formatos XML (*Extensible Mark-up Language*) para el intercambio de información se está demostrando como la más efectiva y está siendo aceptada por todo el mercado.

Asimismo, la utilización de formatos EDIFACT se encuentra extendida en ciertos ámbitos de la Administración.

CRITERIOS:

2.15 Se debe emplear XML (*Extensible Mark-up Language*) y protocolos asociados para interoperabilidad e integración de datos:
- XSL (*Extensible Stylesheet Language*).
- XSD (*Extensible Mark-up Language Schema Definition*).

RECOMENDACIONES:

- La utilización de EDIFACT ha de quedar limitada a aquellos ámbitos donde tradicionalmente venga utilizándose y mientras no se aborden proyectos de migración a XML.
- La utilización de SOAP v1.2 (de W3C) como modelo de aplicaciones distribuidas.
- La utilización de Java 2 Enterprise Edition para el desarrollo e integración de aplicaciones. Igualmente se recomienda el uso de JavaBeans v2.0, JDBC v2.0, JST 2.3, JSP 1.2, JMS 1.0,JTA 1.0, Javamail 1.2, JAXP 1.1, J2EE Connector API 1.0, JAAS 1.0.
- La utilización de CORBA para la creación, distribución y gestión de programas distribuidos.

NORMAS APLICABLES:

Electronic data interchange for administration, commerce and transport (EDIFACT)

- ISO 9735:1998 (Estándar internacional). La norma ISO 9735 (UNE 1145) define las reglas de sintaxis del nivel de aplicación para la estructuración normalizada de los mensajes.

eXtensible Mark-up Languaje (XML)

- Estándar de facto editado por W3C. XML es un lenguaje derivado del *SGML (Standard Generalised Mark-up Language*) que se utiliza para crear formatos de datos estructurados.

AMPLIACIÓN TÉCNICA:

- EDIFACT: http://www.iso.ch/cate/cat.html
- XML: http://www.w3c.org/xml
- J2EE: http://java.sun.com/j2ee
- CORBA: http://www.omg.org

3 Metadatos

Sistema de información común de registros de entrada y salida

CONSIDERACIONES:

En el marco de la especificación SICRES, Sistema de Información Común de Registros de Entrada y Salida, funciona como una aplicación cerrada orientada a satisfacer la exigencia de informatización de los Registros, de acuerdo con la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Además los ficheros de intercambio SICRES pueden enviarse mediante tres formatos: fichero plano, formato EDIFACT y formato XML, los tres desarrollados en el proyecto 'Ventanilla Única' para que los ficheros de asientos registrales puedan ser intercambiado entre las entidades de registro de todas las Administraciones Públicas.

CRITERIOS:

3.1 Se deben aplicar las especificaciones de SICRES v2 y los correspondientes formatos de intercambio de ficheros de intercambio de asientos registrales.

NORMAS APLICABLES:

- Las especificaciones de SICRES y los correspondientes formatos de intercambio de ficheros de intercambio de asientos registrales.

AMPLIACIÓN TÉCNICA:

- ATRIO, Almacenamiento, Tratamiento y Recuperación de Información de Oficinas. http://www.csi.map.es/csi/pg5a10.htm
- SICRES http://www.csi.map.es/csi/pg5s40.htm
- ESTROFA, Especificaciones para el Tratamiento de Flujos Administrativos Automatizados. http://www.csi.map.es/csi/pg5e30.htm
- EDIFACT: http://www.csi.map.es/csi/pdf/nr011_sicres2_guia_edifact.pdf
- XML: http://www.csi.map.es/csi/pdf/nr012_sicres2_guia_xml11.pdf

4 Desarrollo de sistemas de información

Metodología de planificación, desarrollo y mantenimiento de sistemas de información

CONSIDERACIONES:

La metodología MÉTRICA Versión 3 ofrece un instrumento útil para la sistematización de las actividades que dan soporte al ciclo de vida del software. MÉTRICA v3 contempla el desarrollo de Sistemas de Información para las distintas tecnologías que actualmente están conviviendo y los aspectos de gestión que aseguran que un proyecto cumple sus objetivos en términos de calidad, coste y plazos.

CRITERIOS:

4.1 Se debe aplicar MÉTRICA versión 3.

4.2 Los programas y aplicaciones puestos por la Administración a disposición del ciudadano para fines de servicios de aquella deben poder funcionar sobre diversas plataformas, alternativas. (Véase capítulo '*Software libre y de fuentes abiertas*')

NORMAS APLICABLES:

- MÉTRICA versión 3 http://www.csi.map.es/csi/metrica3/index.html

5 Requisitos de diseño de páginas web y de accesibilidad para personas con discapacidad

CONSIDERACIONES:

Un sitio web accesible es aquél que puede ser utilizado correctamente por el mayor número posible de usuarios, incluyendo a personas con diferentes tipos de discapacidades.

Según las **Pautas de la Iniciativa de Accesibilidad a la Web (WAI)**, para cuya realización se ha contado con respaldo financiero de la Comisión Europea a través del Programa de Aplicaciones Telemáticas del IV Programa Marco, así como de varios gobiernos y otras organizaciones, para ser accesible, el sitio debe albergar un contenido fácilmente comprensible y navegable, presentado de manera clara, con lenguaje claro y simple y con mecanismos obvios de navegación para moverse entre las páginas sin pérdida de contenido y funcionalidad, en diversos navegadores, aunque éstos no soporten o tengan desactivada la visualización de imágenes, y la información que suministran ha de poder ser captada por los usuarios con independencia del equipo físico que utilicen, de los programas que estén usando y de sus posibles deficiencias físicas, sensoriales y cognitivas.

Con antelación al año 2003, el Año Europeo de los discapacitados, se publicó la *Comunicación de la Comisión COM(2001)529 final eEurope 2002: accesibilidad de los sitios web públicos y de su contenido* que persigue facilitar la adopción y aplicación de las citadas pautas, e incluye en anexos una guía rápida para las mismas.

Además, la política europea de fomento de la accesibilidad de la información en los sitios públicos de la *web* se orienta a que las "*páginas web del sector público y su contenido, en los estados miembros y las instituciones europeas deben diseñarse de manera que sean accesibles*" (Plan de Acción eEurope, 2c); acción que debe realizarse por las instituciones europeas y los 15 Estados miembros gracias a la adopción de las citadas Pautas de la Iniciativa de Accesibilidad a la Web (WAI).

Por otra parte, los requisitos para el acceso de las personas con discapacidad a las plataformas informáticas están basados en las normas de AENOR UNE 139801 EX para soportes físicos y UNE 139802 EX para soportes lógicos.

Los requisitos incluidos en estas normas están relacionados con las características de las siguientes minusvalías tipificadas:

- Personas con limitaciones motrices.
- Personas con limitaciones psíquicas.
- Personas con limitaciones auditivas de leves a severas.
- Personas con limitaciones visuales.
- Personas con ceguera o sordo-ciegas.

Existen además una serie de dispositivos tales como ayudas técnicas, aplicaciones y soportes físicos adaptados y distintas herramientas de acceso diseñadas para facilitar la utilización de los soportes y aplicaciones informáticos a las personas con discapacidad.

Por otra parte, la norma UNE-EN ISO 9999 especifica y clasifica las ayudas existentes para personas con discapacidad.

Para que una persona con limitaciones motrices pueda trabajar sobre las mismas aplicaciones que cualquier otra persona sin discapacidad se requiere la inclusión de programas emuladores para los siguientes dispositivos de entrada:

- Teclado: Para los usuarios que pueden utilizar únicamente el teclado, se requiere un emulador de ratón por teclado.
- Ratón: Para los usuarios que únicamente pueden utilizar el ratón, se requiere un programa emulador de teclado controlado por ratón.
- Pulsador: Para los usuarios que únicamente pueden utilizar pulsadores, se requiere un programa emulador de teclado y otro de ratón.

En al Anexo 1 se incluyen varios apartados con un resumen orientativo de requisitos extraídos de las normas UNE anteriormente citadas.

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- La Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico, ha establecido en su disposición adicional quinta que las Administraciones Públicas deberán adoptar las medidas necesarias para que la información disponible en sus respectivas páginas de Internet pueda ser accesible a personas con discapacidad y de edad

avanzada de acuerdo con los criterios de accesibilidad al contenido generalmente reconocidos antes del 31 de diciembre de 2005. Asimismo, podrán exigir que las páginas de Internet cuyo diseño o mantenimiento financien apliquen los criterios de accesibilidad antes mencionados. Igualmente, se promoverá la adopción de normas de accesibilidad por los prestadores de servicios y los fabricantes de equipos y software, para facilitar el acceso de las personas con discapacidad o de edad avanzada a los contenidos digitales.

- La *Orden PRE/1551/2003, de 10 junio, por la que se desarrolla la disposición final primera del Real Decreto 209/2003, de 21de febrero de 2003, que regula los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de certificados por los ciudadanos,* establece que el registro telemático y el servicio de notificación telemática deberán cumplir los requerimientos en materia de accesibilidad establecidos por la Iniciativa para una Web Accesible (WAI) del Consorcio World Wide Web y en particular las especificaciones de la Recomendación de 5 de mayo de 1999 sobre Pautas de Accesibilidad del Contenido en la Web, versión 1.0, en su nivel AA.

CRITERIOS:

5.1 Se deben tener en cuenta los requisitos de accesibilidad, en general, y para personas con discapacidad y mayores, en particular, en el desarrollo e implantación de los sistemas de información y especialmente de las interfaces, de acuerdo con las normas aplicables.

5.2 Los servicios electrónicos puestos por la Administración a disposición del ciudadano deben ser visualizables, accesibles y funcionalmente operables desde diversos navegadores alternativos. En particular, se deben adaptar las aplicaciones *web* a los estándares del *World Wide Web Consortium* (W3C), evitar la utilización de extensiones propietarias de navegadores y verificar el sitio web, al menos, con http://validator.w3.org. (Véase capítulo '*Software libre y de fuentes abiertas*')

5.3 Se deben incluir en los pliegos de prescripciones técnicas cláusulas sobre accesibilidad a sitios web en términos tales como los siguientes:

- "*El sitio web debe cumplir los requerimientos en materia de accesibilidad establecidos por el W3C a través de la WAI (Iniciativa para una Web Accesible, del Consorcio World Wide Web) y , en concreto, las especificaciones de la Recomendación de 5 de mayo de 1999 sobre Pautas de Accesibilidad del Contenido en la Web, versión 1.0, en su nivel AA.*"

5.4 Los servidores *web* deben soportar al menos HTML v3.2 y debe verificarse que sus contenidos son accesibles desde cualquier navegador o cliente ligero.

5.5 En la creación de sitios Web se deberá cumplir, al menos, el siguiente decálogo:

- **Imágenes y animaciones**. Usar el atributo **alt** para describir la función de cada elemento visual.
- **Mapas de imagen**. Usar el elemento **map** de tipo cliente y texto para las zonas activas.
- **Multimedia**. Proporcionar subtítulos y transcripción del sonido, y descripción del vídeo.
- **Enlaces hipertextuales**. Usar texto que tenga sentido leído fuera de contexto. Por ejemplo, evitar "pincha aquí".

- **Organización de las páginas**. Usar encabezados, listas y estructura consistente. Usar **CSS** para la maquetación donde sea posible.
- **Gráficos y esquemas**. Resumir o usar el atributo **longdesc.**
- **Scripts, applets y plug-ins**. Ofrezca contenido alternativo si las funciones nuevas no son accesibles.
- **Marcos (Frames)**. Usar el elemento **noframes** y títulos con sentido.
- **Tablas.** Disponer que puedan leerse línea a línea. Resumir.
- **Revise su trabajo**. Verificar. Usar las herramientas, lista de comprobación y pautas de **www.w3.org/TR/WCAG.**

NORMAS APLICABLES:

- AENOR UNE 139801 EX para soportes físicos.
- UNE 139802 para soportes lógicos.
- UNE-EN ISO 9999.
- *Web Content Accesibility Guidelines 1.0 ; W3C Recommendation of 5-May-1999* http://www.w3.org/TR/WAI-WEBCONTENT
- Recomendación de 5 de mayo de 1999 sobre Pautas de Accesibilidad del Contenido en la Web, versión 1.0 (traducción española no oficial, elaborada por Carlos Egea y Alicia Sarabia http://usuarios.discapnet.es/disweb2000/PautaWAI/WCAG10.htm.
- *Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico.* Disposición Adicional Quinta.

AMPLIACIÓN TÉCNICA:

- Sitio web sobre la discapacidad en España http://www.discapnet.es
- Comité Español De Representantes De Minusválidos (CERMI) http://www.cermi.es/
- Sidar, Seminario de Iniciativas sobre Discapacidad y Accesibilidad en la Red (España) http://www.sidar.org
- Página de accesibilidad a la red de la Unidad "Acceso" de la Universidad de Valencia http://acceso.uv.es/accesibilidad/
- Traducciones de documentos sobre accesibilidad en la web del WAI, realizadas por Carlos Egea y Alicia Sarabia: http://usuarios.discapnet.es/disweb2000/webaccesible/index.htm
- *Web Accessibility Initiative* http://www.w3.org/wai
- AWARE (*Accessible Web Authoring Resources and Education*). Materiales originales en inglés sobre accesibilidad en la web: http://aware.hwg.org/
- Useit.com, sitio web de Jakob Nielsen sobre usabilidad http://www.useit.com
- Programa de validación de la accesibilidad Bobby http://www.cast.org/bobby/
- Herramienta TAW (*Test Accesibility Web*) disponible en http://www.tawdis.net/

6 Software libre y de fuentes abiertas

CONSIDERACIONES:

Se denomina *software libre* aquél software, todo software, producto o desarrollo a medida, que se distribuye bajo una licencia, según la cual el autor (cedente de la licencia) cede una serie de libertades básicas al usuario (licenciatario) en el marco de un acuerdo de concesión (licencia):

- La libertad de ejecución; es decir, de utilizar el programa con cualquier fin en cuantos ordenadores se desee.
- La libertad de conocer y estudiar cómo funciona el programa.
- La libertad de modificar o mejorar el programa.
- La libertad de redistribuir copias a otros usuarios.

La licencia es un contrato entre el desarrollador o proveedor de un software sometido a propiedad intelectual y derechos de autor y el usuario, el cual contiene un conjunto de cláusulas esencialmente orientadas a reconocer derechos, a denegar derechos y a limitar responsabilidades del desarrollador o proveedor del software en cuestión. Es el desarrollador, el proveedor, o quien detente los derechos de explotación, quien elige la licencia según la cual distribuye el software.

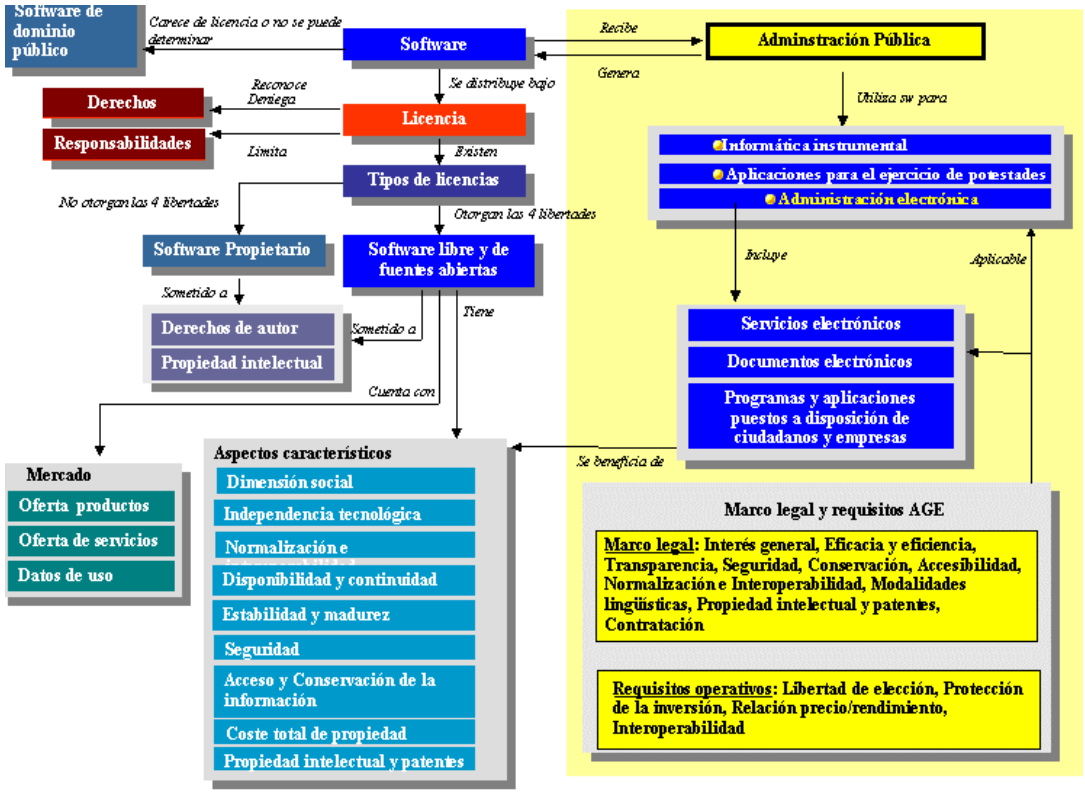
El fenómeno del software libre y de fuentes abiertas constituye una revolución en el ámbito de las tecnologías de la información sin parangón desde que se produjeron los primeros momentos de expansión de Internet o, tal vez, desde la introducción de las políticas de sistemas abiertos. El debate en términos de 'software libre sí o no', se encuentra a estas alturas superado por una realidad *de facto* que tiene un alcance estratégico y unas dimensiones que no pueden ni obviarse ni ignorarse; es un hecho su presencia creciente en organizaciones del sector público y del sector privado.

En la Unión Europea, y fuera de ella, las administraciones vienen desarrollando actividades para configurar políticas y decisiones operativas en relación con el software libre y de fuentes abiertas. En el marco de la Unión Europea, diversos actos y documentos como el Plan de Acción eEurope 2005, la Comunicación de la Comisión Europea sobre "*El papel de la Administración electrónica para el futuro de Europa*", el Programa IDA y el VI Programa Marco de I+DT, recogen el papel del software libre en el desarrollo de la Administración electrónica, contemplando la promoción de su uso y ligándolo estrechamente a la extensión de los denominados estándares abiertos y al logro de la interoperabilidad.

Para la Administración, ente generador y receptor de software, el ejercicio de las libertades de ejecución, conocimiento, modificación y redistribución tiene consecuencias de alcance en las aplicaciones utilizadas para el ejercicio de potestades, que afectan a cuestiones tales como la defensa del interés general, la transparencia, la eficacia, la independencia tecnológica, la seguridad, el control sobre los propios programas y aplicaciones, el acceso y conservación de la información en soporte electrónico y, en concreto, a cuatro requisitos operativos perseguidos por la Administración a lo largo de sucesivas oleadas tecnológicas, ya planteados en su día en la política de sistemas abiertos, y que pueden ser aplicados asimismo en relación con el software libre y de fuentes abiertas:

- Libertad de elección, del equipo físico, los programas o los servicios. El síndrome de *cliente cautivo* con frecuencia conduce a que actualizaciones y migraciones en entornos *propietarios* se hagan en unas condiciones de negociación muy desfavorables para la Administración.
- Protección de la inversión, en equipo físico, en programas, en formación de técnicos y usuarios, frente a la discontinuidad de los productos, bien por políticas comerciales o bien por desaparición del mercado del suministrador.
- Mejor relación precio/rendimiento. En el caso del software libre y de fuentes abiertas, los precios no se determinan en régimen de monopolio de oferta, pues favorece la competencia.
- Garantía de comunicación e interoperabilidad de los sistemas, especialmente si se tiene en cuenta la necesidad de la Administración de ofrecer el servicio público a los ciudadanos.

En particular, en relación con el desarrollo de la Administración electrónica, la extensión del uso del software libre y de fuentes abiertas impacta en tres cuestiones capitales: al acceso por ciudadanos y empresas a los servicios electrónicos de la Administración, a los documentos puestos por la Administración en soporte electrónico y a los programas y aplicaciones puestos por la Administración a disposición para sus fines y servicios. Este impacto se debe a aspectos tales como la dimensión social del software libre y de fuentes abiertas, la interoperabilidad y la normalización, la confianza y la seguridad, el acceso y conservación de los documentos en soporte electrónico, la protección de las modalidades lingüísticas, la estabilidad, calidad y madurez del software, el coste total de propiedad y la propiedad intelectual y las patentes, según la visión panorámica que se muestra a continuación:



Se ha adoptado la voz '*software libre y de fuentes abiertas'* entendiendo que las expresiones a ambos lados de la conjunción se refieren esencialmente al mismo ente, es decir, al software que se distribuye con las libertades de ejecución, conocimiento, modificación y redistribución. Se añade la voz '*de fuentes abiertas*' porque ha sido la expresión escogida por la Comisión Europea debido a las ambigüedades que en la traducción literal al inglés de 'software libre' introduce la voz inglesa 'free', que se puede interpretar a la vez como 'libre' y como 'gratuito'. El *software libre* presenta la ventaja de la independencia frente a vicisitudes y arbitrariedades en cuanto a las estrategias comerciales y a la continuidad de diversas herramientas y formatos que se utilicen para el tratamiento de la información en soporte electrónico.

