MINISTERIO
DE ADMINISTRACIONES
PÚBLICAS

SECRETARÍA DE ESTADO
PARA LA ADMINISTRACIÓN
PÚBLICA

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

Aplicaciones utilizadas para el ejercicio de potestades

CRITERIOS DE CONSERVACIÓN

28 de Febrero de 2003

Madrid, febrero de 2003

Índice

Historial del documento

Versión	***Comentarios.***
Versión 1 Final. Presentada al Pleno de CIABSI de 26 de septiembre de 2001.	N/A.
Versión 1.1. Presentada al Pleno de CIABSI de 24 de octubre de 2001.	N/A.

Versión 1.2. Presentada al Pleno de CIABSI de 18 diciembre de 2001.	Versión publicada.
Versión 2. 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.

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).
- **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://www.dlmforum.eu.org

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://www.dlmforum.eu.org

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.

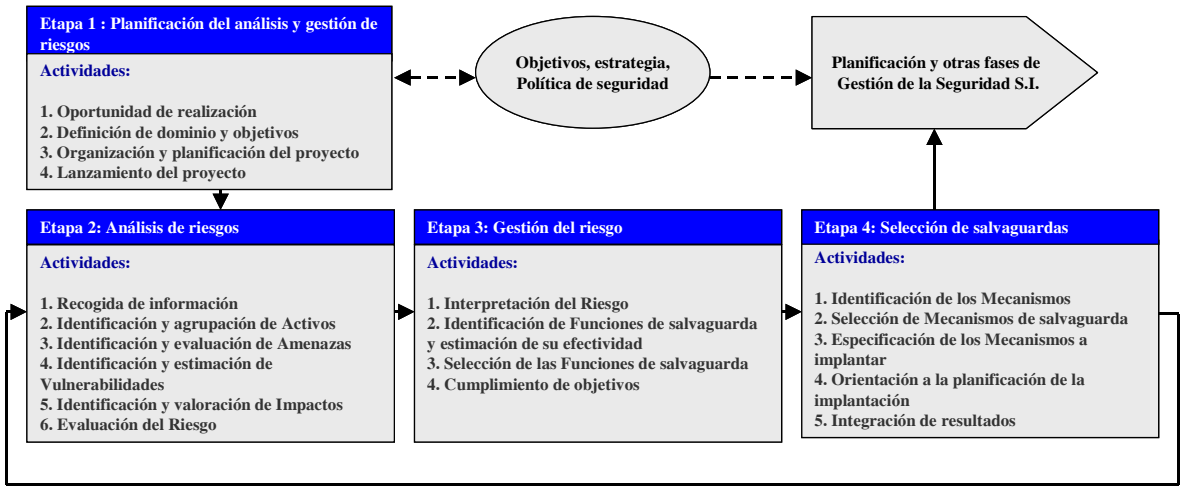
En segundo lugar, existen **amenazas** tales como las siguientes:

- 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.map.es/csi/pg5m20.htm
- Guía de la información electrónica (DLM Forum) http://www.dlmforum.eu.org

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 los 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:

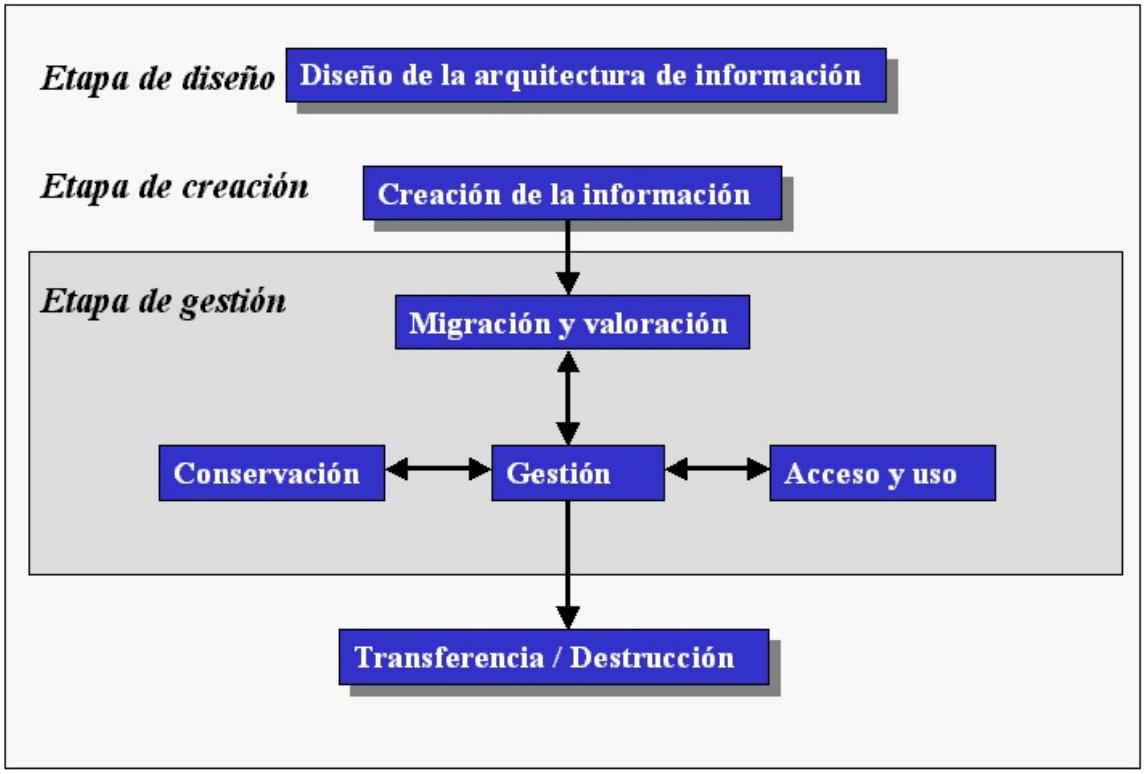
- Los ciudadanos tienen derecho a acceder a los registros y a los documentos que obren en los archivos administrativos, cualquiera que sea la forma de expresión gráfica, sonora o en imagen o en el tipo de soporte material en que figuren, en las condiciones en las condiciones que se establecen (expedientes 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://www.dlmforum.eu.org
- IDA MoReq (*Model requirments for the management of electronic records*) http://europa.eu.int/ISPO/ida/

