Política de gestión de documentos electrónicos MINHAP.

Ponencias complementarias al documento

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

:) @dministración electrónica

"Política de gestión de documentos electrónicos MINHAP"

Ponencias complementarias al documento

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

@dministración electrónica

Equipo responsable de la elaboración del documento

"*Política de gestión de documentos-e MINHAP*"

Grupo de Apoyo de Tecnología y Normativa

(Grupo de Trabajo para la Coordinación de Archivos)

Coordinador:	
Gerardo Bustos Pretel	Secretaría General Técnica
Equipo de redacción:	
Rosa Martín Rey	Secretaría General Técnica
Luis Romera Iruela	Secretaría General Técnica
José Luis García Martínez	Secretaría General Técnica
Grupo de trabajo:	
Josefina Otheo de Tejada Barasoin	AEAT
Andrea Ruiz de Garibay	AEAT
Carmen Conejo Fernández	D.G. Catastro
Miguel A. Amutio Gómez	DGMPIAE
Andoni Pérez de Lema Sáenz de Viguera	Intervención General de la Administración del Estado
Alejandro Millaruelo Gómez	Intervención General de la Administración del Estado
Álvaro Tapias Sancho	D.G. Catastro
Cristina Martínez Merencio	División de Sistemas Información y Telecomunicaciones
Juan Antonio Zapardiel López	Inspección General
Santiago Vélez Fraga	Sub. Gral. Tecnologías Inform. y Telecomunicaciones
M. Carmen Barroso González	D.G. Función Pública
Javier Hernández Díez	División de Sistemas Información y Telecomunicaciones
Álvaro Reig González	INAP
Cándida Pérez Clemente	Secretaría General Técnica
Begoña Rada	División de Sistemas Información y Telecomunicaciones
Petra Fernández Álvarez	DGMPIAE
José Luis Lapuente Perea	DGMPIAE
Ministerio de Educación, Cultura y Deportes	
Ricard Pérez Alcázar	Subdirección General de Archivos Estatales
Carlos César Herrero García	S.G. Tecnologías
Ministerio de la Presidencia	
Dominica Graíño Ferrer	Secretaría General Técnica
Fernando Iniesta Sánchez	S.G. Tecnologías
Isabel Barrio Martín	Secretaría General Técnica

Edita:
© Ministerio de Hacienda y Administraciones Públicas
Secretaría General Técnica
Subdirección General de Información, Documentación y Publicaciones
Centro de Publicaciones

Impresión y encuadernación:
Oficialía Mayor del Ministerio de Hacienda y Administraciones Públicas

NIPO: 630-14-160-X
Esta publicación es electrónica. El ejemplar impreso se edita exclusivamente como garantía de edición y conservación

ÍNDICE

Pág.

PRESENTACIÓN

La utilidad de las ponencias relacionadas con el expediente-e

El 12 de diciembre de 2013 se constituyó el Grupo de Apoyo de Tecnología y Normativa (GATN), creado en el seno del Grupo de Trabajo para la Coordinación de Archivos del Ministerio de Hacienda y Administraciones Públicas (GTCA). Se trata de un grupo "*de carácter tecnológico normativo*", cuyos "*cometidos se centrarán en la elaboración de un documento de política de gestión documental para todo el Departamento en el marco del ENI, así como en la contribución al diseño de una aplicación de gestión de archivo electrónico que implemente dicha política y que permita el desarrollo de herramientas de gestión de archivo de documentos electrónicos*".

Un dato fundamental a tener en cuenta es la composición del grupo, de carácter multidisciplinar: profesionales del mundo del archivo y de las tecnologías de la información y las comunicaciones. Asimismo, la variedad ha venido también de la mano de los organismos representados: Secretaría General Técnica, AEAT, Catastro, IGAE, Dirección General de Modernización Administrativa, Inspección General, Función Pública, Subdirección General de Tecnologías de Información y las Comunicaciones, División de Sistemas de Información y Comunicaciones, INAP.