No es la gratuidad la cualidad sobre la que inciden los principales logros de los productos de libre disposición o de fuente abierta, sino que su atractivo radica en el hecho de poder disponer del código fuente, tener la posibilidad de modificarlo y adaptarlo a unas necesidades concretas, o ampliar sus funcionalidades, y poner a disposición de otros las aportaciones propias, con la esperanza de beneficiarse de las contribuciones de todos. Por otra parte, el esfuerzo continuo de revisión, junto con la seguridad aportada por las repetidas adaptaciones y pruebas a las que se someten las aplicaciones, es lo que aporta calidad a estos productos.

La Unión Europea ha reconocido el papel y la importancia de este tipo de *software* tanto en los documentos e iniciativas estratégicas como en actuaciones de carácter concreto:

- Línea estratégica "Administración en línea" de la iniciativa de la Comisión Europea eEurope aprobada en 2000: "*Fomento de la utilización de programas fuentes abiertas en el sector público*".
- "Comunicación de la Comisión, Seguridad de las redes y de la información: propuesta para un enfoque político europeo" (6 de junio de 2001). Expone que los programas de fuente abierta se consideran clave para facilitar la interoperabilidad y, en particular, para reforzar la confianza en los productos de cifrado.
- Plan de Acción de *eEurope* 2005: Una Sociedad de la Información para todos. Aprobado en el Consejo Europeo de Sevilla, el uso de programas de fuentes abiertas se configura clave para la interoperabilidad y la normalización, entre otros en la línea de acción "Administración en línea". Programa IDA (Intercambio de Datos entre Administraciones), como principal referente de actuaciones concretas:
  - "Estudio del Programa IDA sobre el uso de los programas de fuentes abiertas en el Sector Público"
  - "Estudio del Programa IDA sobre la posibilidad de compartir programas de fuentes abiertas entre las Administraciones Públicas en Europa"
  - "Directrices IDA de migración a software de fuentes abiertas"
  - "Observatorio IDA de software de fuentes abiertas"
  - Desarrollo de instrumentos bien liberados como programas de fuentes abiertas (*Portal Toolkit*) o bien que funcionan en una plataforma de *software* de fuentes abiertas (CIRCA).

CRITERIOS:

6.1 Se deben adoptar programas y aplicaciones de fuente abierta en aquellos ámbitos donde pueda haber soluciones de este tipo que satisfagan las necesidades y requisitos de la aplicación o información a conservar. En particular, se debe tener en cuenta para aprovisionarse, bien de productos o bien de desarrollos de software a medida, la oferta global de software disponible distribuido según diversos tipos de licencias y aplicar los criterios de racionalidad técnica y económica, evaluando, por tanto, todas las posibles alternativas en el marco de las obligaciones e intereses legítimos de la Administración, con independencia de cuáles sean los procedimientos de adquisición aplicables en cada caso.

RECOMENDACIONES:

- Difundir información sobre la posibilidad de utilizar programas y aplicaciones de fuente abierta.
- Exigir la disponibilidad del código fuente para favorecer la continuidad y longevidad de los sistemas.
- Impulsar la compatibilidad e interoperabilidad de las aplicaciones utilizadas para el ejercicio de potestades, utilizando la disponibilidad del código fuente de programas y aplicaciones.

NIVELES DE SEGURIDAD:

- En función de los tipos de datos personales de los ciudadanos, tratados por sistemas y aplicaciones, le es aplicable del RD 994/1999 los artículos relativos a la adopción de medidas de seguridad de nivel básico, medio o alto.
- Cabe establecer los niveles de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en *'Criterios de seguridad'* el capítulo '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

Comisión Europea, DG Empresa. "Estudio sobre el uso del software de fuentes abiertas en el Sector Público, Programa IDA." http://www.csi.map.es/csi/pg5s42.htm

- **Comisión Europea, DG Empresa.** "Estudio del Programa IDA sobre la posibilidad de compartir programas de fuentes abiertas entre las Administraciones Públicas en Europa", (http://europa.eu.int/idabc/en/document/2623 - feasibility)
- **Comisión Europea, DG Empresa.** "Directrices IDA de migración a software de fuentes abiertas." <http://www.csi.map.es/csi/pg5s43.htm>
- **Comisión Europea, DG Empresa.** *The IDA Observatory of Open Source Software.* <http://europa.eu.int/ida/en/chapter/452>
- **Bundesministerium des Innern, Kbst.** *A guide to migrating the basic software components on server and workstation computers, July 2003.* <http://www.kbst.bund.de/>
- **World Wide Web Consortium (W3C).** *W3C Patent Policy. W3C Open Source Software.* <http://www.w3.org>
- **Ministerio de Administraciones Públicas**. *Estrategia de sistemas abiertos.* <http://www.csi.map.es/csi/pg6050.htm>

- **Ministerio de Ciencia y Tecnología.** *Plan Nacional de Investigación Científica, Desarrollo e Innovación Tecnológica 2004-2007; Volumen II.*
- Directiva 91/250/CEE del Consejo de las Comunidades Europeas, de 14 de mayo de 1991, sobre la protección jurídica de programas de odenador.
- 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.csi.map.es/csi/com2001_0298es01.pdf

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico y del Procedimiento Administrativo Común, en su preámbulo, apartado V, se refiere a "garantizar la calidad y transparencia de la actuación administrativa" y a la "tecnificación y modernización de la actuación administrativa en su vertiente de producción jurídica y a la adaptación permanente al ritmo de las innovaciones tecnológicas".
- La citada Ley 30/1992 en su artículo 3 'Principios Generales', se refiere a la "actuación por los criterios de eficacia y servicio a los ciudadanos".
- Cuando sea compatible con los medios técnicos de que dispongan las Administraciones Públicas, los ciudadanos podrán relacionarse con ellas para ejercer sus derechos a través de técnicas y medios electrónicos, informáticos o telemáticos. (Ley 30/1992, art. 45.2)
- Los ciudadanos tienen derecho a acceder a los registros y a los documentos que obren en los archivos administrativos, cualquiera que sea la forma de expresión gráfica, sonora o en imagen o en el tipo de soporte material en que figuren, en las condiciones en las condiciones que se establecen (expedientes terminados, interés legítimo y directo, otras específicas) (Ley 30/1992, art. 45.2)
- Adoptar medidas técnicas y organizativas teniendo en cuenta el estado de la tecnología. (RD 263/1996, art. 4.2)
- La existencia de compatibilidad entre el emisor y el destinatario que permita técnicamente las comunicaciones entre ambos. (RD 263/1996, art. 7.1.c)
- En los supuestos de comunicaciones y notificaciones dirigidas a particulares se considerará el soporte, el medio o aplicación como preferente que estos hayan señalado para sus comunicaciones con la Administración General del Estado. (RD 263/1996, art. 7.2.c)

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

- Adoptar medidas técnicas y organizativas habida cuenta del estado de la tecnología. (LO 15/1999, art. 9.1)

En relación con la propiedad intelectual y las patentes

- L*a Ley de Propiedad Intelectual (RD Legislativo 1/1996, de 12 de abril)* trata en sus artículos 95 a 104 la cuestión de los derechos de autor y los programas de ordenador.
- Según la *Ley 11/1986 de 20 de marzo por la que se aprueba la Ley de Patentes y Modelos de Utilidad* los programas de ordenador no se consideran invenciones y no están sujetos a patentabilidad.

En relación con la protección de las modalidades lingüísticas

- La Constitución recoge la protección y garantía de las *distintas modalidades lingüísticas de España* (artículos 3 y 46) y el *Real Decreto 564/1993, de 16 de abril,* la presencia de la letra "ñ" y demás caracteres específicos del idioma castellano.

7 Anexo 1: Requisitos de accesibilidad para personas con discapacidad

A1.1 REQUISITOS DE ACCESIBILIDAD PARA LAS PERSONAS CON LIMITACIONES MOTRICES

TIPO DE DISCAPACIDAD		LIMITACIONES MOTRICES
ACCESO A:	SOPORTES FISICOS	ENTORNOS OPERATIVOS
REFERENCIA:	AENOR UNE 139801 EX	(UNIDAD CENTRAL)
EPÍGRAFE	DESCRIPCIÓN	
5.1.1	Los controles de la unidad central deben estar localizados en la parte frontal o superior, en especial el botón de encendido/apagado.	
5.1.2	Las opciones ofrecidas por los controles deben ser configurables por software.	
5.1.7	Se recomienda que las unidades de los soportes de almacenamiento utilicen una plataforma móvil de entrada/salida.	
5.1.8	Se debe facilitar la extracción de los soportes de almacenamiento por botón y no por palanca.	
5.1.9	El botón de expulsión del soporte de almacenamiento extraible (disquete, CD-ROM, etc.) debe exigir una fuerza inferior a 2 newtons.	

TIPO DE DISCAPACIDAD		LIMITACIONES MOTRICES
ACCESO A:	SOPORTES FISICOS	ENTORNOS OPERATIVOS
REFERENCIA:	AENOR UNE 139801 EX	(DISPOSITIVOS PERIFERICOS)
EPÍGRAFE	DESCRIPCIÓN	
5.2.1	Los controles del periférico deben estar localizados en la parte frontal, en especial el botón de encendido/apagado.	
5.2.2	La fuerza requerida para pulsar o manejar los controles debe ser menor de 2 newtons.	
5.2.3	Los controles deben tener realimentación táctil.	
5.2.4	Es recomendable que los controles dispongan de realimentación sonora.	
5.2.5	Los controles de los periféricos se deben diseñar con un tamaño adecuado y suficientemente separados.	
5.2.6	Se deben usar controles cóncavos y no deslizantes (rugosos) en los periféricos.	
5.2.7	Se deben evitar controles en los periféricos que precisen movimientos giratorios o complejos.	
5.2.8	Se deben evitar controles de tipo sensor de tacto. Se recomienda el uso de controles de tipo botón o tecla.	
5.2.9	Las opciones ofrecidas por los controles deben ser configurables por software.	
5.2.13	Donde se precise una acción simultánea (mantener apretado un control, mientras se pulsa otro) se debe proporcionar un método alternativo para lograr el mismo resultado, que no requiera una acción simultánea.	

TIPO DE DISCAPACIDAD		LIMITACIONES MOTRICES
ACCESO A:	SOPORTES FISICOS	ENTORNOS OPERATIVOS (DISPOSITIVOS PERIFERICOS)
REFERENCIA:	AENOR UNE 139801 EX	
EPÍGRAFE	DESCRIPCIÓN	
5.2.14	Los periféricos deben tener bases estables y no deslizantes.	
5.2.15	Si el dispositivo por cuestiones de seguridad necesita una cubierta, ésta debe disponer de un enganche que facilite su apertura.	

TIPO DE DISCAPACIDAD		LIMITACIONES MOTRICES
ACCESO A:	SOPORTES FISICOS	MONITOR, TECLADO, RATON, IMPRESORA Y ESCANER
REFERENCIA:	AENOR UNE 139801 EX	
EPÍGRAFE	DESCRIPCIÓN	
5.3.1	El monitor debe ser independiente de la unidad central.	
5.3.2	Los monitores que dispongan de un mecanismo de orientación no deben ofrecer resistencia en su manipulación.	
5.3.3 6.1.10	Se deben evitar frecuencias de parpadeo y refresco en el rango de 5 Hz a 50 Hz.	
5.4.1	Se debe proporcionar realimentación táctil y sonora de las teclas.	
5.4.2	El teclado debe ser independiente de la unidad central para poder sustituirlo por un emulador de teclado.	
5.5.1	El controlador de ratón debe cumplir los requisitos establecidos en la norma UNE 139802 EX.	
5.6.1	Las impresoras deben tener una bandeja para la salida del papel sin cubierta o con posibilidad de eliminarla.	
5.6.2	La bandeja de alimentación de papel debe permitir colocar el papel sin necesidad de extraer todo el cargador o levantar cubiertas adicionales.	

TIPO DE DISCAPACIDAD		LIMITACIONES MOTRICES
ACCESO A:	SOPORTES LÓGICOS	REQUISITOS GENERALES ENTORNOS OPERATIVOS
REFERENCIA:	AENOR UNE 139802 EX	
EPÍGRAFES	DESCRIPCIÓN	
5.1.1	Para los usuarios que pueden utilizar únicamente el teclado, se requiere un emulador de ratón por teclado. Para los usuarios que únicamente pueden utilizar el ratón, se requiere un programa emulador de teclado controlado por ratón. Para los usuarios que únicamente pueden utilizar pulsadores, se requiere un programa emulador de teclado y otro de ratón.	
5.1.2	Se recomienda la incorporación de un sistema de reconocimiento de voz que permita controlar completamente el entorno operativo.	
5.1.5	Las herramientas de acceso que ofrece el entorno operativo deben tener carácter opcional en su activación/desactivación, sin necesidad de reinicializar el entorno.	

5.1.6	Los servicios proporcionados por el entorno operativo deben permitir el cumplimiento de las normas relativas a las aplicaciones que los utilicen.
5.1.16	Se deben evitar frecuencias de parpadeo en el rango de 5 Hz a 50 Hz.
5.1.17	El entorno operativo debe posibilitar a través de alguna opción la expulsión automática de un disquete, CD-ROM o cualquier otro dispositivo de almacenamiento de información extraíble.
5.1.24	Debe existir la posibilidad de cambiar de un área de trabajo a otra.

TIPO DE DISCAPACIDAD		LIMITACIONES MOTRICES
ACCESO A:	SOPORTES LÓGICOS	ENTORNOS OPERATIVOS Y APLICACIONES INFORMATICAS
REFERENCIA:	AENOR UNE 139802 EX	
EPÍGRAFES	DESCRIPCIÓN	
5.1.10 6.1.5	La visualización de la información en la pantalla no debe estar sujeta a requisitos temporales.	
5.1.11 6.1.6	Los mensajes críticos deben ser validados por el usuario antes de desaparecer o tramitarse.	
5.1.18 6.1.11	Todas las funciones que se pueden realizar en el entorno operativo/aplicación deben ser accesibles por teclado.	
5.1.19 6.1.12	Las combinaciones o secuencias de teclas que sirvan para acceder a las diferentes funciones del entorno operativo/aplicación, deberán estar completamente documentadas.	
5.1.20 6.1.13	Donde se precise una acción simultánea (mantener apretada una tecla mientras se pulsa otra) se debe proporcionar un método alternativo para lograr el mismo resultado.	
5.1.21 6.1.14	Todos los menús deben ser accesibles desde el teclado.	
5.1.22 6.1.16	Los menús del entorno operativo deben ser circulares, es decir, estar hechos de tal forma que al alcanzar el último elemento se pase al primero y viceversa.	
5.1.25 6.1.19	Se debe permitir la modificación de tamaño y lugar de los iconos u otros objetos visualizados.	

TIPO DE DISCAPACIDAD		LIMITACIONES MOTRICES
ACCESO A:	SOPORTES LÓGICOS	ENTORNOS OPERATIVOS Y APLICACIONES INFORMATICAS CON VENTANAS
REFERENCIA:	AENOR UNE 139802 EX	
EPÍGRAFE	DESCRIPCIÓN	
5.2.1 6.2.1	Todas las opciones incluidas en una ventana deben ser accesibles por teclado.	
5.2.2 6.2.2	Las ventanas deben posibilitar el ajuste de su tamaño y localización en pantalla.	
5.2.3 6.2.3	Deben existir las opciones de minimizar y maximizar una ventana.	
5.2.5 6.2.5	Debe existir la posibilidad de cambiar de una ventana a otra.	
5.2.4	Debe existir la función de cerrar una ventana.	

TIPO DE DISCAPACIDAD		LIMITACIONES MOTRICES
ACCESO A:	SOPORTES LÓGICOS	ENTORNOS OPERATIVOS Y APLICACIONES INFORMATICAS CON VENTANAS
REFERENCIA:	AENOR UNE 139802 EX	
EPÍGRAFE	DESCRIPCIÓN	
6.2.4	La secuencia de cambio por teclado de un elemento a otro dentro de una caja de diálogo debe ser coherente con su disposición en pantalla.	

TIPO DE DISCAPACIDAD		LIMITACIONES MOTRICES
ACCESO A:	SOPORTES LÓGICOS	ENTORNOS OPERATIVOS (CONTROL DE TECLADO Y RATÓN)
REFERENCIA:	AENOR UNE 139802 EX	
EPÍGRAFE	DESCRIPCIÓN	
5.3.1	Debe incluir una opción que permita bloquear las teclas de control.	
5.3.3	Debe incluir una opción que permita eliminar o retrasar el efecto repetición en la pulsación de una tecla.	
5.3.4	Debe incluir una opción que permita programar el tiempo de aceptación de una tecla.	
5.3.5	Debe incluir una opción que permita programar el tiempo de rechazo de pulsación de una misma tecla.	
5.3.6	Debe incluir una opción que permita redefinir la localización de las teclas.	
5.4.1	Debe incluir una opción que permita modificar la orientación en el movimiento del ratón.	
5.4.2	Debe incluir una opción que permita modificar la velocidad del movimiento del puntero.	
5.4.3	Debe incluir una opción que permita disponer de alternativas de aceleración en la velocidad de movimiento del puntero.	
5.4.4	Debe incluir una opción que permita programar el tiempo de aceptación del clic.	
5.4.5	Debe incluir una opción que permita programar el tiempo entre el primer clic y el siguiente para conseguir la función de doble clic.	
5.4.6	Debe incluir una opción que permita poder realizar el bloqueo de clic para el arrastre disponiendo de un botón del ratón para esta función.	
5.4.7	Debe incluir una opción que permita poder alternar la función del clic del botón derecho e izquierdo.	

TIPO DE DISCAPACIDAD		LIMITACIONES MOTRICES
ACCESO A:	SOPORTES LÓGICOS	REQUISITOS GENERALES APLICACIONES INFORMATICAS
REFERENCIA:	AENOR UNE 139802 EX	
EPÍGRAFES	DESCRIPCIÓN	
6.1.15	La aplicación debe respetar las convenciones de acceso por teclado del entorno operativo.	
6.1.17	Se debe diseñar la aplicación minimizando los pasos necesarios para activar cualquier opción.	

TIPO DE DISCAPACIDAD		LIMITACIONES MOTRICES
ACCESO A:	SOPORTES LÓGICOS	REQUISITOS GENERALES APLICACIONES INFORMATICAS
REFERENCIA:	AENOR UNE 139802 EX	
EPÍGRAFES	DESCRIPCIÓN	
6.1.25	En entornos que no son de ventanas, se debe permitir la superposición en pantalla de la interfaz de otras aplicaciones.	
6.1.26	La aplicación no debe anular la ejecución de las herramientas de acceso cargadas previamente.	
6.1.27	La aplicación debe usar los servicios del entorno operativo.	

TIPO DE DISCAPACIDAD		LIMITACIONES MOTRICES
ACCESO A:	SOPORTES LÓGICOS	NAVEGADORES Y PAGINAS HTML
REFERENCIA:	AENOR UNE 139802 EX	
EPÍGRAFES	DESCRIPCIÓN	
7.1.1	Las características de accesibilidad de los navegadores deberán cumplir los mismos requisitos que cualquier otro programa de usuario.	
7.1.2	Los navegadores de Internet deberán permitir el desplazamiento dentro de las páginas HTML utilizando sólo el ratón y sólo el teclado.	
7.1.3	El navegador debe posibilitar el paso de un enlace a otro, tanto por ratón como por teclado.	
7.1.4	Los navegadores deben facilitar la posibilidad de pasar de un marco (*frame*) a otro, tanto por ratón como por teclado.	
7.2.1	Las características de accesibilidad de las páginas Web, incluyendo HTML, CGIs, Java, etc. deberán cumplir los mismos requisitos que cualquier otro programa de usuario.	

TIPO DE DISCAPACIDAD		LIMITACIONES MOTRICES
ACCESO A:	DOCUMENTACION	
REFERENCIAS:	AENOR UNE 139801 EX / AENOR UNE 139802 EX	
EPÍGRAFE	DESCRIPCIÓN	
6.1 / 8.1	La documentación debe entregarse en formato electrónico.	
6.2 / 8.2	La encuadernación debe permitir abrir la documentación por cualquier página y no precisar sujeción para mantenerla abierta.	
6.3 / 8.3	El papel utilizado en la documentación no debe ser deslizante.	