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://www.dlmforum.eu.org

- *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 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://www.dlmforum.eu.org

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://www.dlmforum.eu.org

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://www.dlmforum.eu.org
- 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://www.dlmforum.eu.org
- *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.

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://www.dlmforum.eu.org
- UK e-GIF (*e-government interoperability framework*), http://www.citu.gov.uk/egif.htm
- 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.
  - 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.
  - ***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 formal de documentos.
  - 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://www.dlmforum.eu.org .
- *IDA Architecture Guidelines, Part II, 3. Service profiles*, http://www.ispo.cec.be/ida/ida.html
- 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://www.dlmforum.eu.org
- IDA Architecture Guidelines, Part II, 3. Service profiles, http://www.ispo.cec.be/ida/ida.html
- CIABSI, cláusula tipo de juego de caracteres, http://www.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	5ª 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		5ª 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	5ª 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	5ª 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	-5ª 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
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://www.dlmforum.eu.org

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:

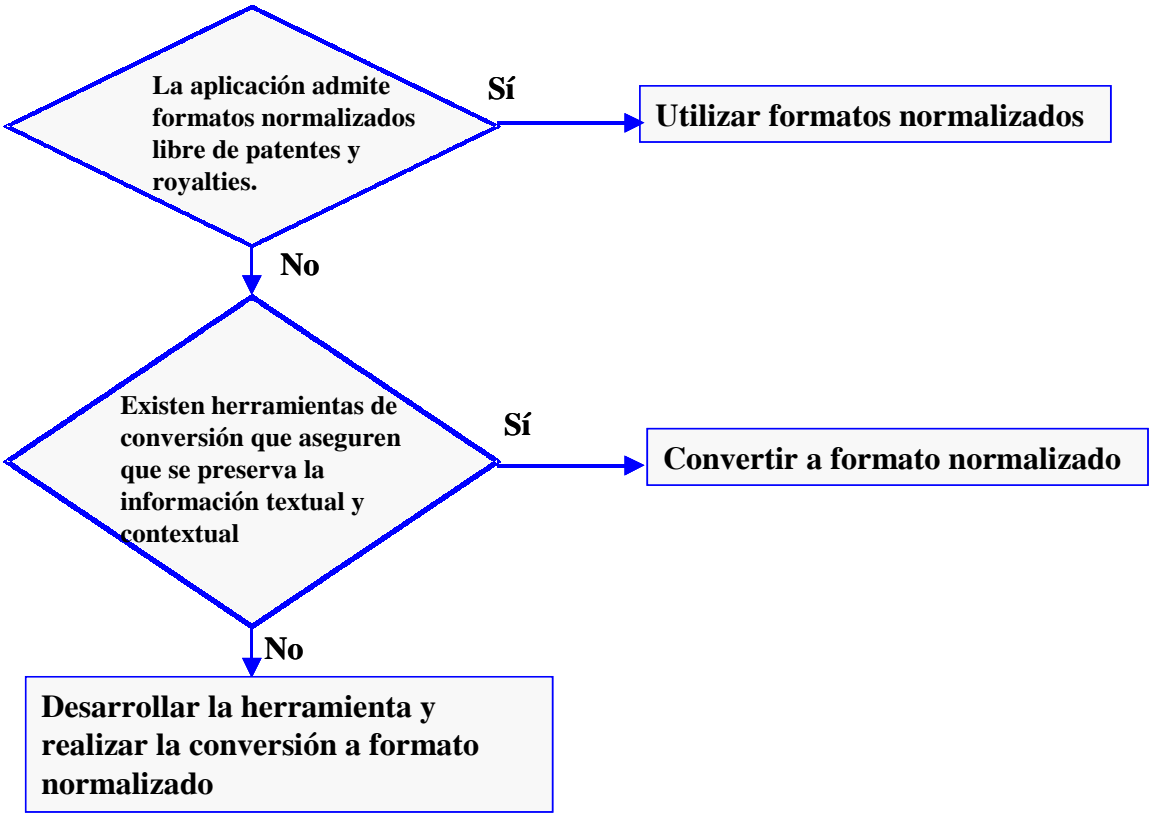
- En función de los tipos de datos personales de los ciudadanos, contenidos en los soportes, le es aplicable del RD 994/1999, la gestión de soportes y la recuperación de datos: artículos 13 y 14 para medidas de seguridad de nivel básico y artículos 20 y 25 para medidas de seguridad de nivel medio y alto.
- 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://www.dlmforum.eu.org