A ello hay que sumar la participación también de la Subdirección General de Archivos Estatales, de la Secretaría de Estado de Cultura. Se trata de una representación de sumo interés, dada su máxima responsabilidad en materia de archivos de la Administración General del Estado. Asimismo, también han participado en el grupo, a petición propia, personas del Ministerio de la Presidencia, que han querido unir sus esfuerzos a los nuestro en el desarrollo de estas tareas. Sin duda, esta amplia composición ha enriquecido los debates y, por tanto, las conclusiones del documento, extendiendo así su validez y utilidad a un abanico mayor en el terreno de las Administraciones Públicas.

Con el fin de avanzar más rápidamente se decidió trabajar en ponencias, sobre algunos de los temas más importantes. En torno a ellas se han generado importantes debates. En algunos casos, como especialmente en el de dibujar el esquema institucional de metadatos en el marco del Esquema Nacional de Interoperabilidad (en adelante ENI), han sido debates largos y enriquecedores. Y lo más importante: todo se ha ido aprobando por consenso, a base de entender que había que conjugar equilibradamente el rigor, el marco legal del ENI y la realidad en la que se movían los distintos centros y organismos.

Entre el 12 de diciembre y el 1 de julio el grupo de trabajo ha celebrado 18 reuniones de cuatro o cinco horas. Fruto de ese trabajo ha sido el borrador del documento de "*Política de gestión de documentos electrónicos MINHAP*", que se presenta hoy al Grupo de Trabajo de Coordinación de Archivos y a la Comisión de Administración Electrónica. Ahí se recogen los criterios y recomendaciones necesarios para garantizar la

interoperabilidad y la recuperación y conservación de documentos y expedientes electrónicos en el MINHAP. Su contenido va a marcar la forma de trabajo administrativo en las próximas décadas.

Sin embargo, consideramos que las ponencias que han servido de arranque en numerosos capítulos del documento tienen un valor documental que no podía perderse. Por un lado, porque pueden servir de orientación a cualquier persona que aborde estas cuestiones del expediente-e y el documento-e. Por otro lado, para quienes vamos a tener que aplicar la "*Política de gestión de documentos electrónicos MINHAP*" las ponencias pueden ayudarnos a conocer por qué razón se optó por uno u otro planteamiento.

No se nos oculta, por otro lado, que actualmente no existe, que sepamos, una política de gestión de documentos-e tan desarrollada como el borrador que nos ocupa. Por tanto, esta recopilación de ponencias puede servir de ayuda en numerosos casos en los que se vaya a elaborar un documento similar. Pues bien, en este sentido el documento propiamente dicho y las ponencias constituyen un conjunto de ayuda y orientación. Al servicio de todos está desde este momento.

Gerardo Bustos Pretel

Coordinador del GANT

Subdirector general de Información, Documentación y Publicaciones

Ministerio de Hacienda y Administraciones Públicas

3 de julio de 2014

Ponencia nº 1

Determinación del Esquema Institucional de Metadatos

Andoni Pérez de Lema Sáenz de Viguera (Intervención General de la Administración del Estado)

Resumen de la ponencia:

Determinación del Esquema Institucional de Metadatos

Andoni Pérez de Lema Sáenz de Viguera (Intervención General de la Administración del Estado)
Ponencia nº 1

Orientaciones y requisitos para la construcción de un esquema de metadatos

De acuerdo con la Norma Técnica de Interoperabilidad (en adelante, NTI) de Política de Gestión de Documentos electrónicos:

- Las **organizaciones garantizarán la disponibilidad e integridad de los metadatos** de sus documentos electrónicos.

- La implementación de los metadatos de gestión de documentos electrónicos para su tratamiento y gestión a nivel interno será **diseñada por cada organización en base a sus necesidades, criterios y normativa específica**.

- Los metadatos de gestión de documentos electrónicos se articularán en **esquemas de metadatos que responderán a las particularidades y necesidades específicas** de gestión de cada organización.

- El **e-EMGDE**, disponible en el Centro de Interoperabilidad Semántica, **podrá ser utilizado como referencia para la adecuación a los requisitos de interoperabilidad** en materia de gestión documental.