A1.2 REQUISITOS DE ACCESIBILIDAD PARA LAS PERSONAS CON LIMITACIONES PSÍQUICAS

TIPO DE DISCAPACIDAD		LIMITACIONES PSIQUICAS
ACCESO A:	SOPORTES FISICOS	ENTORNOS OPERATIVOS UNIDAD CENTRAL, TECLADO
REFERENCIA:	AENOR UNE 139801 EX	
EPÍGRAFE	DESCRIPCIÓN	
5.1.3	Se recomienda que los interruptores y los mandos se etiqueten con símbolos fáciles de comprender.	
5.4.3	Se recomienda que cada grupo funcional de teclas tenga un color distinto.	

TIPO DE DISCAPACIDAD		LIMITACIONES PSIQUICAS
ACCESO A:	SOPORTES LÓGICOS	ENTORNOS OPERATIVOS Y APLICACIONES INFORMATICAS
REFERENCIA:	AENOR UNE 139802 EX	REQ. GENERALES CONTROL TECLADO
EPÍGRAFE	DESCRIPCIÓN	
5.1.4 6.1.3	La salida por voz debe producirse inmediatamente después de que ocurra el evento que la genera.	
5.1.5	Las herramientas de acceso que ofrece el entorno operativo deben tener carácter opcional en su activación/desactivación, sin necesidad de reinicializar el entorno.	
5.1.7	La estructura de datos que define un elemento de la interfaz de usuario en el entorno operativo debe disponer de una identificación de dicho elemento y de servicios para su consulta.	
5.1.8 6.1.2	Se recomienda utilizar mensajes cortos y sencillos.	
5.1.9 6.1.4	El mismo tipo de mensaje debe tomar siempre el mismo formato de visualización.	
5.1.10 6.1.5	La visualización de la información en la pantalla no debe estar sujeta a requisitos temporales.	
5.1.11 6.1.6	Los mensajes críticos deben ser validados por el usuario antes de desaparecer o tramitarse.	
5.1.19 6.1.12	Las combinaciones o secuencias de teclas que sirvan para acceder a las diferentes funciones del entorno operativo, deberán estar completamente documentadas.	
5.1.25 6.1.19	Se debe permitir la modificación de tamaño y lugar de los iconos u otros objetos visualizados.	
5.1.26 6.1.20	Todos los iconos deben tener asociada una etiqueta de texto y se debe facilitar una opción que permita ver sólo esa etiqueta.	
5.3.2	Debe incluir una opción que permita visualizar y escuchar el estado de las teclas de	

TIPO DE DISCAPACIDAD		LIMITACIONES PSIQUICAS
ACCESO A:	SOPORTES LÓGICOS	ENTORNOS OPERATIVOS Y APLICACIONES INFORMATICAS
REFERENCIA:	AENOR UNE 139802 EX	REQ. GENERALES CONTROL TECLADO
EPÍGRAFE	DESCRIPCIÓN	
	control y de las teclas de cambio de estado del teclado.	
6.1.8	Se deben incorporar sistemas de ayuda textual o basada en lengua de signos y abecedarios dactilológicos para facilitar la comprensión de un elemento de la aplicación informática.	
6.1.17	Se debe diseñar la aplicación minimizando los pasos necesarios para activar cualquier opción.	
6.1.24	La aplicación debe ofrecer la opción de finalizar.	
6.1.26	La aplicación no debe anular la ejecución de las herramientas de acceso cargadas previamente.	
6.1.27	La aplicación debe usar los servicios del entorno operativo.	
6.2.4	La secuencia de cambio por teclado de un elemento a otro dentro de una caja de diálogo debe ser coherente con su disposición en pantalla.	
6.2.5	Debe existir la posibilidad de cambiar de una ventana a otra.	

TIPO DE DISCAPACIDAD		LIMITACIONES PSIQUICAS
ACCESO A:	SOPORTES LÓGICOS	NAVEGADORES Y PAGINAS HTML
REFERENCIA:	AENOR UNE 139802 EX	
EPÍGRAFE	DESCRIPCIÓN	
7.1.1	Las características de accesibilidad de los navegadores deberán cumplir los mismos requisitos que cualquier otro programa de usuario.	
7.2.1	Las características de accesibilidad de las páginas web, incluyendo HTML, CGIs, Java, etc. deberán cumplir los mismos requisitos que cualquier otro programa de usuario.	
7.2.2	Los enlaces de tipo texto que sean consecutivos deben ir separados por barras verticales o algún otro carácter que no forme parte del enlace.	
7.2.3	Los enlaces de tipo texto que estén en la misma página deberán ser distintos unos de otros.	
7.2.4	Los puntos de llegada a una zona intermedia de una página web desde un enlace, que sean de tipo texto, deberán ir acompañados de un enlace que apunte a una parte significativa de la página.	
7.2.5	Se debe evitar el uso de textos que se muevan o parpadeen.	
7.2.6	Se debe evitar el uso de textos verticales.	
7.2.7	Se recomienda que los botones o enlaces que tengan una misma función aparezcan siempre en la misma posición de la página.	
7.2.8	Se recomienda que las listas dentro de una página se hagan tipo viñeta o numeradas.	
7.2.12	Se recomienda evitar o minimizar el uso de marcos (frames) en una página.	

TIPO DE DISCAPACIDAD		LIMITACIONES PSIQUICAS
ACCESO A:	SOPORTES LÓGICOS	NAVEGADORES Y PAGINAS HTML
REFERENCIA:	AENOR UNE 139802 EX	
EPÍGRAFE	DESCRIPCIÓN	
7.2.13	Los gráficos internos (formato GIF) o gráficos que necesiten visualizadores externos (JPEG) deberán tener una descripción alternativa en forma textual asociada a la imagen.	
7.2.14	Las piezas de audio que vayan en una página deberán tener un enlace a una página en la que se describa con texto el contenido del audio.	

A1.3 REQUISITOS DE ACCESIBILIDAD PARA LAS PERSONAS CON LIMITACIONES AUDITIVAS DE LEVES A SEVERAS

TIPO DE DISCAPACIDAD		LIMITACIONES AUDITIVAS
ACCESO A:	SOPORTES FISICOS	ENTORNOS OPERATIVOS UNIDAD CENTRAL, DISP. PERIFERICOS
REFERENCIA:	AENOR UNE 139801 EX	
EPÍGRAFE	DESCRIPCIÓN	
5.1.3	Se recomienda que los interruptores y los mandos se etiqueten con símbolos fáciles de comprender.	
5.1.11	Los controles de la unidad central deben estar localizados en la parte frontal o superior, en especial el botón de encendido / apagado.	
5.1.12	Las opciones ofrecidas por los controles deben ser configurables por software, ya sea en el sistema operativo o en software distribuido por el propio fabricante.	
5.1.13	Se recomienda que los interruptores y los mandos se etiqueten con símbolos fáciles de comprender.	
5.1.14	Las etiquetas de identificación de los controles deben ser de alto contraste y utilizar tipo de letra '*sans serif*'.	
5.1.15	Se recomienda que las etiquetas de identificación de los controles tengan un tipo de letra lo más grande posible y en negrita.	
5.2.16	Debe existir indicación visual de sonidos generados en el uso normal del periférico.	
5.2.17	El dispositivo periférico no debe generar campos electromagnéticos o de radiofrecuencia que puedan afectar a usuarios con audífono.	

TIPO DE DISCAPACIDAD		LIMITACIONES AUDITIVAS
ACCESO A:	SOPORTES LÓGICOS	REQ. GENERALES, ENTORNOS OPERATIVOS APLICACIONES
REFERENCIA:	AENOR UNE 139802 EX	
EPÍGRAFE	DESCRIPCIÓN	
5.1.5	Las herramientas de acceso que ofrece el entorno operativo deben tener carácter opcional en su activación/desactivación, sin necesidad de reinicializar el entorno.	
5.1.8 6.1.2	Se recomienda utilizar mensajes cortos y sencillos.	
5.1.9 6.1.4	El mismo tipo de mensaje debe tomar siempre el mismo formato de visualización.	
5.1.10 6.1.5	La visualización de la información en la pantalla no debe estar sujeta a requisitos temporales.	
5.1.11 6.1.6	Los mensajes críticos deben ser validados por el usuario antes de desaparecer o tramitarse.	
5.1.13 6.1.8	Deben incorporarse sistemas de ayuda textual o basada en lengua de signos y abecedario dactilológico para facilitar la comprensión de un elemento del entorno operativo.	
5.1.14	El entorno operativo debe ofrecer la posibilidad de cambiar la frecuencia del sonido de los avisos audio.	
5.1.15 6.1.9	No debe ofrecerse información sólo por vía audio. Cualquier aviso o alarma sonora debe proporcionarse de forma visual.	
6.1.26	La aplicación no debe anular la ejecución de las herramientas de acceso cargadas previamente.	
6.1.27	La aplicación debe usar los servicios del entorno operativo.	

TIPO DE DISCAPACIDAD		LIMITACIONES AUDITIVAS
ACCESO A:	SOPORTES LÓGICOS	NAVEGADORES Y PAGINAS HTML
REFERENCIA:	AENOR UNE 139802 EX	
EPÍGRAFE	DESCRIPCIÓN	
7.1.1	Las características de accesibilidad de los navegadores deberán cumplir los mismos requisitos que cualquier otro programa de usuario.	
7.2.1	Las características de accesibilidad de las páginas web, incluyendo HTML, CGIs, Java, etc. deberán cumplir los mismos requisitos que cualquier otro programa de usuario.	
7.2.14	Las piezas de audio que vayan en una página deberán tener un enlace a una página en la que se describa con texto el contenido del audio.	
7.2.15	Las piezas de vídeo que vayan en una página deberán tener un enlace a una página en la que se describa con texto el contenido del vídeo, o utilizar un sistema de subtitulado.	

A1.4 REQUISITOS DE ACCESIBILIDAD PARA LAS PERSONAS CON LIMITACIONES VISUALES

TIPO DE DISCAPACIDAD		LIMITACIONES VISUALES	
ACCESO A:	SOPORTES FISICOS	UNIDAD CENTRAL DISP. PERIFÉRICOS MONITOR, TECLADO	
REFERENCIA:	AENOR UNE 139801 EX		
EPÍGRAFE	DESCRIPCIÓN		
5.1.4	Las etiquetas de identificación de los controles deben ser de alto contraste y utilizar tipo de letra '*sans serif*'.		
5.1.5	Se recomienda que las etiquetas de identificación de los controles tengan un tipo de letra lo más grande posible y en negrita.		
5.1.6	Para las etiquetas de identificación se deberán facilitar alternativas Braille o táctiles.		
5.1.10	Se debe avisar al usuario de una incorrecta inserción del soporte de almacenamiento		
5.2.10	Las etiquetas de identificación de los controles deben ser de alto contraste y utilizar tipo de letra '*sans serif*'.		
5.2.11	Se recomienda que las etiquetas de identificación de los controles tengan un tipo de letra lo más grande posible y en negrita.		
5.2.12	Para las etiquetas de identificación se deberán facilitar alternativas Braille o táctiles.		
5.3.1	El monitor debe ser independiente de la unidad central para poder situarlo en una posición accesible o sustituirlo por otro más adecuado a las necesidades del usuario.		
5.4.4	Se deben incluir marcas táctiles en las teclas centrales de cada grupo funcional.		

TIPO DE DISCAPACIDAD		LIMITACIONES VISUALES	
ACCESO A:	SOPORTES LÓGICOS	REQ. GENERALES ENTORNOS OPERATIVOS, APLICACIONES, CONTROL TECLADO	
REFERENCIA:	AENOR UNE 139802 EX		
EPÍGRAFE	DESCRIPCIÓN		
5.1.3	Se requiere la inclusión de funciones que ofrezcan la posibilidad de enviar a salida audio cualquier información textual.		
5.1.4 6.1.3	La salida por voz debe producirse inmediatamente después de que ocurra el evento que la genera.		
5.1.5	Las herramientas de acceso que ofrece el entorno operativo deben tener carácter opcional en su activación/desactivación, sin necesidad de reinicializar el entorno.		
5.1.7	La estructura de datos que define un elemento de la interfaz de usuario en el entorno operativo debe disponer de una identificación de dicho elemento y de servicios para su consulta.		
5.1.11 6.1.6	Los mensajes críticos deben ser validados por el usuario antes de desaparecer o tramitarse.		
5.1.12	La visualización de información en la pantalla no debe apoyarse sólo en los colores		

TIPO DE DISCAPACIDAD		LIMITACIONES VISUALES	
ACCESO A:	SOPORTES LÓGICOS	REQ. GENERALES ENTORNOS OPERATIVOS, APLICACIONES, CONTROL TECLADO	
REFERENCIA:	AENOR UNE 139802 EX		
EPÍGRAFE	DESCRIPCIÓN		
6.1.7	de sus elementos.		
5.1.22 6.1.16	Los menús deben ser circulares, es decir, estar hechos de tal forma que al alcanzar el último elemento se pase al primero y viceversa.		
5.1.23 6.1.18	Cuando exista una visualización de textos (edición, cuadros de texto, etc.) su contenido debe poderse recorrer con el cursor.		
5.1.25	Se debe permitir la modificación de tamaño y lugar de los iconos u otros objetos		
5.1.26 6.1.20	Todos los iconos deben tener asociada una etiqueta de texto y se debe facilitar una opción que permita ver sólo esa etiqueta.		
5.1.28 6.1.22	Los gráficos o imágenes deberán ser informados, es decir, deberán ir acompañados de un texto descriptivo.		
5.3.2	Debe incluir una opción que permita visualizar y escuchar el estado de las teclas de control y de las teclas de cambio de estado del teclado.		
6.1.1	Todo elemento textual y de identificación (nombre de la ventana, etiqueta del icono, etc.) de la aplicación debe ser susceptible de emitirse por voz, utilizando los servicios facilitados por el entorno operativo.		
6.1.26	La aplicación no debe anular la ejecución de las herramientas de acceso cargadas previamente.		
6.1.27	La aplicación debe usar los servicios del entorno operativo.		

TIPO DE DISCAPACIDAD		LIMITACIONES VISUALES
ACCESO A:	SOPORTES LÓGICOS	NAVEGADORES Y PAGINAS HTML
REFERENCIA:	AENOR UNE 139802 EX	
EPÍGRAFE	DESCRIPCIÓN	
7.1.1	Las características de accesibilidad de los navegadores deberán cumplir los mismos requisitos que cualquier otro programa de usuario.	
7.1.2	Los navegadores de Internet deberán permitir el desplazamiento dentro de las páginas HTML utilizando sólo el ratón y sólo el teclado.	
7.1.3	El navegador debe posibilitar el paso de un enlace a otro, tanto por ratón como por teclado.	
7.1.4	Los navegadores deben facilitar la posibilidad de pasar de un marco (*frame*) a otro, tanto por ratón como por teclado.	
7.2.1	Las características de accesibilidad de las páginas web, incluyendo HTML, CGIs, Java, etc., deberán cumplir los mismos requisitos que cualquier otro programa de usuario.	
7.2.2	Los enlaces de tipo texto que sean consecutivos deben ir separados por barras verticales o algún otro carácter que no forme parte del enlace.	

TIPO DE DISCAPACIDAD		LIMITACIONES VISUALES
ACCESO A:	SOPORTES LÓGICOS	NAVEGADORES Y PAGINAS HTML
REFERENCIA:	AENOR UNE 139802 EX	
EPÍGRAFE	DESCRIPCIÓN	
7.2.3	Los enlaces de tipo texto que estén en la misma página deberán ser distintos unos de otros.	
7.2.4	Los puntos de llegada a una zona intermedia de una página web desde un enlace, que sean de tipo texto, deberán ir acompañados de un enlace que apunte a una parte significativa de la página.	
7.2.5	Se debe evitar el uso de textos que se muevan o parpadeen.	
7.2.6	Se debe evitar el uso de textos verticales.	
7.2.7	Se recomienda que los botones o enlaces que tengan una misma función aparezcan siempre en la misma posición de la página.	
7.2.8	Se recomienda que las listas dentro de una página se hagan tipo viñeta o numeradas.	
7.2.9	Se recomienda evitar el uso de tablas en las páginas.	
7.2.10	Si se usan formularios hay que proporcionar una copia del formulario que se pueda rellenar por correo electrónico fuera de línea.	
7.2.11	Si se facilita información en formatos alternativos (PDF, MS-Word, etc.) se debe poner la misma información en HTML o en ASCII.	
7.2.12	Se recomienda evitar o minimizar el uso de marcos (*frames*) en una página.	
7.2.13	Los gráficos internos (formato GIF) o gráficos que necesiten visualizadores externos (JPEG) deberán tener una descripción alternativa en forma textual asociada a la imagen.	
7.2.15	Las piezas de vídeo que vayan en una página deberán tener un enlace a una página en la que se describa con texto el contenido del vídeo, o utilizar un sistema de subtítulos.	
7.2.16	Si se utilizan mapas sensibles hay que poner una lista de todos los enlaces a los que se puede acceder a través de él, o se puede dar una página alternativa en modo texto.	
7.2.17	Se recomienda probar el contenido de las páginas web utilizando navegadores que no soporten gráficos.	

TIPO DE DISCAPACIDAD	LIMITACIONES VISUALES	
ACCESO A:	DOCUMENTACION	
REFERENCIAS:	AENOR UNE 139801 EX / AENOR UNE 139802 EX	
EPÍGRAFE	DESCRIPCIÓN	
6.1 / 8.1	La documentación debe entregarse en formato electrónico.	
6.4 / 8.4	La información gráfica deberá ir acompañada de una descripción textual de su contenido.	
6.5 / 8.5	El color del papel y de la letra deben tener un alto contraste.	
6.6 / 8.6	Se deben evitar informaciones que se apoyen exclusivamente en el color.	

A1.5 REQUISITOS DE ACCESIBILIDAD PARA LAS PERSONAS CON CEGUERA O SORDO CIEGAS

TIPO DE DISCAPACIDAD		PERSONAS CON CEGUERA O SORDO CIEGAS
ACCESO A:	SOPORTES FISICOS	ENTORNOS OPERATIVOS, UNIDAD CENTRAL, DISP. PERIFERICOS, TECLADO
REFERENCIA:	AENOR UNE 139801 EX	
EPÍGRAFE	DESCRIPCIÓN	
5.1.6	Para las etiquetas de identificación se deberán facilitar alternativas Braille o táctiles.	
5.1.10	Se debe avisar al usuario de una incorrecta inserción del soporte de almacenamiento (no aplicable a personas sordo ciegas).	
5.2.12	Para las etiquetas de identificación se deberán facilitar alternativas Braille o táctiles.	
5.4.4	Se deben incluir marcas táctiles en las teclas centrales de cada grupo funcional.	

TIPO DE DISCAPACIDAD		PERSONAS CON CEGUERA O SORDO CIEGAS
ACCESO A:	SOPORTES LÓGICOS	REQ. GENERALES, ENTORNOS OPERATIVOS, CONTROL TECLADO, APLICACIONES
REFERENCIA:	AENOR UNE 139802 EX	
EPÍGRAFE	DESCRIPCIÓN	
5.1.3	Se requiere la inclusión de funciones que ofrezcan la posibilidad de enviar a salida audio cualquier información textual (no aplicable a personas sordo ciegas).	
5.1.4 6.1.3	La salida por voz debe producirse inmediatamente después de que ocurra el evento que la genera.	
5.1.5	Las herramientas de acceso que ofrece el entorno operativo deben tener carácter opcional en su activación/desactivación, sin necesidad de reinicializar el entorno.	
5.1.7	La estructura de datos que define un elemento de la interfaz de usuario en el entorno operativo debe disponer de una identificación de dicho elemento y de servicios para su consulta.	

TIPO DE DISCAPACIDAD		PERSONAS CON CEGUERA O SORDO CIEGAS
ACCESO A:	SOPORTES LÓGICOS	REQ. GENERALES, ENTORNOS OPERATIVOS, CONTROL TECLADO, APLICACIONES
REFERENCIA:	AENOR UNE 139802 EX	
EPÍGRAFE	DESCRIPCIÓN	
5.1.11 6.1.6	Los mensajes críticos deben ser validados por el usuario antes de desaparecer o tramitarse.	
5.1.22 6.1.16	Los menús del entorno operativo deben ser circulares, es decir, estar hechos de tal forma que al alcanzar el último elemento se pase al primero y viceversa.	
5.1.23 6.1.18	Cuando exista una visualización de textos (edición, cuadros de texto, etc.) su contenido debe poderse recorrer con el cursor.	
5.1.26 6.1.20	Todos los iconos deben tener asociada una etiqueta de texto y se debe facilitar una opción que permita ver sólo esa etiqueta.	
5.1.27 6.1.21	Se debe evitar el uso de gráficos para poner textos. Para ello se deben usar los tipos de letra y funciones de escritura de texto facilitadas por el propio entorno operativo.	
5.1.28 6.1.22	Los gráficos o imágenes deberán ser informados, es decir, deberán ir acompañados de un texto descriptivo.	
5.1.29 6.1.23	En los formularios se debe poner la etiqueta a la izquierda y alineado horizontalmente con la primera línea del campo de entrada o de visualización de datos.	
5.3.2	Debe incluir una opción que permita visualizar y escuchar el estado de las teclas de control y de las teclas de cambio de estado del teclado.	
6.1.1	Todo elemento textual y de identificación (nombre de la ventana, etiqueta del icono, etc.) de la aplicación debe ser susceptible de emitirse por voz (no aplicable a personas sordo ciegas).	
6.1.3	La salida por voz debe producirse inmediatamente después de que ocurra el evento que la genera.	
6.1.26	La aplicación no debe anular la ejecución de las herramientas de acceso cargadas previamente.	
6.1.27	La aplicación debe usar los servicios del entorno operativo.	