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.map.es/csi/pg5m20.htm
- Guía de seguridad informática (SEDISI), punto 3.6 'Medios de almacenamiento'. http://www.sedisi.es/ 05_index.htm

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.map.es/csi/pg5m20.htm.
- Guía de la información electrónica (DLM Forum) http://www.dlmforum.eu.org

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.

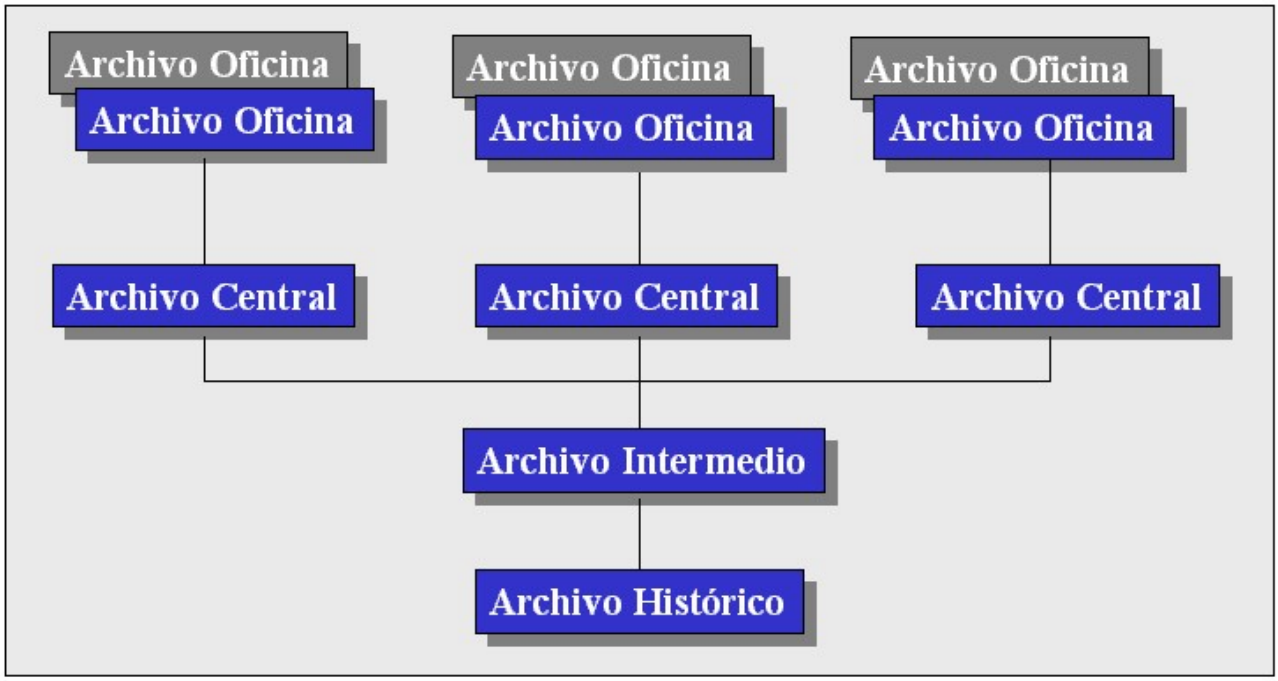
Es de aplicación aquí lo previsto en los '*Criterios de Normalización*' en el capítulo de '*Software libre y de fuentes abiertas*'.

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://www.dlmforum.eu.org

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://www.dlmforum.eu.org

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://www.dlmforum.eu.org

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://www.dlmforum.eu.org