    - e-EMGDE incluye los **metadatos mínimos obligatorios**, definidos en las *NTI de Documento electrónico y Expediente electrónico*, **así como otros metadatos complementarios** pertinentes en una política de gestión y conservación de documentos electrónicos.

En concordancia con las directrices de la ISO, es mejor y más sencillo para una organización adoptar un esquema normalizado de metadatos (como e-EMGDE) que ya existe, que está bien diseñado, y está apoyado globalmente, que construir un esquema específico. Si se construyera un esquema nuevo, eso implicaría la necesidad de gestionarlo y mantenerlo durante el tiempo de vida de los documentos. Esto incluye la actualización del esquema y el aseguramiento de la compatibilidad en el pasado y en el futuro, la aparición de metadatos sobre el esquema de metadatos, su catalogación y el resto de la infraestructura necesaria para mantener la implementación, etc.

Por los motivos expuestos, y dado que el esquema de metadatos recomendado por el ENI es e-EMGDE, partiremos del mismo para establecer un esquema institucional de metadatos para el Ministerio (que podría ser extrapolable a otros), que permita cumplir simultáneamente dos objetivos:

- soportar todas las transacciones que tienen lugar en los procesos de gestión documental identificados en la NTI de Política de Gestión de Documentos Electrónicos.

- permitir a los diferentes organismos que lleven a cabo la adecuación al Esquema Nacional de Interoperabilidad con un esfuerzo de desarrollo moderado.

Siempre que sea posible, se deberá evitar introducir ningún elemento nuevo, porque reduce la interoperabilidad. En consecuencia, si fuera necesario introducir algún cambio, se limitarían a introducir:

- mejoras específicas (subelementos adicionales).

- esquemas codificados específicos, por ejemplo listas controladas de términos, reglas sobre como introducir nombres, fechas, etc.

PLANTEAMIENTO DE LA ESTRATEGIA DE IMPLEMENTACIÓN DEL e-EMGDE

A pesar de su clara orientación multi-entidad, el e-EMGE permite una implementación mono-entidad, al objeto de minimizar el esfuerzo de desarrollo. No obstante, para cumplir con los requisitos de las NTI de Documento Electrónico, Expediente Electrónico, Copiado y Conversión, y Digitalización de Documentos, **es necesario contemplar algunos metadatos que en e-EMGDE obligan a disponer también de las entidades: Regulación, Agente, Actividad y Relación.** Por tanto, se adoptará una **aproximación de e-EMGDE multi-entidad**, haciendo especial énfasis en la entidad "Documento", y limitando al mínimo imprescindible las informaciones recogidas en el resto de entidades.

DECLARACIÓN DEL CONJUNTO DE METADATOS DE GESTIÓN DOCUMENTAL SELECCIONADOS DEL e-EMGDE

A partir de un análisis detallado de los procesos de gestión de documentos a lo largo de su ciclo de vida - en los términos regulados en la NTI de Política de Gestión de Documentos Electrónicos -, se ha determinado el conjunto de metadatos preciso para soportar las diferentes transacciones que tienen lugar en dichos procesos, con una doble pretensión: asegurar el cumplimiento del Esquema Nacional de Interoperabilidad, y minimizar el esfuerzo de desarrollo requerida. Presentamos a continuación el repertorio de metadatos seleccionado para el Ministerio de Hacienda y Administraciones Públicas, desglosado por cada entidad de e-EMGDE:

ENTIDAD "DOCUMENTO"

METADATOS OBLIGATORIOS

- eEMGDE 1 – Categoría
- eEMGDE 2 – Identificador
  - eEMGDE 2.1 – Secuencia de Identificador
  - eEMGDE 2.2 – Esquema de identificador
- eEMGDE4 – Fechas
  - eEMGDE 4.1 – Fecha Inicio
  - eEMGDE 4.2 – Fecha fin (éste sub-elemento se rellenará cuando finalice la existencia de una Entidad –documento- o de una Relación).
- eEMGDE14 – Características Técnicas
  - eEMGDE14.1 – Soporte origen
  - eEMGDE14.2 – Nombre de formato
  - eEMGDE14.3 - Versión de formato
  - eEMGDE14.4 – Nombre de la aplicación de creación
  - eEMGDE14.5 – Versión de la aplicación de creación
  - eEMGDE14.7 - Resolución
  - eEMGDE14.8 - Tamaño
- eEMGDE17 – Firma
  - eEMGDE17.1 – Tipo de Firma
  - eEMGDE17.2 – Formato de Firma
  - eEMGDE17.3 – Rol de Firma
- eEMGDE18-Tipo Documental
- eEMGDE20 – Estado de Elaboración
  - eEMGDE20.1 – Denominación del Estado
  - eEMGDE20.2 – Características de la Copia