TIPO DE DISCAPACIDAD		PERSONAS CON CEGUERA O SORDO CIEGAS
ACCESO A:	SOPORTES LÓGICOS	NAVEGADORES Y PAGINAS HTML
REFERENCIA:	AENOR UNE 139802 EX	
EPÍGRAFE	DESCRIPCIÓN	
7.1.1	Las características de accesibilidad de los navegadores deberán cumplir los mismos requisitos que cualquier otro programa de usuario.	
7.1.2	Los navegadores de Internet deberán permitir el desplazamiento dentro de las páginas HTML utilizando sólo el ratón y sólo el teclado.	

TIPO DE DISCAPACIDAD		PERSONAS CON CEGUERA O SORDO CIEGAS
ACCESO A:	SOPORTES LÓGICOS	NAVEGADORES Y PAGINAS HTML
REFERENCIA:	AENOR UNE 139802 EX	
EPÍGRAFE	DESCRIPCIÓN	
7.1.3	El navegador debe posibilitar el paso de un enlace a otro, tanto por ratón como por teclado	
7.1.4	Los navegadores deben facilitar la posibilidad de pasar de un marco (*frame*) a otro, tanto por ratón como por teclado.	
7.2.1	Las características de accesibilidad de las páginas web, incluyendo HTML, CGIs, Java, etc., deberán cumplir los mismos requisitos que cualquier otro programa de usuario.	
7.2.2	Los enlaces de tipo texto que sean consecutivos deben ir separados por barras verticales o algún otro carácter que no forme parte del enlace.	
7.2.3	Los enlaces de tipo texto que estén en la misma página deberán ser distintos unos de otros.	
7.2.4	Los puntos de llegada a una zona intermedia de una página web desde un enlace, que sean de tipo texto, deberán ir acompañados de un enlace que apunte a una parte significativa de la página.	
7.2.5	Se debe evitar el uso de textos que se muevan o parpadeen.	
7.2.6	Se debe evitar el uso de textos verticales.	
7.2.7	Se recomienda que los botones o enlaces que tengan una misma función aparezcan siempre en la misma posición de la página.	
7.2.8	Se recomienda que las listas dentro de una página se hagan tipo viñeta o numeradas.	
7.2.9	Se recomienda evitar el uso de tablas en las páginas.	
7.2.10	Si se usan formularios hay que proporcionar una copia del formulario que se pueda rellenar por correo electrónico fuera de línea.	
7.2.11	Si se facilita información en formatos alternativos (PDF, MS-Word, etc.) se debe poner la misma información en HTML o en ASCII.	
7.2.12	Se recomienda evitar o minimizar el uso de marcos (*frames*) en una página.	
7.2.13	Los gráficos internos (formato GIF) o gráficos que necesiten visualizadores externos (JPEG) deberán tener una descripción alternativa en forma textual asociada a la imagen.	
7.2.15	Las piezas de vídeo que vayan en una página deberán tener un enlace a una página en la que se describa con texto el contenido del vídeo, o utilizar un sistema de subtítulos.	
7.2.16	Si se utilizan mapas sensibles hay que poner una lista de todos los enlaces a los que se puede acceder a través de él, o se puede dar una página alternativa en modo texto.	
7.2.17	Se recomienda probar el contenido de las páginas web utilizando navegadores que no soporten gráficos.	

TIPO DE DISCAPACIDAD	PERSONAS CON CEGUERA O SORDO CIEGAS	
ACCESO A:	DOCUMENTACION	
REFERENCIAS:	AENOR UNE 139801 EX / AENOR UNE 139802 EX	
EPÍGRAFE	DESCRIPCIÓN	
6.1 / 8.1	La documentación debe entregarse en formato electrónico.	
6.4 / 8.4	La información gráfica deberá ir acompañada de una descripción textual de su contenido.	

A1.6 REQUISITOS DE ACCESIBILIDAD A SOPORTES LÓGICOS

Se especifican requisitos para:

- Accesibilidad al entorno operativo, que incluyen requisitos generales, ventanas, controlador de teclado y controlador de ratón.
- Accesibilidad de las aplicaciones informáticas que incluye igualmente requisitos generales y aplicaciones con ventanas.
- Accesibilidad a las autopistas de la información que incluye navegadores y páginas web.
- Accesibilidad de la documentación.

Para que el grupo con limitaciones motrices (LF) pueda trabajar sobre las mismas aplicaciones que cualquier otra persona sin discapacidad se requiere la inclusión de programas emuladores para los siguientes dispositivos de entrada:

- Teclado: Para los usuarios que pueden utilizar únicamente el teclado, se requiere un emulador de ratón por teclado.
- Ratón: Para los usuarios que únicamente pueden utilizar el ratón, se requiere un programa emulador de teclado controlado por ratón.
- Pulsador: Para los usuarios que únicamente pueden utilizar pulsadores, se requiere un programa emulador de teclado y otro de ratón.

La norma requiere la inclusión de funciones que ofrezcan la posibilidad de enviar a la salida audio cualquier información textual y especifica sus características.

MINISTERIO
DE ADMINISTRACIONES
PÚBLICAS

SECRETARIA GENERAL
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 CONSERVACIÓN

24 de junio de 2004

Madrid, junio de 2004

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. Presentada al Pleno de CIABSI de 18 de 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.
Versión 2.2. Aprobada por la Sesión plenaria de la CIABSI de 24 de junio de 2004.	Actualización programada: actualización de contenidos, revisión editorial.

1 Presentación

Introducción

Este documento 'Criterios de conservación', elaborado por el Consejo Superior de Informática y para el impulso de la Administración Electrónica, expone los requisitos, criterios y recomendaciones para la conservación de la información en soporte electrónico en 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 conservación de la información en el marco 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 conservación contemplan donde procede 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* 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.*

Objetivos

Los 'Criterios de conservación' 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 conservación de la información en soporte electrónico relativa a 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 conservación de la información manejada por las aplicaciones utilizadas para el ejercicio de potestades.
- 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.

Adopción de medidas de conservación organizativas y técnicas

La conservación de la información no debe considerarse de forma aislada; junto con la utilización y acceso a la información, es una etapa más del ciclo de vida de la misma en soporte electrónico. La gestión de dispositivos, soportes electrónicos y formatos debe ponerse en práctica aplicando procedimientos orientados a la manipulación de datos sensibles, especialmente si son de carácter personal; a la salvaguarda frente a deterioro, daño, robo o acceso no autorizado; a la eliminación o destrucción de soportes; a la gestión de los soportes removibles, etc. Estas medidas para la

conservación de la información deben adoptarse de acuerdo con los especialistas en la gestión de archivos para diseñar soluciones prácticas a la medida de sus necesidades.

Estructura y contenidos

El documento se estructura en los siguientes capítulos:

- Conservación de la información en soporte electrónico
- Ciclo de vida de la información en soporte electrónico
- Formato de la información en soporte electrónico
- Soportes
- Medidas de almacenamiento y conservación
- Sistema de archivos

Para cada uno de estos capítulos se tratan los siguientes aspectos:

- Las ***prescripciones o requisitos legales,*** que obligan a aplicar las distintas medidas para la conservación de la información, en particular en relación con la validez de los procedimientos administrativos y con los datos de carácter personal.
- Los ***criterios*** señalan las medidas de seguridad organizativas y técnicas que se deben adoptar para satisfacer los requisitos anteriores; además, se numeran para facilitar su localización y referencia.
- Las ***recomendaciones*** complementan a los criterios expuestos con otras medidas técnicas u organizativas posibles.
- Los ***niveles de seguridad*** desarrollan los niveles de seguridad a los que se refiere el Real Decreto 994/1999, de 11 de junio, Reglamento de medidas de seguridad de los ficheros automatizados que contienen datos de carácter personal y que se aplican a los criterios.

  No obstante, las medidas necesarias para garantizar la seguridad que deben reunir los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervienen en el tratamiento y conservación de los datos de carácter personal, están expuestas con más detalle en el documento 'Criterios de seguridad'.

- La ***ampliación técnica*** da referencias que permiten profundizar y ampliar los conceptos técnicos y organizativos en los que se fundamentan las distintas medidas de conservación.

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

  Los criterios y recomendaciones incluidos en este documento tienen en cuenta términos de referencia ampliamente aceptados y difundidos como la *Guía de la información electrónica* elaborada por el DLM Forum.

Modo de empleo

En todo momento ha de tenerse en cuenta que la aplicación de las medidas de conservación expuestas en este documento debe realizarse atendiendo, en general, al **principio de proporcionalidad** que se establece entre la naturaleza de los datos y los tratamientos, 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**.

Asimismo, no todas las recomendaciones expuestas son aplicables en todos los casos y, obviamente, han de considerarse las situaciones particulares y, en determinadas circunstancias, la necesidad de incluir o desarrollar aspectos no incluidos en este documento.

Finalmente, por la naturaleza de sus contenidos, ha de tenerse en cuenta que este es un **documento vivo** que ha de verse **sometido a actualización con cierta regularidad**, para añadir, perfeccionar o completar de manera conveniente los apartados que lo requieran.

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".

Destinatarios

Va dirigido 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.

2 Conservación de la información en soporte electrónico

Documentos administrativos y de los ciudadanos

CONCEPTOS:

- **Documento:** entidad identificada y estructurada que contiene texto, gráficos, sonidos, imágenes o cualquier otra clase de información que puede ser almacenada, editada, extraída e intercambiada entre sistemas de tratamiento de la información o usuarios como una unidad diferenciada (RD 263/1996).
- **Documento electrónico**: Se considera documento electrónico el redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente. El documento electrónico será soporte de:

  a) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.

  b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.

  c) Documentos privados. (Ley 59/2003).

- **Soporte**: objeto sobre el cual o en el cual es posible grabar y recuperar datos (RD 263/1996).
- **Medio**: mecanismo, instalación, equipo o sistema de tratamiento de la información que permite, utilizando técnicas electrónicas, informáticas o telemáticas, producir, almacenar o transmitir documentos, datos e informaciones (RD 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 (RD 263/1996).

CONSIDERACIONES:

Como explica el *Manual de Documentos Administrativos* la actividad administrativa se distingue por su carácter documental, de tal forma que los documentos administrativos:

- constituyen el testimonio de su actividad,
- son el soporte en el que se materializan los distintos actos de la Administración Pública
- y son la forma externa de dichos actos.

Los documentos administrativos responden a dos funciones principales, que son:

- la función de constancia
- y la función de comunicación.

Responden a la función de constancia, pues al asegurar la pervivencia de las actuaciones administrativas se garantiza:

- la conservación de los actos y la posibilidad de demostrar su existencia, sus efectos y sus posibles errores o vicios,
- así como el derecho de los ciudadanos a acceder a los mismos. Responden a la función de comunicación, pues sirven de medio de comunicación de los actos de la Administración;

En cuanto a la función de comunicación, ésta puede ser interna a la Administración o externa de la Administración con los ciudadanos y con otras organizaciones.

Entre los documentos de la Administración se encuentran:

- Documentos de *decisión:* Resoluciones, Acuerdos
- Documentos de *transmisión*: Comunicaciones, Notificaciones, Publicaciones
- Documentos de *constancia*: Actas, Certificados
- Documentos de *juicio*: Informes
- Otros documentos: de información, de carácter cultural, histórico, etc.

Entre los documentos de los ciudadanos se encuentran:

- Solicitudes, Denuncias, Alegaciones, Recursos.

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Los documentos emitidos por los órganos y entidades del ámbito de la Administración General del Estado y por los particulares en sus relaciones con aquellos, 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. (RD 263/1996, 6.1)

En relación con los derechos del ciudadano de acceso a archivos y registros administrativos:

- Los ciudadanos tienen derecho a acceder a los registros y a los documentos que obren en los archivos administrativos, cualquiera que sea la forma de expresión gráfica, sonora o en imagen o en el tipo de soporte material en que figuren, en las condiciones en las condiciones que se

establecen (expedientes terminados, interés legítimo y directo, otras específicas) (Ley 30/1992, art. 45.2)

CRITERIOS:

2.1 Se deben conservar los documentos registrados, generados o recibidos, cuyo contenido y estructura sea evidencia, o prueba de valor legal, de una actividad administrativa, en el marco de la aplicación para el ejercicio de potestades.

2.2 Se debe conservar el contenido de los documentos administrativos y de los ciudadanos en soporte electrónico, informático o telemático, en un formato compatible con los medios técnicos de que disponen las Administraciones Públicas, que aseguren la independencia necesaria para garantizar su pervivencia así como la no discriminación respecto a la accesibilidad de los ciudadanos a la misma.

2.3 Se deben utilizar normas y estándares, disponibles públicamente, de derecho y especificaciones públicas libres de *royalties* y patentes. (Véase capítulos '*Formato de la información*' y '*Soportes*').

NIVELES DE SEGURIDAD:

- En función de los datos de carácter personal contenidos en el documento le son aplicables las medidas de nivel básico, medio o alto contempladas en el RD 994/1999, artículo 4 'Aplicación de los niveles de seguridad'.
- Cabe establecer los niveles de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento '*Criterios de seguridad*' el capítulo '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

- Manual de documentos administrativos, Ministerio de Administraciones Públicas; ed. Tecnos.
- Guía de la información electrónica (DLM Forum)
  http://europa.eu.int/historical_archives/dlm_forum/index_en.htm

Almacenamiento de la información en soporte electrónico

CONCEPTOS:

- Información almacenada en soporte electrónico es todo dato conservado con un formato que permite su tratamiento automático y que no es posible leerla y recuperarla sin la ayuda de una herramienta específica.

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Guardar la información de los ciudadanos: relacionada con los actos administrativos que afecten a los derechos y obligaciones del ciudadano; producida mediante técnicas electrónicas, informáticas o telemáticas, y contenida en soportes del mismo tipo. Almacenar la información electrónica, en soportes de la misma naturaleza, y en el mismo formato en que se originó o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. (RD 263/1996, art. 8.1,2)

En relación con los derechos del ciudadano de acceso a archivos y registros administrativos:

- Los ciudadanos tienen derecho a acceder a los registros y a los documentos que obren en los archivos administrativos, cualquiera que sea la forma de expresión gráfica, sonora o en imagen o en el tipo de soporte material en que figuren, en las condiciones en las condiciones que se establecen (expedientes terminados, interés legítimo y directo, otras específicas) (Ley 30/1992, art. 45.2)

CRITERIOS:

2.4 Se debe almacenar en soporte electrónico la información resultado de las actuaciones administrativas en el marco de la aplicación para el ejercicio de potestades.

2.5 Se debe almacenar la información electrónica, si no es posible hacerlo en el formato original, en un formato que asegure que puede reproducirse con el mismo contenido y estructura que el original.

2.6 Se deben utilizar normas y estándares, disponibles públicamente, de derecho y especificaciones públicas libres de *royalties* y patentes. (Véase capítulos '*Formato de la información*' y '*Soportes*').

NIVELES DE SEGURIDAD:

- En función de los datos de carácter personal contenidos en el documento le son aplicables las medidas de nivel básico, medio o alto contempladas en el RD 994/1999, artículo 4 'Aplicación de los niveles de seguridad'.
- Cabe establecer los niveles de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento '*Criterios de seguridad*' el capítulo '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

- Manual de documentos administrativos, Ministerio de Administraciones Públicas, ed. Tecnos.
- Guía de la información electrónica (DLM Forum)
  http://europa.eu.int/historical_archives/dlm_forum/index_en.htm

Análisis y gestión de riesgos

CONSIDERACIONES:

La conservación de los documentos en soporte electrónico tiene lugar en un entorno complejo y no exento de riesgos.

En primer lugar, la **evolución continua de la tecnología** hace que sea difícil la selección de soportes y formatos estables y duraderos, por los siguientes motivos:

- Aparición constante de nuevas versiones de plataformas, sistemas operativos y programas.
- Introducción de cambios en las características físicas de los soportes (tamaños, densidad de grabación, etc.).
- Ciertos soportes pueden tener una mayor vida útil, como objeto físico, pero pueden estar sometidos a una rápida obsolescencia tecnológica.

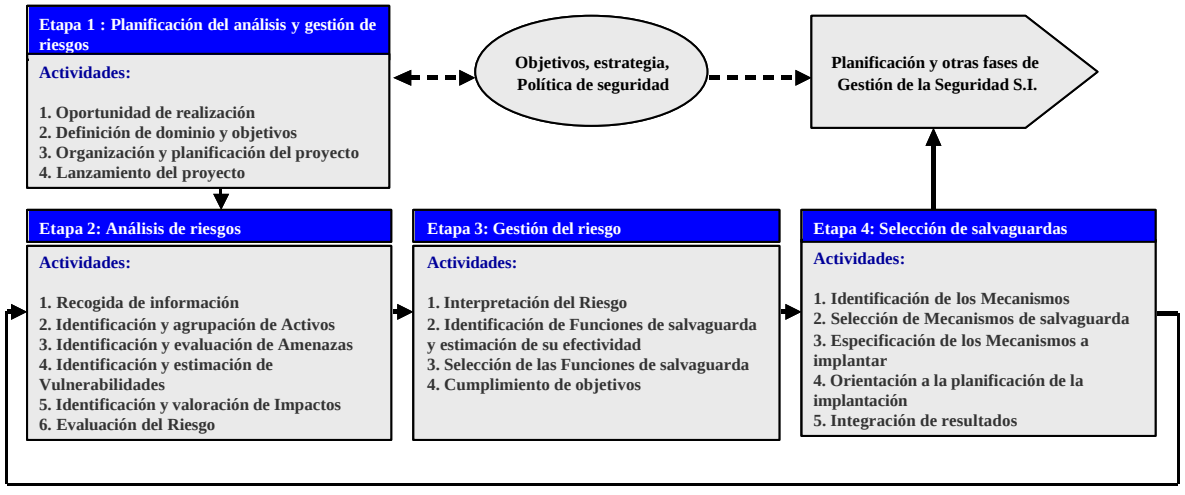
- Generación de nuevas formas de documentos electrónicos, tales como los documentos compuestos, hipertexto o multimedia.
- Disponibilidad de una gran capacidad de procesamiento y de almacenamiento que no va acompañada de los procedimientos necesarios para el control adecuado de documentos.
- Desarrollo de sistemas de información orientados a la gestión de datos pero no tanto a la gestión de documentos.

En segundo lugar, existen **amenazas** tales como las siguientes:

- Acumulación incontrolada de documentos.
- Destrucción accidental o incontrolada de documentos.
- Manipulación no autorizada de los mismos (acceso, alteración, destrucción).
- Ausencia de documentación asociada y de metadatos, que da lugar a ineficiencias en el acceso.
- Existen factores agresivos que facilitan su deterioro, tal es el caso de los campos magnéticos, de la oxidación o de la degradación de los materiales.
- Presencia de costes no deseados derivados de la adquisición de una capacidad de almacenamiento adicional sobredimensionada.

La adopción de medidas organizativas y técnicas para la conservación de la información se debe realizar de forma rigurosa y proporcionada a los riesgos detectados. El proceso de análisis y gestión de riesgos constituye la tarea primera y a la vez esencial de toda actuación organizada. 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 (implicación de la dirección, objetivos, políticas) y en las de carácter específico (planificación, organización, implantación de salvaguardas, sensibilización, acción diaria y mantenimiento).

- **Análisis de los riesgos:** Identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como 'activos'); para determinar la vulnerabilidad de los mismos ante esas amenazas y para estimar el impacto o grado de perjuicio que una materialización de las mismas puede tener, obteniendo cierto conocimiento del riesgo que se corre.
- **Gestión de los riesgos** Selección e implantación de las medidas 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.



Es decir, el análisis y gestión de riesgos debe ayudar a **formular y responder preguntas claves**, como las siguientes:

- ¿Qué información se ha de conservar y proteger?, ¿de qué tipo es? y ¿cuál es su valor?
- ¿De qué tipo es?
- ¿Cuáles son los plazos de conservación?
- ¿En qué soportes y formatos está?
- ¿Qué problemas de durabilidad, longevidad y degradación se plantean?
- ¿Quién tiene acceso, a qué, para qué, cuándo y cómo?
- ¿Qué amenazas afectan a la información?
- ¿Cuáles son las consecuencias si se materializan?
- ¿Qué medidas organizativas y técnicas se deben adoptar?

El análisis y gestión de riesgos aporta, por tanto, la racionalidad necesaria para la adopción de medidas organizativas y técnicas en el marco del **principio de proporcionalidad** que se establece entre la naturaleza de la información, los riesgos a los que está sometida, el estado de la tecnología y los costes (tanto de la ausencia de seguridad como de las salvaguardas).

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 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)
- Los medios o soportes en que se almacenen documentos deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos. (RD 263/1996, art. 8.4)
- Para las medidas técnicas seguir especificaciones de soportes, medios y aplicaciones conformes con las normas nacionales o internacionales que sean exigibles. (RD 263/1996, arts. 4.4 y 9.3c)

En relación con los derechos del ciudadano de acceso a archivos y registros administrativos:

- Los ciudadanos tienen derecho a acceder a los registros y a los documentos que obren en los archivos administrativos, cualquiera que sea la forma de expresión gráfica, sonora o en imagen o en el tipo de soporte material en que figuren, en las condiciones en las condiciones que se establecen (expedientes terminados, interés legítimo y directo, otras específicas) (Ley 30/1992, art. 45.2)

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, 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:

2.7 Se debe realizar el análisis y gestión de riesgos aplicando MAGERIT, Metodología de análisis y gestión de riesgos de los sistemas de información, orientado a la conservación de la información en soporte electrónico, para identificar, relacionar y valorar los activos de información, determinar y clasificar las posibles amenazas, evaluar su vulnerabilidad, estimar los posibles impactos, y, con los resultados de este análisis, desarrollar una gestión de riesgos para seleccionar, especificar y adoptar medidas organizativas y técnicas para prevenir daños y reducir su impacto.

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

2.9 Los riesgos y las salvaguardas de la aplicación se deben revisar cuando sea adecuado y periódicamente como una parte más de la gestión de la seguridad.

NIVELES DE SEGURIDAD:

- En función de los datos de carácter personal contenidos en el documento le son aplicables las medidas de nivel básico, medio o alto contempladas en el RD 994/1999, artículo 4 'Aplicación de los niveles de seguridad'.
- Cabe establecer los niveles de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento '*Criterios de seguridad*' el capítulo '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT), http://www.csi.map.es/csi/pg5m20.htm
- Guía de la información electrónica (DLM Forum) http://europa.eu.int/historical_archives/dlm_forum/index_en.htm

EJEMPLO DE SOLUCIÓN:

La elaboración de un análisis y gestión de riesgos orientado a la conservación de la información en soporte electrónico y en otros soportes puede hacerse siguiendo el conjunto de pautas sistemáticas especificadas en la metodología MAGERIT para conocer el estado de situación y, en base a este conocimiento, introducir las medidas organizativas y técnicas oportunas. La Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones públicas, MAGERIT, es un método formal para investigar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

El análisis de riesgos, siguiendo la metodología de análisis y gestión de riesgos MAGERIT, debe plantearse en términos de:

- **Activos**, estudio de los activos cuya conservación hay que asegurar:
  - *Entorno*: instalaciones físicas, apoyo logístico (suministros, repuestos y consumibles).
  - *Medios*: instalación ofimática, aplicaciones y equipos o sistema de tratamiento de la información.

- *Información* en soporte electrónico y en otros soportes (papel, microfilm, etc.)
- *Organización*: personas y usuarios.
- *Otros activos*: asociados a la credibilidad, intimidad e imagen de las personas físicas o jurídicas.

- **Amenazas**, examen de los posibles eventos accidentales o deliberados que pueden desencadenar un incidente, con la consiguiente producción de daños materiales e inmateriales en los activos. En el análisis de las amenazas inciden de forma muy directa las consecuencias derivadas del posible impacto de la evolución tecnológica, así como las posibles amenazas.
- **Vulnerabilidad**, investigación de las debilidades de los activos frente a las posibles amenazas.
- **Impacto**, estimación de las posibles consecuencias por la materialización de un incidente, resultado de la agresión sobre un activo. El impacto tiene consecuencias cuantitativas, si se trata de activos cuantificables, o cualitativas, si las consecuencias están asociadas a la cualidad del activo (pérdida de autenticidad, integridad, confidencialidad y disponibilidad); asimismo el impacto representa pérdidas directas e indirectas y afecta a la posibilidad de reemplazar o reconstruir el activo dañado.
- **Riesgo**, valoración de la posibilidad de que se produzca un impacto, obtenido como resultado del análisis de todos bs elementos anteriores, es decir, como expresión que indica la medida de la vulnerabilidad y del impacto que procede de la amenaza que puede actuar sobre el activo.
- **Salvaguardas**, medidas organizativas y técnicas, acciones y mecanismos de salvaguarda, que operan antes de la materialización de la amenaza y después de la agresión, en forma:
  - *Preventivas*, actúan sobre la vulnerabilidad neutralizando la amenaza, como es el caso de errores humanos.
  - *Curativas*, actúan sobre el impacto modificando y reduciendo el resultado de la agresión, como es el caso de los accidentes.

El análisis de riesgos proporciona elementos de conocimiento para tomar decisiones razonadas, y su resultado determina las prioridades a la hora de implantar salvaguardas, así como para determinar los costes que suponen las medidas adoptadas, costes deducidos al comparar los recursos dedicados a estas salvaguardas con los costes derivados de la falta, o de los fallos, de las mismas.

3 Ciclo de vida de la información en soporte electrónico

Ciclo de vida

CONSIDERACIONES:

Es preciso abordar la conservación de la información en soporte electrónico, y en otros soportes, desde una perspectiva global que contemple, al igual que se hace con los sistemas de información, todo el ciclo de vida de la misma, desde su creación, hasta su conservación, o en su caso destrucción, pasando por las etapas de mantenimiento y gestión. Sólo así se puede adoptar un conjunto coherente de normas y estándares que permita dar respuesta a los requisitos de seguridad y conservación, y a los de economía de gestión y de eficacia.

Esta perspectiva global se ha de manifestar, en particular, en una estrategia a largo plazo que garantice:

- La conservación de la información
- La accesibilidad de la misma
- La protección de los datos, especialmente los de carácter personal.

Esta estrategia se debe definir además, no de una forma aislada, sino en relación con la globalidad del sistema de información y teniendo en cuenta que, al igual que sucede con los documentos en papel, la información en soporte electrónico atraviesa a lo largo de su ciclo de vida tres grandes etapas:

- Diseño de la estrategia de gestión de la información en soporte electrónico.
- Creación de la información en soporte electrónico.
- Gestión y Conservación de la información.

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Guardar la información de los ciudadanos relacionada con los actos administrativos que afecten a los derechos e intereses del ciudadano; producida mediante técnicas electrónicas, informáticas o telemáticas, y contenida en soportes del mismo tipo. Almacenar la información electrónica, en soportes de la misma naturaleza, y en el mismo formato en que se originó o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. (RD 263/1996, art. 8.1,2)
- Los medios o soportes en que se almacenen documentos deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos. (RD 263/1996, art. 8.4)

En relación con los derechos del ciudadano de acceso a archivos y registros administrativos:

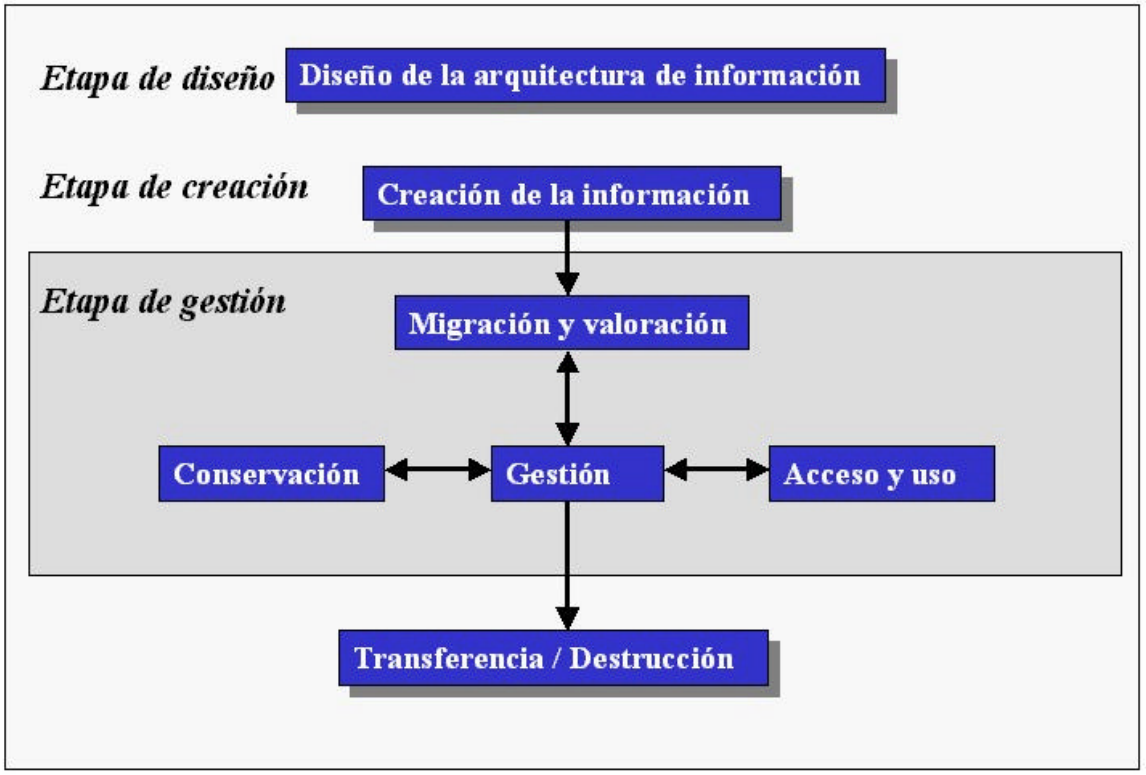
- Los ciudadanos tienen derecho a acceder a los registros y a los documentos que obren en los archivos administrativos, cualquiera que sea la forma de expresión gráfica, sonora o en imagen o en el tipo de soporte material en que figuren, en las condiciones en las condiciones que se establecen (expedientes terminados, interés legítimo y directo, otras específicas) (Ley 30/1992, art. 45.2)

CRITERIOS:

3.1 Se debe tratar la información en soporte electrónico, como en otro tipo de soporte, desde una perspectiva global que contemple todo el ciclo de vida, desde su diseño hasta su conservación o destrucción, pasando por las etapas de creación y gestión. ; sólo así se puede adoptar un conjunto coherente de medidas que permitan dar respuesta a los requisitos de seguridad, economía de gestión y eficacia.

RECOMENDACIONES:

- El modelo de ciclo de vida de la información elaborado por el DLM-Forum puede servir de guía:



NIVELES DE SEGURIDAD:

- Aplicar cuando la información contenga datos de carácter personal, las medidas del RD 994/1999 de seguridad: artículos 10 'Registro de incidencias', 11 'Identificación y autenticación', 12 'Control de accesos', 13 'Gestión de soportes' y 14 'Recuperación de datos'.
- Cabe establecer los niveles de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento '*Criterios de seguridad*' el capítulo '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

- Guía de la información electrónica (DLM Forum) http://europa.eu.int/historical_archives/dlm_forum/index_en.htm
- IDA MoReq (*Model requirments for the management of electronic records*) http://www.csi.map.es/csi/pg5m52.htm

Análisis del documento electrónico

CONSIDERACIONES:

Para tener la posibilidad de recuperar una información específica es necesario estructurarla, y según la finalidad de la información hay dos medios de hacerlo:

- Base de datos, como forma de almacenar los datos para que puedan ser recuperados y actualizados.

- Documento, como forma de presentar un asunto o describir una actividad administrativa.

  Un documento debe ser inalterable, su puesta al día generará un nuevo documento, y una base de datos puede ponerse al día con regularidad. No obstante, la actualización de una base de datos dará lugar a un documento si así está definido por procedimiento administrativo.

  El documento se puede estructurar en torno a los aspectos siguientes:

- Contenido del documento, con información del siguiente tipo:
  - *Texto*, páginas, párrafos y palabras,
  - Números,
  - Tablas,
  - *Dibujos*, gráficos, sonido y vídeo,
  - Enlaces hipertexto.
- Estructura lógica, incorporada al (o separada del) propio documento y que puede ser diferente de la estructura física.
- Contexto, documento asociado, que incluye:
  - *Descripción* de la actuación que corresponda.
  - *Metadatos técnicos:* aplicaciones y equipo necesario, número de versión, estructura del fichero, descripción de los datos, enlaces y relación con otros documentos.
  - Presentación, documento independiente que trata los aspectos de la propia presentación.

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Los medios o soportes en que se almacenen documentos deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos. (RD 263/1996, art. 8.4)

RECOMENDACIONES:

- Analizar la información manejada a fin de estructurar los datos en forma de documentos y bases de datos, para almacenar la información, y adoptar un criterio coherente de clasificación de los mismos.
- Agrupar los documentos (correspondencia, expedientes y registros), que describen una actividad, en un solo fichero o unidad coherente de información. En cada unidad de información clasificar los documentos por orden cronológico y temático o por palabras clave para facilitar la búsqueda y recuperación de la información.
- Conservar las bases de datos copiando los datos a un formato de bajo nivel (texto plano o en modo de acceso secuencial indexado) o si son bases de datos propietarias, debe considerarse la posibilidad de exportarlas a una base de datos de software libre, de forma automática o semiautomática.

NIVELES DE SEGURIDAD:

- En función de los datos de carácter personal contenidos en el documento le son aplicables las medidas de nivel básico, medio o alto contempladas en el RD 994/1999, artículo 4 ‘Aplicación de los niveles de seguridad’.

- Cabe asimismo establecer los niveles de medidas de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento *'Criterios de seguridad'* el capítulo '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

- Guía de la información electrónica (DLM Forum) http://europa.eu.int/historical_archives/dlm_forum/index_en.htm
- *Dublin Core* **[DC]** http://purl.org/DC
- *Content Standards for Digital Geospatial Metadata* **[FGDC]** http://www.fgdc.gov/metadata/
- *HyperText Markup Language***[HTML]** http://www.w3.org/MarkUp/
- *Platform for Privacy Preferences* **[P3P]** http://www.w3.org/P3P/
- *Platform for Internet Content Selection* **[PICS]** http://www.w3.org/PICS/
- *Resource Description Framework* http://www.w3.org/RDF
- *Standard Generalised Markup Language* **[SGML]** http://www.w3.org/MarkUp/SGML
- *World-Wide Web Consortium* **[W3C]** http://www.w3.org
- *eXtensible HyperText Markup Language* **[XHTML]** http://www.w3.org/TR/xhtml1
- *eXtensible Markup Language* **[XML]** http://www.w3.org/XML
- **[Z39.50]** http://lcweb.loc.gov/z3950/agency/

EJEMPLO DE SOLUCIÓN:

A continuación se identifican elementos de metadatos o del contexto de un documento para analizar y estructurar la información:

- Código, número de expediente.
- *Título*, denominación dada a los documentos electrónicos.
- Número de versión.
- *Creador o Autor*, persona/s responsable/s del contenido del documento.
- Destinatario, número de copias.
- *Tema*, palabras claves que describen el contenido, utilizadas en vocabularios o descriptores.
- *Descripción*, del contenido textual del documento, o resumen con un enlace a la propia descripción.
- *Editor*, entidad responsable y que da acceso a la información.
- *Colaboradores*, persona/s u organismo/s además del creador que aportaron una contribución importante.
- *Fecha*, expresada en forma de número de ocho cifras: (D) día; (M) mes y (A) año, tipo: DDMMAAAA.
- *Tipo*, categoría de la información elegida de entre una lista de tipos: borrador; trabajo, informe técnico.

- *Formato*, representación de los datos de la información: elegidos de entre los de una lista, que pueda aportar información sobre las aplicaciones, programas y equipos necesarios para poder visualizarlos o ejecutarlos.
- *Identificador*, número utilizado para identificar la información, el número o localizador de la dirección de una página de información en Internet (URL o URN) son un ejemplo de identificador, pero pueden utilizarse identificadores únicos o números oficiales.
- *Fuente*, obra impresa o electrónica de donde procede la información, por ejemplo la versión papel del documento que sirvió para su transcripción a versión electrónica.
- *Lenguaje*, lengua del contenido de la información, puede coincidir con los códigos de caracteres para los lenguajes escritos.
- *Relación con otra información*, tiene por finalidad el expresar la relación entre documentos, por ejemplo, imágenes de un documento, partes o capítulos o de un libro.
- *Alcance*, características espaciales o temporales de la información.
- *Derechos de autor*, declaración de la gestión de los derechos o del servicio que informa de las condiciones de acceso, rectificación, cancelación y oposición a la información.
- Niveles de seguridad y medidas aplicables.
- Palabras clave.
- Anexos.

Diseño de la estrategia de gestión

CONSIDERACIONES:

La estrategia de gestión puede considerar esencialmente las siguientes tres alternativas:

- 1. Traducción de los documentos digitales a formas independientes del equipo informático.

  Esta estrategia tiene que hacer frente al reto de la dificultad de una base formal para la normalización según un formato neutro, pero ofrece una solución al problema de la conservación de la información: Usando especificaciones internacionales libres de patentes y royalties se garantiza una accesibilidad completa a la información y una sencilla transición en caso de que se necesite transformarlo a otro formato de versión más reciente.

- 2. Prolongar la longevidad de los equipos informáticos y de sus soportes lógicos originales.

  Si bien esta estrategia puede ser de utilidad en algún caso concreto (por ejemplo, corto y medio plazo), representa una solución parcial al problema de la conservación, lo que la hace desaconsejable:

  - Puede convertir a la organización en un *museo de la informática*.
  - Puede originar elevados costes de reparación, sustitución y formación difícilmente justificables.
  - Por otra parte, una solución orientada a la utilización de emuladores exige una especificación minuciosa del equipo a emular.

- 3. Incorporar la traducción de la información a las nuevas tecnologías *hardware y software* como parte del desarrollo o mantenimiento de los sistemas.

  Esta estrategia parte de un enfoque global según el cual el documento o la información se debe conservar con independencia del soporte físico o de la tecnología. Para ello es necesario convertir,

regenerar, copiar o transferir de un soporte y tecnología a otra; mantener la autenticidad, integridad, identidad del autor; gestionar su plazo de conservación y su volumen; gestionar la conservación de la información y la accesibilidad de la misma; todo lo anterior en relación con la globalidad del sistema de información. Para desarrollar esta estrategia cabe considerar los siguientes elementos:

- *Métodos y procedimientos* para creación, modificación, duplicación, almacenamiento, conservación, recuperación, destrucción de la información en soporte electrónico.
- *Formación* de los actores implicados.
- *Trazabilidad* de las operaciones de creación, modificación,... ¿quién?, ¿cuándo?, ¿qué hizo?, ¿con qué resultados?
- *Auditorías periódicas*, para determinar grado de seguimiento de los procedimientos documentados.

CRITERIOS:

3.2 Se debe desarrollar y utilizar procedimientos documentados que identifiquen tareas, responsables y medios para la conservación y archivo de la documentación de acuerdo con las etapas del ciclo de vida de la información.

RECOMENDACIONES:

- Adoptar procedimientos para la estrategia de gestión de la información con planteamientos a corto, medio y largo plazo de acuerdo con las necesidades reales de conservación. Entre los aspectos a considerar figuran los siguientes:
  - La política de la organización y la asignación de responsabilidades.
  - La estructura de los ficheros con los datos de carácter personal y la descripción del sistema de información que los trata.
  - Las condiciones de identificación de usuarios e interesados, en la creación y eliminación de la información, y de protección y acceso a la misma por personal autorizado, junto con las medidas de seguridad aplicadas a la información que contiene datos personales.
  - La elección de formatos de fichero normalizados y perdurables para asegurar la independencia de los datos de sus soportes.
  - Los plazos de conservación, archivo y traspaso de la información.
  - La traducción de la información a formatos normalizados e independientes del equipo físico.
  - Las condiciones de realización de copias de respaldo y de recuperación de los datos.
  - Las condiciones de la renovación de sistemas y sustitución de soportes.
  - Mantener un registro o historial de las operaciones de tratamiento de la información en soporte electrónico.
  - Hacer auditorias periódicas de seguimiento de la utilización de los procedimientos.

  Estos procedimientos pueden formar parte de procedimientos de seguridad y, además, estar documentados como procedimientos de calidad.

NIVELES DE SEGURIDAD:

- En función de los tipos de datos personales de los ciudadanos contenidos en la información, le es aplicable del RD 994/1999, los artículos relativos al documento de seguridad y a las funciones y obligaciones del personal: artículos 8 y 9 para el nivel básico y artículo 15 para los niveles medio y alto.
- Cabe establecer los niveles de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento '*Criterios de seguridad*' el capítulo '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

- Guía de la información electrónica (DLM Forum)
  http://europa.eu.int/historical_archives/dlm_forum/index_en.htm

Creación de la información en soporte electrónico

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Cuando la Administración General del Estado o las entidades de derecho público vinculadas o dependientes de aquélla utilicen técnicas electrónicas, informáticas y telemáticas en actuaciones o procedimientos que afecten de forma directa o indirecta a derechos o intereses de los ciudadanos, se garantizará la identificación y el ejercicio de la competencia por el órgano correspondiente. (RD 263/1996, art. 2.2)
- 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)
- Hacer pública, mediante Ordenes ministeriales y Resoluciones, en el BOE la utilización de programas o aplicaciones de tratamiento para ejercicio de potestades. (RD 263/1996, art. 9.4)

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

- Hacer público, mediante disposición general, en el BOE la creación de toda base de datos que contenga datos de carácter personal. (LO 15/1999, art. 20.1)

CRITERIOS:

3.3 Se deben establecer reglas de creación de información en soporte electrónico, y convertir la información en papel a documentos electrónicos, para facilitar su consulta y utilización.

3.4 Se debe incluir y mantener por cada tipo de documento información de contexto para conocer su evolución.

3.5 Se deben generar copias de los documentos emitidos en soportes no reescribibles (Véase en el capítulo '*Soportes*', el apartado '*Tipos de soportes de almacenamiento de la información*').

3.6 Se deben generar copias de los documentos administrativos emitidos en soportes no reescribibles como es el caso de los **CD-R** y **DVD-R** de tipo WORM (múltiple lectura única escritura); estos soportes duran más años y no se ven afectados por el número de veces que se lean; también se conocen en el mercado como soportes 'no repudiables'. (Véase en el capítulo '*Soportes*', el apartado '*Tipos de soportes de almacenamiento de la información*').

3.7 Se deben utilizar en la creación de información en soporte electrónico formatos, soportes y juegos de caracteres que faciliten la normalización y la longevidad (véase capítulos '*Formato de la información*' y '*Soportes*').

RECOMENDACIONES:

- Transformar los documentos que estén en soporte de papel en documentos electrónicos (escaneado del original) mediante técnicas de reconocimiento de caracteres (OCR), y en un formato que permita su tratamiento automático, tal como buscar, copiar y extraer información.
- Codificar los documentos una vez escaneados mediante programas de reconocimiento de caracteres, digitalización de imágenes y vectorialización de gráficos, para obtener un fichero que pueda ser manipulado por cualquier editor de textos, imágenes o gráficos.
- Cambiar el formato de los documentos escaneados una vez codificados por otro más estandarizado o de mayor perdurabilidad.

NIVELES DE SEGURIDAD:

- En función de los datos de carácter personal contenidos en el documento le son aplicables las medidas de nivel básico, medio o alto contempladas en el RD 994/1999, artículo 4 'Aplicación de los niveles de seguridad'.
- Cabe establecer los niveles de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento '*Criterios de seguridad*' el capítulo '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

- Guía de la información electrónica (DLM Forum)
  http://europa.eu.int/historical_archives/dlm_forum/index_en.htm

Gestión de la información en soporte electrónico

CONCEPTOS:

Se considera información de gestión aquella que no ha sido traspasada a otros archivos, centrales o históricos, en función de la normativa de gestión documental aplicable.

La ***compactación*** es el proceso mediante el cual se eliminan aquellos datos no esenciales de la aplicación. Es un proceso que se ejecuta con el fin de ahorrar espacio de almacenamiento. La información compactada puede mantenerse en el equipo o bien puede ser salvada y eliminada del mismo.

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Guardar el principio de unidad del expediente, cuyo inicio y resolución se lleva a cabo en el organismo que tiene la competencia sobre su formación. (RD 263/1996, art. 2.2)
- Designar el organismo gestor de la información electrónica cuando haya varios organismos involucrados. (RD 263/1996, art. 2.2)

CRITERIOS:

3.8 Se debe conservar y preservar la fiabilidad, autenticidad, integridad de la información electrónica durante la vida del documento, y transferir la responsabilidad de su gestión al final de la parte activa de su ciclo de vida.

3.9 Se debe clasificar la información mediante un sistema de codificación comprensible y claro.

RECOMENDACIONES:

Con carácter general:

- Mantener un archivo de oficina para la gestión de la información en soporte electrónico.
- Registrar, y transferir, la información de los expedientes en un soporte único, papel o electrónico, pero no en ambos a la vez (preferentemente electrónico).
- Transferir la responsabilidad de la gestión de la información a otro archivo (Archivo Central) al final de la parte activa de su ciclo de vida, en función de la frecuencia de utilización y los plazos de prescripción.

En relación con la compactación de la información:

- Cuando no sea posible que el servidor de la aplicación pueda mantener los datos de gestión activamente, se aplicará un proceso de compactación que deberá permitir eliminar del soporte de almacenamiento, con una periodicidad determinada, aquellos datos que no sean utilizados para el ejercicio de potestades.
- En el caso de que los datos compactados sean a su vez salvados a otro soporte de almacenamiento, y a continuación sean eliminados del soporte de gestión, existirá otro proceso que permita reincorporar los datos compactados de forma que sean legibles por la aplicación o por otra aplicación sustitutiva.

- Los datos compactados se mantendrán accesibles a los usuarios de la aplicación hasta que dicha información adquiera el carácter de histórica en función de la normativa aplicable. La información que pertenezca a expedientes activos, no archivados, no estará sujeta al proceso de compactación.

Cambios de versiones, sistemas operativos o aplicaciones:

- Cuando la aplicación sea sustituida por una nueva aplicación, se aplicarán los procesos necesarios para incorporar toda la información existente hasta ese momento a su nuevo formato.
- Si la aplicación deja de utilizarse y su funcionalidad no es sustituida por una nueva aplicación se estará en alguno de los dos siguientes casos:
  - Si el mantenimiento de los soportes y medios que ejecutan dicha aplicación se encuentra garantizado en el plazo en el que los datos deben ser conservados, tanto la aplicación como los soportes se mantendrán, así como la documentación necesaria para la explotación del sistema.
  - Si el mantenimiento no se encuentra garantizado, entonces, al menos, los datos básicos de la aplicación de carácter no histórico se traspasarán a un nuevo formato cuya durabilidad se encuentre garantizada. Para evitar situaciones de este tipo deben ser traspasados previamente todos los datos a un formato normalizado.

NIVELES DE SEGURIDAD:

- En función de los datos personales de los ciudadanos contenidos en la información le son aplicables del R.D. 994/1999, las medidas de seguridad requeridos por artículo 4 'Aplicación de los niveles de seguridad', y el articulo 7 'Ficheros temporales'.
- Cabe establecer los niveles de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento '*Criterios de seguridad*' el capítulo '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

- Normativa sectorial de especial interés: Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
- Guía de la información electrónica (DLM Forum)
  http://europa.eu.int/historical_archives/dlm_forum/index_en.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).

Traspaso de la información al archivo

MARCO LEGAL:

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

- Cancelar los datos de carácter personal que ya no son necesarios ni conservar datos que ayuden a identificar al interesado, a menos que un procedimiento determinado reglamentariamente permita

conservar determinados datos de valor histórico, estadístico o científico. (LO 15/1999, arts. 4.5 y 20.3)

- Transferir a otro archivo la documentación que conserva valor administrativo al mismo tiempo que se hace la entrega física de los soportes de información electrónica. (LO 15/1999, art. 21.1)

CRITERIOS:

3.10 Se deben traspasar documentos electrónicos completos, auténticos y fiables, al Archivo central al finalizar la etapa activa de su ciclo de vida, y al mismo tiempo eliminar aquellos documentos que carecen de utilidad o valor administrativo.

RECOMENDACIONES:

- Eliminar la información que carece de valor administrativo con la ayuda de las normas establecidas por el archivo.
- Hacer copias de los ficheros y de las bases de datos, verificar la consistencia de la información, documentar los errores de los ficheros y de los documentos.
- Abrir los documentos poseedores de una firma electrónica o cifrados, para acceso público antes de transferirlos al Archivo central.
- Comprobar que toda la información, y su contexto, está completa, documentada, y es conforme a los procedimientos y requisitos de conservación establecidos por el Archivo al que se transfiere.
- No preservar la operatividad de las firmas electrónicas, ya que la documentación y los procedimientos de transferencia al Archivo central garantizan la autenticidad de los datos.
- Asegurarse de que se almacena en un formato normalizado internacional libre de patentes y *royalties*.

NIVELES DE SEGURIDAD:

- En función de los tipos de datos personales de los ciudadanos, contenidos en la información, le es aplicable del R.D. 994/1999, el artículo 7 'Ficheros temporales', y las medidas de seguridad de nivel medio establecidas en los artículos 17, 18, 19 y 20 para aquellos otros que conservan valor histórico, estadístico o científico, y que todavía contengan datos que permitan obtener una evaluación de la personalidad del individuo.
- Cabe asimismo establecer los niveles de medidas de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento *'Criterios de seguridad'* el capítulo '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

- Guía de la información electrónica (DLM Forum)
  http://europa.eu.int/historical_archives/dlm_forum/index_en.htm
- *Keeping Electronic Records, Policy for electronic recordkeeping in the Commonwealth Government, Australian Archives.*

EJEMPLO DE SOLUCIÓN:

- Una forma de tratar la transferencia de series documentales entre archivos puede hacerse de acuerdo a las siguientes pautas:
  - Contactar con el archivo al que se van a transferir las series documentales, al objeto de conocer sus normas, procedimientos y requisitos de transferencia.

- Preparar la información de los documentos que se van a transferir.
- Revisar todos los expedientes a transferir y comprobar que no falta ningún documento.
- Reclamar los documentos que faltan en el expediente a las personas responsables de su salida.
- Identificar y documentar los errores encontrados en la revisión de la documentación.
- Identificar y documentar el contenido de los soportes con los documentos que se transfieren.
- Confeccionar una relación de entrega para controlar las series documentales que pasan al otro archivo.

Acceso y difusión a la información de soporte electrónico

CONSIDERACIONES:

Hay varias maneras de permitir a los usuarios interesados el acceso a la información electrónica, entre ellas:

- Acceso en el sitio, en sala de lectura electrónica en la que se facilita al usuario los medios y aplicaciones.
- Acceso en línea, mediante un sistema que proporcione la visión automática de la información.

En ambos casos se suele proporcionar al usuario una copia de consulta, un documento sin modificación alguna, o bien un documento adaptado y transformado a un nuevo formato.

Hay varias formas de poner en práctica una política de difusión de la información electrónica, entre ellas:

- Difusión activa, enviando determinada información a un grupo seleccionado de usuarios.
- Difusión pasiva, dejando al usuario la iniciativa de localizar la información a través de herramientas de navegación en línea.

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Utilizar protocolos que garanticen la disponibilidad y acceso a la información, y permitan la compatibilidad de la transmisión y recepción de las comunicaciones. (RD 263/1996, art. 7.1 a, b)
- Utilizar la relación pública de aplicaciones, protocolos, soportes y formatos de ficheros normalizados que permitan la comunicación y acceso a la información. (RD 263/1996, art. 10.1)

En relación con los derechos del ciudadano de acceso a archivos y registros administrativos:

- Los ciudadanos tienen derecho a acceder a los registros y a los documentos que obren en los archivos administrativos, cualquiera que sea la forma de expresión gráfica, sonora o en imagen o en el tipo de soporte material en que figuren, en las condiciones en las condiciones que se establecen (expedientes terminados, interés legítimo y directo, otras específicas) (Ley 30/1992, art. 45.2)

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

- Facilitar el derecho de acceso a la información de las personas interesadas. (LO 15/1999, art. 15.1)

- Proporcionar la información mediante consulta, visualización o indicación de los datos. (LO 15/1999, art. 15.2)

CRITERIOS:

3.11 Se deben adoptar las prácticas que mejor se adapten a la difusión de la información, y facilitar que esta sea accesible al mayor número de personas, dentro del ámbito de la Administración y entre ésta y los particulares.

3.12 Cuando se pongan los documentos administrativos a disposición del ciudadano debe utilizarse un formato o formatos tales que puedan ser accedidos desde diversos productos alternativos. A este fin son de referencia los formatos incluidos en el capítulo *'Formato de la información en soporte electrónico*'.

RECOMENDACIONES:

Protocolos, soportes y formatos recomendados para facilitar el acceso y difusión de la información:

- 1.- Soportes magnéticos para distribución de información:
  - Disquete de 3 1/2".
  - CD-ROM y DVD.
- 2.- Protocolos Internet para comunicación e intercambio de documentos:
  - HTTP para páginas hipertexto.
  - FTP para ficheros.
- 3.- Formatos de documentos:
  - XML para definir documentos independientes de la plataforma.
  - HTML para páginas Web y documentos breves.
  - PDF para visualización de documentos.
- 4.- Formatos de bases de datos:
  - SQL2 para consulta de bases de datos relacionales.
  - ISAM para almacenamiento de ficheros secuenciales indexados.

NIVELES DE SEGURIDAD:

- En función de los tipos de datos personales de los ciudadanos, contenidos en la información, le es aplicable del RD 994/1999 los artículos relativos a la identificación y autenticación, y al control de acceso: artículos 11 y 12 para medidas de seguridad de nivel básico; artículos 18 y 19 para medidas de seguridad de nivel medio y el artículo 24 'Registro de acceso' para medidas de seguridad de nivel alto.
- Cabe establecer los niveles de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento '*Criterios de seguridad*' el capítulo '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

- Normativa sectorial de especial interés: Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

- Guía de la información electrónica (DLM Forum) http://europa.eu.int/historical_archives/dlm_forum/index_en.htm
- UK e-GIF (*e-government interoperability framework*), http://www.e-envoy.gov.uk/Home/Homepage/fs/en
- http://www.docbook.org/
- http://www.oasis-open.org/committees/docbook/

4 Formato de la información en soporte electrónico

CONSIDERACIONES:

El criterio de selección de formatos de fichero normalizados y perdurables, requiere hacer por cada tipo de fichero las siguientes consideraciones:

- *Ficheros de texto*, la elección del tipo de fichero es distinta dependiendo de su utilización, si los documentos se distribuyen sólo para consulta o lectura, o si después serán manipulados con procesadores de texto. Los ficheros de texto también son distintos si conservan la estructura y la presentación. El texto es un conjunto de caracteres: letras; números y símbolos que forman palabras o sentencias. La estructura es el texto ordenado en capítulos y títulos, con índice y tabla de ilustraciones, y la presentación es el texto en negrita, cursiva o subrayados.
- *Ficheros de datos*, al no existir un formato normalizado de fichero, y para poder leer los datos después de un largo período de tiempo, se requiere disponer de una herramienta capaz de leer el formato antiguo o bien conservar el programa que los generó.
- *Ficheros gráficos*, la elección del tipo de fichero depende de la calidad de cada formato, es decir de la relación entre el número de bits por pixel y número de colores que soporta el formato, y también de la perdida o no de información relevante después de su compresión, dando lugar a relaciones de compresión más altas dependiendo del grado de deterioro que puede aceptarse de una imagen.
- *Ficheros de vídeo y audio*, en la medida de lo posible conviene recurrir a especificaciones públicas y libres *royalties* y de patentes.

Tipos de formatos de ficheros

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Publicar la relación de las aplicaciones, medios y soportes a través de los cuales se podrán efectuar las comunicaciones y notificaciones con los particulares, especificando en su caso los formatos y códigos normalizados para su utilización. (RD 263/1996, art. 10.1,2)
- Los Departamentos y entidades mantendrán permanentemente actualizada y a disposición de los ciudadanos la relación de aplicaciones, medios y soportes a que se refiere el apartado anterior. (RD 263/1996, art. 10.1,2)

CRITERIOS:

4.1 Se debe seleccionar un conjunto común de estándares de formato de fichero: gráfico, texto, datos, audio y vídeo que faciliten el acceso y circulación de la información, y su posterior recuperación y conservación.

RECOMENDACIONES:

- En el caso de aquellos formatos para los que no existe una norma: se generarán las especificaciones que son requeridas para la representación de la información para ser presentadas a una entidad de certificación/normalización (AENOR).
- Utilizar un formato texto que conserve la estructura del fichero, puesto que con estructura el fichero es independiente del equipo y de fácil manejo, mientras que sin estructura el fichero es una secuencia de caracteres difícil de manejar.
- Utilizar aquellos formatos de datos y programas para los que en la medida se disponga de especificaciones públicas y libres de *royalties* y patentes.
- Utilizar un formato de gráficos cuya relación calidad y pérdida de información sea menos relevante en relación al mayor grado de compresión obtenido.
- Utilizar el formato de audio y vídeo que en la medida de lo posible sean especificaciones públicas y libres de royalties y patentes.
- Los formatos de fichero recomendados como propuesta ideal figuran en **negrita** y *cursiva* en cada uno de los siguientes tipos:
- 1.- Formatos de texto:
  - ***TXT:*** formato simple que permite su lectura a cualquiera.
  - ***PDF***: permite visualizar documentos reproduciendo todas las características del original en ficheros de menor tamaño, independientes de la aplicación y plataformas, su especificación es pública y también se encuentra extendido para la distribución y difusión formal de documentos y para su acceso y visualización.
  - **RTF**: formato que constituye un mínimo común entre procesadores de texto diferentes.
  - **SGML**: norma internacional ISO 8879, del mundo editorial, que almacena el texto y su estructura, pero no tiene atributos de presentación; actualmente está siendo reemplazado por XML y HTML.
  - ***XML:*** dialecto del SGML adecuado para definir documentos independientes de la plataforma y procesarlos de forma automática pues distingue entre estructura, contenido y presentación, ofreciendo mayores posibilidades que HTML.
  - ***HTML:*** versión simplificada del SGML que se utiliza en los servidores web, muy útil para la difusión de información.
  - ***SXW***: formato de los documentos de texto manejados por el software libre openoffice.org.
  - Encapsulated PostScript: utilizado para enviar e imprimir documentos junto con su presentación, de forma que se asegure que la salida impresa es correcta con independencia del dispositivo utilizado.
  - Especificación CSV para el intercambio de tablas, delimitadas por comas.
- 2.- Formatos de datos estructurados:

- ***XML:*** dialecto del SGML adecuado para definir documentos independientes de la plataforma y procesarlos de forma automática pues distingue entre estructura, contenido y presentación, ofreciendo mayores posibilidades que HTML.
- ***Bases de Datos***: Usar bases de datos relacionales conformes con las normas internacionales sobre SQL, ANSI X3.135-1992/ISO 9075:1992.
- ***MIME*** : para mensajes de correo electrónico e intercambio electrónico de datos y ficheros adjuntos.
- Formularios, sólo es posible conservar información y datos, junto con una copia del formulario en blanco.

- 3.- Formatos Gráficos:
- *Gráficos de Mapa de Puntos*, imagen constituida por puntos y utilizada para posteriores codificaciones.
  - ***JPEG***, ISO 10918. Hay que tener en cuenta que es destructivo con un nivel de compresión alto, por lo que se debe comprobar que la perdida de imagen es aceptable. Soporta 16,7 millones de colores (24 bits por pixel).
  - ***TIF***, utilizado en ficheros generados por escáneres con varias posibilidades según el número de colores elegido: blanco y negro; escala de grises y color. No es destructivo pero de nivel de compresión bajo.
  - ***PNG***, con características similares e incluso superiores a GIF, está libre de *royalties* y patentes. Soporta 16,7 millones de colores y se puede utilizar sin necesidad de licencias de software.
  - ***FAX***, formatos de ficheros fax: Grupo III y Grupo IV según el tipo de la línea telefónica usada: normal y RDSI.
  - Otros formatos gráficos, propietarios como el BMP, PCX o Kodak Photo CD, cuya durabilidad no está garantizada a largo plazo.
- *Gráficos Vectoriales*, gráfico que conserva las coordenadas de los vectores que lo componen, y es utilizado en la digitalización de planos.
  - ***CGM***, formato para gráficos 2D, imágenes combinadas raster y vectoriales.
  - ***VML***, *Vector Markup Language*.
- 4.- Formatos comprimidos:
  - Especificación ZIP 2.0 para el intercambio de datos comprimidos.

NIVELES DE SEGURIDAD:

- En función de los datos de carácter personal contenidos en el documento le son aplicables las medidas de nivel básico, medio o alto contempladas en el RD 994/1999, artículo 4 'Aplicación de los niveles de seguridad'.
- Cabe establecer los niveles de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento '*Criterios de seguridad*' el capítulo '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

- *International Standards Organization* http://www.iso.ch
- *World Wide Web Consortium* http://www.w3c.org
- *Internet Engineering Task Force* http://www.ietf.org
- *European Association for Standardizing Information and Communication Systems* http://www.ecma.org
- *American National Standards Institute* http://www.ansi.org
- *Unicode Consortium* http://www.unicode.org
- Guía de la información electrónica (DLM Forum) http://europa.eu.int/historical_archives/dlm_forum/index_en.htm.
- *IDA Architecture Guidelines, Part II, 3. Service profiles,* http://europa.eu.int/idabc/en/document/3485/5585
- http://www.w3.org/Graphics/PNG/

Juego de caracteres

MARCO LEGAL:

- La protección y garantía de las *distintas modalidades lingüísticas de España* se recoge en el Título I de la **Constitución** "*De los derechos y deberes fundamentales*", como en el Título VIII *"De la Organización Territorial del Estado"*. Los artículos 3 y 46 de la **Constitución** encomiendan a los poderes públicos que garanticen la protección y conservación de las *distintas modalidades lingüísticas de España* como patrimonio cultural de nuestro país. A su vez el artículo 149 de la norma fundamental en su apartado 2 configura como deber y atribución del Estado el servicio de la cultura.
- El **Real Decreto 564/1993, de 16 de abril**, sobre presencia de la letra *"ñ"* y demás caracteres específicos del idioma castellano en los teclados de determinados aparatos de funcionamiento mecánico, eléctrico o electrónico que se utilicen para la escritura (BOE 23/04/1993), en su artículo único dispone lo siguiente:

  "Todos los aparatos de funcionamiento mecánico, eléctrico o electrónico, que se utilicen para la escritura, grabación, impresión, retransmisión de información y transmisión de datos, y que se vendan en España, deberán incorporar la letra <<ñ>> y los signos de apertura de interrogación y de exclamación."

CRITERIOS:

4.2 Se deben seleccionar los medios, equipos o sistemas, que permitan la utilización de todos los caracteres gráficos empleados por las distintas lenguas de España.

4.3 Se debe utilizar bien el juego de 191 caracteres gráficos del alfabeto latino nº1 codificados sobre un octeto, según la norma ISO 8859-1 o bien el juego de caracteres codificados multi-octeto, según la norma ISO 10646 (ISO/IEC 10646:1:2000 /Unicode v3.0 in UTF-8 / UTF-16), de forma que ambas permiten satisfacer las necesidades del Castellano, Catalán, Euskera y Gallego, así como las variantes de estas lenguas

4.4 Debe haber presencia de la letra "ñ", símbolo de euro, y signos de apertura y cierre de admiración y exclamación en los teclados de los distintos tipos de equipos utilizados.

AMPLIACIÓN TÉCNICA:

- Guía de la información electrónica (DLM Forum) http://europa.eu.int/historical_archives/dlm_forum/index_en.htm
- *IDA Architecture Guidelines, Part II, 3. Service profiles,* http://europa.eu.int/ida/en/document/2317/
- CIABSI, cláusula tipo de juego de caracteres, http://www.csi.map.es/csi/silice/Ctciabsi32.html

EJEMPLO DE SOLUCIÓN:

Cláusula de la CIABSI sobre juegos de caracteres: “Los juegos de caracteres de los equipos físicos y lógicos ofrecidos para dar cumplimiento al objeto de contrato, deberán ser conformes con la norma ISO 8859-1: "Tratamiento de la información. Juego de caracteres gráficos codificados sobre un sólo octeto. Parte 1: Alfabeto latino nº 1", además, en el caso de los equipos lógicos, los juegos de caracteres deberán incorporar el símbolo de la moneda única europea (euro).”

5 Soportes

Tipos de soportes de almacenamiento de la información

CONCEPTOS:

Soporte: objeto sobre el cual o en el cual es posible grabar y recuperar datos.

Los elementos clave en relación con la conservación de los soportes son la accesibilidad, la legibilidad, la perdurabilidad y la preservación de la autenticidad.

CONSIDERACIONES:

A la hora de afrontar la conservación de la información en soporte electrónico se deben tener presentes los siguientes aspectos y características de los soportes:

- *Los soportes de almacenamiento magnético* utilizados habitualmente como *backup*, a corto, medio e incluso largo plazo, sólo permiten un acceso secuencial a la información y aunque pueden llegar a tener una capacidad significativa de almacenamiento, se debe tener en cuenta que pueden ser modificados o borrados.
- *El almacenamiento magnético de tipo “storage”* obviamente necesita *backup* e igualmente puede ser modificado o borrado.
- *Los soportes de almacenamiento óptico* de tipo única escritura múltiple lectura, no modificables por tanto, permiten satisfacer requisitos de archivo, constituyen un soporte longevo a medio y largo plazo, tienen gran capacidad de almacenamiento y permiten el acceso directo a la información.
- El *microfilm*, que no es un soporte electrónico, no permite modificaciones y la búsqueda de la información resulta complicada. Se ha de tener en cuenta que dependiendo de la calidad del material utilizado pueden surgir incertidumbres sobre su duración a largo plazo.

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Las especificaciones técnicas de los soportes, medios y aplicaciones utilizados en el ámbito de la Administración General del Estado en sus relaciones externas y cuando afecten a derechos e intereses de los ciudadanos deberán ser conformes, en su caso, a las normas nacionales e internacionales que sean exigibles. (RD 263/1996, art. 4.4)
- Publicar la relación de las aplicaciones, medios y soportes a través de los cuales se podrán efectuar las comunicaciones y notificaciones con los particulares. (RD 263/1996, art. 10.1)

CRITERIOS:

5.1 Se debe almacenar la información en un soporte normalizado y perdurable, el que sea más adecuado a las necesidades de conservación a corto, medio o largo plazo.

5.2 Para el almacenamiento de documentos administrativos en condiciones que permitan garantizar su conservación, integridad y calidad se deben utilizar los soportes ópticos no reescribibles, como es el caso de los **CD-R** y **DVD-R** del tipo WORM (múltiple lectura única escritura), dado que estos soportes duran muchos más años y no se ven afectados por el número de veces que se lean; también se conocen en el mercado como "*soportes no repudiables*".

RECOMENDACIONES:

- En relación con la conservación de los soportes cabe exigir a los fabricantes:
  - El cumplimiento de las normas de fabricación.
  - Un manual claro de conservación y de protección física de los diversos soportes.
  - Certificados de durabilidad de los soportes, comprobando que garanticen la duración de la salvaguardia en los plazos que la legislación haya determinado.
- Que para los soportes se especifique:
  - Tiempo medio de funcionamiento entre fallos.
  - Vida útil de la unidad.
  - Vida útil de las unidades grabadas.

La tabla siguiente contiene un resumen de tipos de soportes con sus características de capacidad, condiciones ambientales y plazo de almacenamiento recomendados junto con otras consideraciones. Se señalan en negrilla los soportes que deben utilizarse para la conservación de la información.

1.Soportes Magnéticos	Capacidad	Condiciones Ambientales	Plazo Almacén	Consideraciones
Disquete 3 ½	1,44 a 120 MB	5º a 32º C y 20% a 60% HR	2 a 5 años	Regrabable +1.000 veces Norma ISO/IEC 9529
Cinta Magnética 1.600 bpi		5º a 45º C y 20% a 80% HR	5 a 10 años	Regrabable + 1.000 veces Reescribir cada 10 años Rebobinar cada 2 años Norma ISO/IEC 3788
Cinta Magnética 6.350 bpi	112,5 GB			
Cartucho 1/2" y 1/4"	80 MB / 2 GB	5º a 32º C y 20% a 80% HR	5 a 10 años	Regrabable +1.000 veces Reescribir cada 10 años Rebobinar cada 2 años. Norma ISO 8462
Cinta DAT de 4mm.	2 a 24 GB	5º a 32º C y 20% a 60% HR.	5 a 10 años	Regrabable + 1.000 veces Reescribir cada 10 años Rebobinar cada 2 años Normas ISO/IEC 11319 y 12246
Cinta de 8mm	3,5 a 25 GB			
2. Soportes Ópticos	**Capacidad**	**Condiciones Ambientales**	**Plazo Almacén**	**Consideraciones**
CD-ROM, **CD-R** y CD-RW	0,65 GB	-5º a + 30º C y 5% a 60% HR	10 a 20 años	Regrabable (RW) + 1.000 veces Reescribir cada 10 años Normas ISO/IEC 9660 y 1014
DVD-ROM DVD-RAM **DVD-R** y DVD_RW	4,7 a 18 GB 4,7 a 9,4 GB 4,7 GB	-10ª a 50º C 3% a 85% HR		Regrabable (RW) + 100 veces Reescribir cada 10 años Normas ISO/IEC 16824
3. Soporte Microfilm	**Capacidad**	**Condiciones Ambientales**	**Plazo Almacén**	**Consideraciones**
Micro film: Poliéster y Halógeno de plata		17º C 20% a 30% HR	100 años	Más estable que el papel e independiente de la obsolescencia tecnológica de sistemas y aplicaciones. Normas ISO 6199, 10602

4. Condiciones Ambientales de Conservación		
Soporte	Temperatura	Humedad Relativa
Papel	17º C +/- 1º C.	52% +/- 3%
Microfilm:		
- Película Nitrato	- 20º C hasta 2º C +/- 1º C	30% +/- 3%
- Película Poliester	- 20º C hasta 17º C +/- 1º C	20% hasta 30% +/- 3%
Electromagnético	+ 2ºC hasta 18º C +/- 1º C	40% +/- 2%
Óptico	+ 2ºC hasta 18º C +/- 1º C	40% hasta 55% +/- 2%

NIVELES DE SEGURIDAD:

- En función de los tipos de datos personales de los ciudadanos contenidos en los soportes es aplicable del RD 994/1999 la gestión de soportes: artículo 13 para medidas de seguridad de nivel básico y artículo 20 para medidas de seguridad de nivel medio y alto.
- Cabe establecer los niveles de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento '*Criterios de seguridad*' el capítulo '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

- Guía de la información electrónica (DLM Forum)
  http://europa.eu.int/historical_archives/dlm_forum/index_en.htm

6 Medidas de almacenamiento y conservación

Reescritura de los archivos en soporte electrónico

CONSIDERACIONES:

El volver a grabar la información de los soportes electrónicos, a pesar de su coste añadido, permite resolver muchos problemas derivados de los soportes no normalizados, que son la mayor parte de los soportes magnético - ópticos. Durante cada reescritura se debe tener en cuenta medidas técnicas de perdurabilidad y preservación que aseguren la accesibilidad, legibilidad y la autenticidad de los archivos electrónicos.

Si la aplicación genera datos en un formato propietario, existen varias soluciones para conservar los datos a largo plazo, como es el caso de conservar el sistema completo para poder acceder a la información o migrar ésta a un formato estandarizado, aunque el coste de conversión de la información electrónica a un nuevo formato sea elevado, ya que el no hacerlo puede tener un coste aún más importante.

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Medidas que garanticen la conservación de la información en el marco del principio de proporcionalidad. (RD 263/1996, art. 4.2)
- Los medios o soportes en que se almacenen documentos deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos. (RD 263/1996, art. 8.4)

CRITERIOS:

6.1 Se deben realizar grabaciones periódicas de los archivos electrónicos, teniendo en cuenta la duración de los soportes y la evolución de su tecnología, ya sea reutilizando los mismos soportes o migrando hacia otros más modernos.

6.2 Se deben convertir los ficheros antiguos, creados con aplicaciones propietarias, a formatos que corresponden a especificaciones abiertas libres de patentes y *royalties*.

RECOMENDACIONES:

- Preservar la información de soporte electrónico volviendo a grabar los soportes magnéticos y ópticos según los plazos recomendados para los distintos tipos de soportes (véase el capítulo '*Soportes*').
- Se recomienda migrar hacia un soporte más moderno una vez cumplido su plazo de vida útil.

NIVELES DE SEGURIDAD:

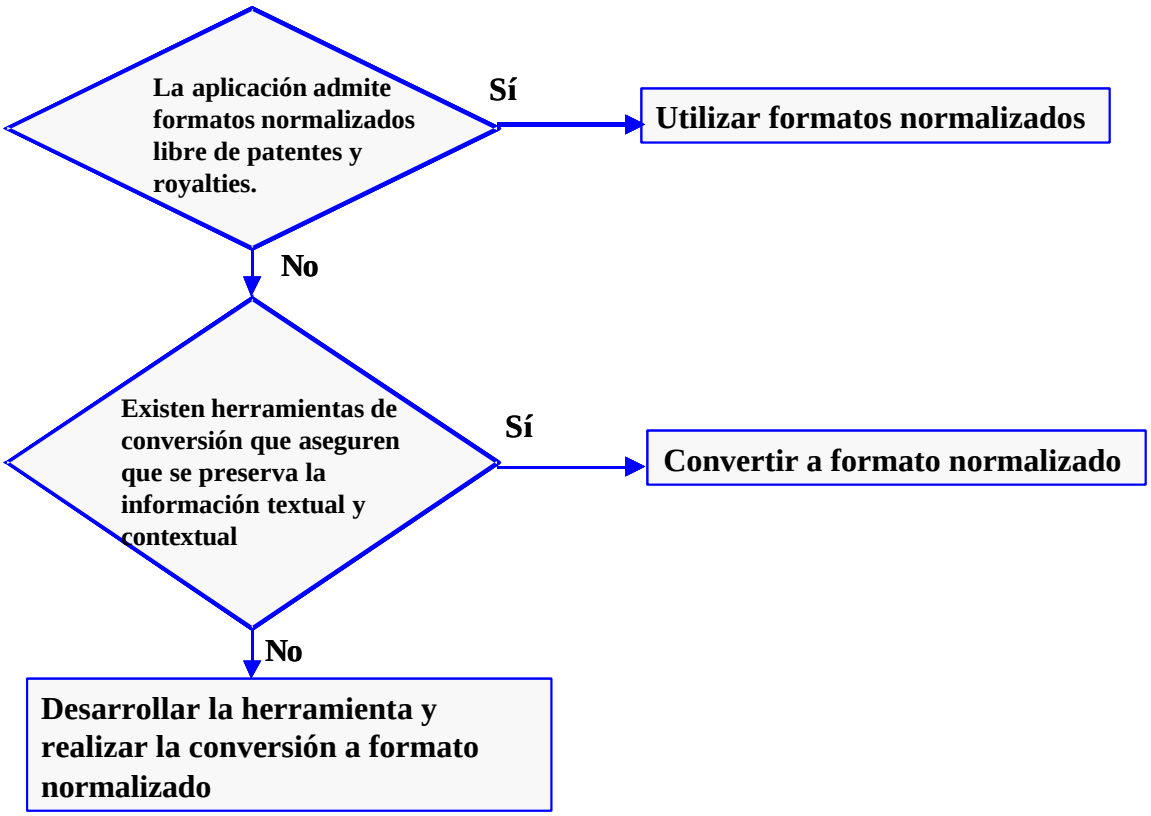
- En función de los tipos de datos personales de los ciudadanos, contenidos en los soportes, le es aplicable del RD 994/1999, la gestión de soportes y la recuperación de datos: artículos 13 y 14 para medidas de seguridad de nivel básico y artículos 20 y 25 para medidas de seguridad de nivel medio y alto.
- Cabe asimismo establecer los niveles de medidas de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento *'Criterios de seguridad'* el capítulo '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

- Guía de la Información Electrónica (DLM Forum)
  http://europa.eu.int/historical_archives/dlm_forum/index_en.htm

EJEMPLO DE SOLUCIÓN:

Opciones de conversión o conservación de formatos propietarios:



Protección contra el deterioro físico

CONSIDERACIONES:

Existen diversos factores que afectan al deterioro físico de los soportes, tal es el caso de los campos eléctricos y magnéticos, la oxidación y degradación de los materiales con los que están hechos.

Seleccionar un sistema de almacenamiento de la información y las copias de seguridad no es una cuestión simple. Por ejemplo, las unidades de cinta magnética han sido la solución tradicional, pero ahora han irrumpido en el mercado las unidades ópticas, con un coste menor y una vida útil más prolongada, aunque pueden tener el inconveniente de que su velocidad de transferencia de datos sea lenta.

MARCO LEGAL:

En relación con las aplicaciones para el ejercicio de potestades:

- Establecer un procedimiento de protección del archivo de soportes electrónicos. Conservación de la información en el marco del principio de proporcionalidad. (RD 263/1996, arts. 4.2 y 8.4)
- Los medios o soportes en que se almacenen documentos deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos. (RD 263/1996, art. 8.4)

CRITERIOS:

6.3 Se deben realizar controles periódicos del archivo de soportes electrónicos para protegerlos del deterioro físico.

6.4 Se debe disponer de segundas copias del archivo de soportes electrónicos.

RECOMENDACIONES:

Entre los procedimientos de protección contra el deterioro físico de los soportes electrónicos figuran los siguientes:

- Procedimientos de protección:
  - Detallar la forma de protección contra el deterioro físico del contenido de la biblioteca de soportes.
  - Determinar la frecuencia de tiempo con que se realizarán copias de respaldo y recuperación.
  - Determinar la migración de soportes en función de su vida útil.
  - Definir la manera de inventariar periódicamente los contenidos de la biblioteca de soportes.
  - Mantener y verificar el inventario de los soportes.
  - Especificar los plazos de tiempo de conservación de los soportes, su puesta fuera de servicio y el borrado de ficheros.
- Identificación y control de soportes:
  - Identificar los soportes por su nombre, fecha de creación, durabilidad y período de retención.
  - Identificar y controlar la duración de los equipos y soportes.
  - Mantener registros de entrada / salida de los soportes recibidos y enviados.
  - Determinar el modo en que debe realizarse el traslado de los soportes.
  - Autorizar, por su responsable, la salida de soportes fuera de los locales en que están ubicados.
  - Impedir cualquier recuperación de la información almacenada en los soportes posterior a su baja en el inventario o a consecuencia de su salida fuera de los locales en que están ubicados.
- Control de los cambios.
  - Proteger los soportes de cambios no autorizados.
  - Documentar y justificar la necesidad del cambio.
  - Evaluar las consecuencias del cambio.
  - Aprobar, implantar y verificar la realización de los cambios.
- Seguir la evolución y los cambios que puedan afectar a la aplicación y la plataforma

NIVELES DE SEGURIDAD:

- En función de los tipos de datos personales de los ciudadanos, contenidos en los soportes, le es aplicable del RD 994/1999, la gestión de soportes y la recuperación de datos: artículos 13 y 14 para

medidas de seguridad de nivel básico y artículos 20 y 25 para medidas de seguridad de nivel medio y alto.

- Cabe asimismo establecer los niveles de medidas de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento *'Criterios de seguridad'* el capítulo '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT). http://www.csi.map.es/csi/pg5m20.htm
- Guía de seguridad informática (SEDISI), punto 3.6 'Medios de almacenamiento'. http://www.sedisi.es/05_Estudios/05_general.htm - seg

Seguridad de la información

CONSIDERACIONES:

Mediante procedimientos de seguridad, los soportes y dispositivos de almacenamiento se controlan y protegen contra daño, robo, acceso no autorizado, revelación de contenido y mal uso. Estos procedimientos, siguiendo el principio de proporcionalidad, buscan un equilibrio entre la naturaleza de la información y los riesgos a los que se encuentra expuesta, especialmente provenientes de amenazas deliberadas de origen humano.

Los criterios de conservación de soportes, su custodia y accesibilidad, están incluidos en los planes de seguridad y contingencia.

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, 4.3)
- Los medios o soportes en que se almacenen documentos deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos. (RD 263/1996, art. 8.4)

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. (LO 15/1999, art. 9.1)

CRITERIOS:

6.5 Se deben 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.

6.6 Se deben aplicar procedimientos en relación con las siguientes cuestiones: biblioteca de soportes, gestión de soportes removibles, manipulación de datos de datos de carácter personal y eliminación de soportes, tales como los siguientes.

- Biblioteca de soportes:
  - Ubicar la biblioteca de soportes en un área cuyo entorno tenga condiciones físicas de seguridad y restricción de acceso al personal autorizado.
  - Asignar responsabilidades a personas concretas para la gestión de la biblioteca de soportes.
  - Utilizar otras instalaciones distintas para almacenar copias de seguridad.
- Gestión de soportes removibles:
  - Documentar todos los procedimientos y niveles de autorización: quién tiene acceso a qué soportes.
  - Retirar los soportes con autorización escrita y mantener su registro y trazabilidad: registro de salida.
  - Evitar identificar los datos almacenados a partir de la etiqueta del soporte.
  - Reutilizar y retirar los soportes eliminando sus contenidos con diferentes patrones de borrado.
  - Realizar *in situ* reparaciones de medios, equipos y sistemas, para evitar el riesgo de fuga de datos.
- Manipulación de datos de carácter personal:
  - Documentar la manipulación y esquema de etiquetado de todos los soportes.
  - Mantener un registro actualizado con la lista de personas autorizadas.
  - Controlar los datos, acusar recibo y marcar las copias remitidas a los receptores autorizados.
  - Registrar las operaciones de creación, modificación y borrado, para su trazabilidad.
  - Realizar auditorías periódicas para determinar el grado de cumplimiento de los procedimientos.
  - Cifrar la información de carácter sensible, requisito de confidencialidad.
  - Firmar y fechar digitalmente la información sensible, requisito de autenticidad.
  - Ubicar de forma segura los soportes; disponer de una caja de seguridad para el almacenamiento de los soportes.
- Documentación del sistema de conservación:
  - Establecer controles para proteger al sistema de accesos no autorizados.
  - Ubicar físicamente la documentación en armarios robustos.
  - Almacenar la documentación separada de los ficheros de aplicaciones y programas.
  - Proteger la documentación asignándole el adecuado nivel de acceso.
- Eliminación de soportes:

- Eliminar los soportes que contengan información de carácter sensible, o borrar sus datos para su reutilización. Destruir mediante trituradoras o medios similares los impresos y el papel.
- Identificar los soportes que deban destruirse de forma segura, tales como fax, telex, papel carbón, cintas, discos removibles, casetes, listados de programas, datos de prueba y documentos del sistema.
- Encomendar la destrucción de soportes a organizaciones especializadas, seleccionándolas por su experiencia y condiciones de control de seguridad.
- Llevar un registro de la destrucción de soportes con información sensible, a efectos de auditoría.
- Evitar la acumulación de gran cantidad de información sensible para su destrucción.

RECOMENDACIONES:

- Realizar el seguimiento del estado de la tecnología y de los costes de la seguridad y de las salvaguardas.

NIVELES DE SEGURIDAD:

- En función de los tipos de datos personales de los ciudadanos, contenidos en los soportes, le son aplicables del RD 994/1999, los artículos relativos a las medidas de seguridad: nivel básico, nivel medio y nivel alto.
- Cabe establecer los niveles de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento '*Criterios de seguridad*' el capítulo '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT), http://www.csi.map.es/csi/pg5m20.htm.
- Guía de la información electrónica (DLM Forum) http://europa.eu.int/historical_archives/dlm_forum/index_en.htm

Software libre y de fuentes abiertas

CONSIDERACIONES:

Desde el punto de vista de la conservación de la información en soporte electrónico, la utilización de software libre y de fuentes abiertas facilita un mayor control de las aplicaciones y de los formatos en los que se almacena la información, en términos de longevidad, estabilidad y mantenimiento, frente a posibles vicisitudes relativas a la continuidad de los productos, herramientas y formatos por razón de soporte, descatalogación o política comercial.

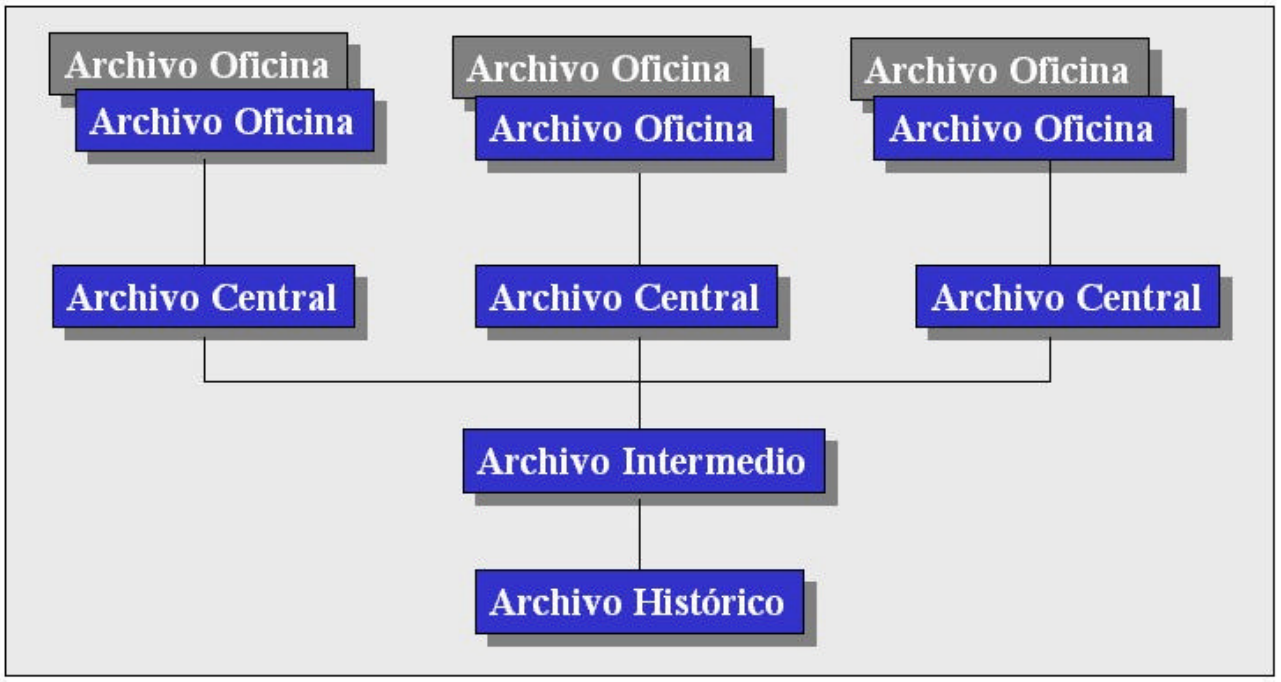
Es de aplicación aquí lo previsto en los *'Criterios de Normalización*' en el capítulo de '*Software libre y de fuentes abiertas*'.

7 Sistema de archivos

CONSIDERACIONES:

La documentación administrativa sigue un mismo proceso con distintas etapas de ciclo de vida, en cada una de las cuales el documento cumple unas funciones específicas y recibe un tratamiento diferente, en el que mantiene siempre su identidad.

El Sistema de Archivos de la Administración, establecido por el Decreto 914/1969 de 8 de mayo, define cuatro tipos distintos de archivo que se diferencian entre sí por las funciones específicas que les corresponden. Cada archivo afecta a determinados actores y, en ellos, los requisitos de conservación de la información pueden influir tanto a soportes como a formatos.



Los archivos protegen su contenido contra catástrofes debidas a derrumbamiento del edificio, choque de vehículos, explosiones en las inmediaciones, actos de guerra y atentados terroristas. De igual forma los archivos salvaguardan su contenido contra incendios, robo e inundaciones, ya sea esta derivada de la extinción de un incendio, fuga de las conducciones de agua o alcantarillado, o a consecuencia de lluvia abundante y mala evacuación del agua.

En sus diferentes dependencias y depósitos, los archivos cuentan con una protección razonable de sus series documentales e históricas. Protección contra la decadencia natural de los soportes causada por las condiciones del ambiente a que están expuestos, tal es el caso de la depuración del aire, temperatura y humedad relativa, la luz natural, artificial y ultra violeta, así como por la acción de animales, microorganismos y polvo.

Aunque en el Sistema de Archivos de la Administración no hay regulación similar sobre soportes electrónicos, se trata en los apartados siguientes de trasladar las prácticas de gestión documental, ya establecidas y operativas, a un entorno electrónico, es decir a la gestión de documentos electrónicos procedentes de los archivos de oficina y a la conservación de documentación electrónica en archivos de carácter permanente.

Archivo de oficina

CONSIDERACIONES:

Para la correcta organización de un archivo de oficina conviene distinguir cuatro grupos de documentos:

- Correspondencia, escritos y comunicados que una unidad administrativa mantiene con particulares o con otros organismos.
- Registros, instrumentos de control donde quedan consignadas diligencias de inicio (entrada) y finalización (salida), y asentadas las actividades de control administrativo que tienen valor jurídico, gracias al cual puede certificarse la existencia de un documento aunque éste no se haya conservado.
- Expedientes, conjunto de documentos ordenado y agrupado que materializan las actuaciones y diligencias encaminadas a la resolución administrativa de un asunto determinado.
- Textos legales, publicaciones, informes, circulares y otros documentos que tienen una función de apoyo informativo y son necesarios para el correcto desarrollo de la gestión administrativa.

MARCO LEGAL:

En relación con el archivo de documentos en soporte papel:

- Ley 16/1985 del Patrimonio Histórico Nacional, artículos 55 y 58 ‘Eliminación de documentos’.
- Decreto 914/1969 Sistema de Archivos de la Administración.

En relación con los derechos del ciudadano de acceso a archivos y registros administrativos:

- Los ciudadanos tienen derecho a acceder a los registros y a los documentos que obren en los archivos administrativos, cualquiera que sea la forma de expresión gráfica, sonora o en imagen o en el tipo de soporte material en que figuren, en las condiciones en las condiciones que se establecen (expedientes terminados, interés legítimo y directo, otras específicas) (Ley 30/1992, art. 45.2)

En relación con la protección de datos de carácter personal:

- Determinar el valor y plazos de conservación de los documentos administrativos en función de la utilización y acceso a los documentos. (LO 15/1999, art. 4.5)

CRITERIOS:

7.1 Mantener el archivo de oficina en función de la utilización y acceso a los documentos establecidos en los procedimientos de gestión.

7.2 Conservar los documentos generados por la oficina productora que se encuentren en trámite, mientras dura su formación e incluso al terminar ésta si las necesidades de utilización y consulta son continuas. En su caso destruir los documentos que carezcan de valor administrativo, con la aprobación previa del responsable de su gestión.

7.3 Poner al frente del archivo de oficina una persona encargada de su gestión, organización y control.

RECOMENDACIONES:

- Mantener el archivo de oficina aplicando los procedimientos descritos en 'Ciclo de vida de la información en soporte electrónico' y en 'Medidas de almacenamiento y conservación'.
- No custodiar documentos que superen más de 10 años de antigüedad.

NIVELES DE SEGURIDAD:

- En función de los datos personales de los ciudadanos, contenidos en la información, le son aplicables del RD 994/1999, las medidas de seguridad requeridas por los artículos 4 'Aplicación de los niveles de seguridad' y 7 'Ficheros temporales'.
- Cabe establecer los niveles de medidas de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento '*Criterios de seguridad*' el capítulo '*Identificación y clasificación de activos a proteger'*.

AMPLIACIÓN TÉCNICA:

- Ley 16/1985 del Patrimonio Histórico Nacional, artículos 55 y 58 'Eliminación de documentos'.
- Decreto 914/1969 Sistema de Archivos de la Administración.
- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
- Manual de tratamiento de archivos administrativos; Ministerio de Cultura 1992, Normas técnicas de la Dirección de Archivos Estatales.
- Guía de la información electrónica (DLM Forum) http://europa.eu.int/historical_archives/dlm_forum/index_en.htm

Archivo central

MARCO LEGAL:

En relación con el archivo de documentos en soporte papel:

- Ley 16/1985 del Patrimonio Histórico Nacional, artículos 55 y 58 'Eliminación de documentos'.
- Decreto 914/1969 Sistema de Archivos de la Administración.

En relación con los derechos del ciudadano de acceso a archivos y registros administrativos:

- Los ciudadanos tienen derecho a acceder a los registros y a los documentos que obren en los archivos administrativos, cualquiera que sea la forma de expresión gráfica, sonora o en imagen o en el tipo de soporte material en que figuren, en las condiciones en las condiciones que se establecen (expedientes terminados, interés legítimo y directo, otras específicas) (Ley 30/1992, art. 45.2)

CRITERIOS:

7.4 Transferir los documentos desde los archivos de oficina de las unidades administrativas productoras al Archivo Central una vez finalizado su trámite y cuando las necesidades de utilización no sean frecuentes, a consecuencia de la perdida paulatina de su valor administrativo.

RECOMENDACIONES:

- Mantener el Archivo Central de soportes electrónicos aplicando los procedimientos descritos en 'Ciclo de vida de la información en soporte electrónico' y en 'Medidas de almacenamiento y conservación'.
- Proporcionar información para:
  - Informar sobre la posibilidad de eliminación o de conservación permanente de las series documentales.
  - Informar a las oficinas del organismo sobre los fondos custodiados en este archivo, o respecto de fondos ya transferidos al Archivo Intermedio, canalizando y coordinando este tipo de consultas.
- Mantener el archivo central aplicando los procedimientos descritos en 'Ciclo de vida de la información en soporte electrónico' y en 'Medidas de almacenamiento y conservación'.
- Establecer procedimientos documentados para:
  - Conservar las series documentales en instalaciones acondicionadas al tipo de soporte.
  - Identificar las series documentales, respecto de su procedencia, estructura, sujeto productor y tipo documental.
  - Valorar el testimonio administrativo legal, jurídico e informativo presente en cada serie documental.
  - Determinar los plazos de reserva, frecuencia de consulta por la oficina productora, y periodos de prescripción de los valores administrativos.
  - Eliminar documentos duplicados.

NIVELES DE SEGURIDAD:

- En función de los tipos de datos personales de los ciudadanos, contenidos en la información, le es aplicable del RD 994/1999, las medidas de seguridad de nivel medio establecidas en los artículos 17, 18, 19 y 20 para aquella información que conserva valor histórico, estadístico o científico, y que todavía contenga datos que permiten obtener una evaluación de la personalidad del individuo.
- Cabe establecer los niveles de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento '*Criterios de seguridad*' el capítulo '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

- Ley 16/1985 del Patrimonio Histórico Nacional, artículos 55 y 58 'Eliminación de documentos'.
- Decreto 914/1969 Sistema de Archivos de la Administración.
- Manual de tratamiento de archivos administrativos; Ministerio de Cultura 1992, Normas técnicas de la Dirección de Archivos Estatales.

- Guía de la información electrónica (DLM Forum)
  http://europa.eu.int/historical_archives/dlm_forum/index_en.htm

Archivo intermedio

MARCO LEGAL:

En relación con el archivo de documentos en soporte papel:

- Ley 16/1985 del Patrimonio Histórico Nacional, artículos 55 y 58 'Eliminación de documentos'.
- Decreto 914/1969 Sistema de Archivos de la Administración.

En relación con los derechos del ciudadano de acceso a archivos y registros administrativos:

- Los ciudadanos tienen derecho a acceder a los registros y a los documentos que obren en los archivos administrativos, cualquiera que sea la forma de expresión gráfica, sonora o en imagen o en el tipo de soporte material en que figuren, en las condiciones en las condiciones que se establecen (expedientes terminados, interés legítimo y directo, otras específicas) (Ley 30/1992, art. 45.2)

CRITERIOS:

7.5 Transferir los documentos desde los Archivos Centrales de los organismos al Archivo Intermedio cuando la necesidad de consulta por los organismos productores sea ocasional y mantenerla hasta que su valor administrativo desaparezca.

RECOMENDACIONES:

- Mantener el Archivo Intermedio de soportes electrónicos aplicando los procedimientos descritos en 'Ciclo de vida de la información en soporte electrónico' y en 'Medidas de almacenamiento y conservación'.
- Establecer procedimientos documentados para:
  - Conservar las series documentales hasta la total prescripción de sus valores administrativos.
  - Valorar la trascendencia de las series documentales como testimonio de la actuación de la Administración y de la sociedad en su conjunto.
  - Determinar la temporalidad del soporte, dependiendo de su envejecimiento natural y del riesgo de pérdida de legibilidad o reproducción derivada de la caída en desuso del equipo y del programa necesario para reproducirlo.
  - Cambiar de soporte en función de la temporalidad y vida útil del mismo.
  - Eliminar las series documentales que no son de utilidad administrativa y carezcan de valor histórico.
  - Transferir las series documentales cuya valoración determine su conservación permanente porque tienen validez histórica.
  - No conservar documentos que superen más de 50 años de antigüedad.

- Cumplir con los criterios de transferencia establecidos para las series históricas en soporte electrónico por los archivos históricos, tales como:
  - Tener información del contexto y metadatos.
  - Ser conforme a los medios de tratamiento y formatos que soporta.

NIVELES DE SEGURIDAD:

- En función de los tipos de datos personales de los ciudadanos, contenidos en la información, le es aplicable del RD 994/1999, las medidas de seguridad de nivel medio establecidas en los artículos 17, 18, 19 y 20 para aquella información que conserva valor histórico, estadístico o científico, y que todavía contenga datos que permiten obtener una evaluación de la personalidad del individuo.
- Cabe establecer los niveles de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento '*Criterios de seguridad*' el capítulo '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

- Ley 16/1985 del Patrimonio Histórico Nacional, artículos 55 y 58 'Eliminación de documentos'.
- Decreto 914/1969 Sistema de Archivos de la Administración.
- Manual de tratamiento de archivos administrativos; Ministerio de Cultura 1992, Normas técnicas de la Dirección de Archivos Estatales.
- Guía de la información electrónica (DLM Forum) http://europa.eu.int/historical_archives/dlm_forum/index_en.htm

Archivo histórico

MARCO LEGAL:

En relación con el archivo de documentos y el patrimonio histórico:

- Ley 16/1985 del Patrimonio Histórico Nacional, artículos 55 y 58 'Eliminación de documentos'.
- Decreto 914/1969 Sistema de Archivos de la Administración.
- El Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de los documentos administrativos en soporte distinto al original.

En relación con los derechos del ciudadano de acceso a archivos y registros administrativos:

- Los ciudadanos tienen derecho a acceder a los registros y a los documentos que obren en los archivos administrativos, cualquiera que sea la forma de expresión gráfica, sonora o en imagen o en el tipo de soporte material en que figuren, en las condiciones en las condiciones que se establecen (expedientes terminados, interés legítimo y directo, otras específicas) (Ley 30/1992, art. 45.2)

CRITERIOS:

7.6 Transferir los documentos desde el Archivo Intermedio al Archivo Histórico correspondiente cuando la valoración de los documentos determine su conservación permanente.

7.7 La durabilidad de las series históricas del archivo es de un periodo mínimo de 100 años.

7.8 No apreciar ningún deterioro significativo en la consulta de cualquier documento del archivo histórico.

RECOMENDACIONES:

- Mantener el Archivo Histórico de soportes electrónicos aplicando los procedimientos descritos en 'Ciclo de vida de la información en soporte electrónico' y en 'Medidas de almacenamiento y conservación'.

Soportes recomendados para la conservación de series históricas:

- 1.- Soporte Óptico: Discos ópticos, en cualquiera de sus formatos: disco compacto; disco óptico; CD-R y DVD-R.
- 2.- Soporte Microfilm: Microfilm, película madre, de poliéster con halógeno de plata revelada por inversión. Película madre y duplicado, deben cumplir la calidad de filmación indicada en el Anexo C de la norma ISO 6199. Las copias de trabajo se hacen del duplicado en película blanco y negro, y esta debe seguir la norma ISO 10602.

NIVELES DE SEGURIDAD:

- En función de los tipos de datos personales de los ciudadanos, contenidos en la información, le es aplicable del RD 994/1999, las medidas de seguridad de nivel medio establecidas en los artículos 17, 18, 19 y 20 para aquella información que conserva valor histórico, estadístico o científico, y que todavía contengan datos que permiten obtener una evaluación de la personalidad de las personas.
- Cabe establecer los niveles de seguridad en función de los subestados de seguridad de autenticación, confidencialidad, integridad y disponibilidad reflejados a su vez en la 'función' o 'necesidad de conocer'. Véase en el documento '*Criterios de seguridad*' el capítulo de '*Identificación y clasificación de activos a proteger*'.

AMPLIACIÓN TÉCNICA:

- Ley 16/1985 del Patrimonio Histórico Nacional, artículos 55 y 58 'Eliminación de documentos'.
- Decreto 914/1969 Sistema de Archivos de la Administración.
- Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de los documentos administrativos en soporte distinto al original.
- Manual de tratamiento de archivos administrativos; Ministerio de Cultura 1992, Normas técnicas de la Dirección de Archivos Estatales.
- Guía de la información electrónica (DLM Forum)
  http://europa.eu.int/historical_archives/dlm_forum/index_en.htm

ANEXO: EQUIPO RESPONSABLE DEL PROYECTO - versión 2.2

COORDINADOR DEL PROYECTO:
D. Francisco López Crespo
Jefe del Área de Sistemas Telemáticos Ministerio de Administraciones Públicas

JEFE DEL PROYECTO:
D. Miguel Ángel Amutio Gómez
Jefe del Área de Planificación y Explotación - Ministerio de Administraciones Públicas

ASESOR TÉCNICO:
D. Ricardo Cantabrana González
Técnico Superior de Tecnologías de la Información - Ministerio de Administraciones Públicas

SECRETARIA DEL PROYECTO:
D.ª Reyes Villalba Arranz
Titulada Superior - Ministerio de Administraciones Públicas

EDICIÓN WEB:
Dª Mª Paloma Balairón de la Poza
Analista Programador - Ministerio de Administraciones Públicas