METADATOS COMPLEMENTARIOS

- eEMGDE3 – NOMBRE
  - eEMGDE3.1 –Nombre Natural
- eEMGDE5 - DESCRIPCIÓN
- eEMGDE 8 – SEGURIDAD
  - eEMGDE8.1.1. – Clasificación de acceso
  - eEMGDE8.4- Sensibilidad Datos de Carácter Personal
  - eEMGDE8.5 – Clasificación ENS
- eEMGDE 9 – DERECHOS DE ACCESO, USO Y REUTILIZACIÓN
  - eEMGDE 9.1 – Condiciones de acceso, uso y reutilización
  - eEMGDE 9.2 – Tipo de acceso
- eEMGDE 11-IDIOMA
- eEMGDE 12-PUNTO DE ACCESO
- eEMGDE 13- CALIFICACION
  - eEMGDE 13.1 - Valoración
  - eEMGDE 13.2 – Dictamen
- eEMGDE 15 – UBICACIÓN
  - eEMGDE 15.1 – Soporte
  - eEMGDE 15.2 - Localización
- eEMGDE 16 –VERIFICACION DE INTEGRIDAD
  - eEMGDE 16.1 – Algoritmo
  - eEMGDE 16.2 - Valor
- eEMGDE 21-TRAZABILIDAD
  - eEMGDE 21.1 - Acción
  - eEMGDE 21.2 – Motivo reglado
  - eEMGDE 21.3 – Usuario de la acción
  - eEMGDE 21.4 - Descripción
  - eEMGDE 21.5 – Modificación en los metadatos
  - eEMGDE 21.6 – Historia del cambio

ENTIDAD “REGULACIÓN”

METADATOS OBLIGATORIOS

- eEMGDE 1 – Categoría
- eEMGDE 2 – Identificador
  - eEMGDE 2.1 – Secuencia de Identificador
  - eEMGDE 2.2 – Esquema de identificador
- eEMGDE4 – Fechas
  - eEMGDE 4.1 – Fecha Inicio
  - eEMGDE 4.2 – Fecha fin (este sub-elemento se rellenará cuando finalice la existencia de una Entidad.

METADATOS COMPLEMENTARIOS

- eEMGDE3 – NOMBRE
  - eEMGDE3.1 –Nombre Natural

- eEMGDE5 - DESCRIPCIÓN
- eEMGDE12 – PUNTOS DE ACCESO

ENTIDAD “AGENTE”

METADATOS OBLIGATORIOS

Deberán implementarse en los gestores documentales los siguientes **metadatos obligatorios** y sub-elementos asociados para la entidad Agente (donde se han excluido aquellos sub-elementos no obligatorios que a nuestro juicio no aportan valor, o no resultan imprescindibles para la adecuación al ENI, de acuerdo con nuestro análisis del apartado V):

- eEMGDE 1 – Categoría
- eEMGDE2 – Identificador
  - eEMGDE2.1 – Secuencia de Identificador
  - eEMGDE2.2 – Esquema de identificador
- eEMGDE4 – Fechas
  - eEMGDE4.1 – Fecha Inicio
  - eEMGDE4.2 – Fecha fin (este sub-elemento se rellenará cuando finalice la existencia de una Entidad.

METADATOS COMPLEMENTARIOS

- eEMGDE3 – NOMBRE
  - eEMGDE3.1 –Nombre Natural
- eEMGDE5 – DESCRIPCIÓN
- eEMGDE8-SEGURIDAD
  - eEMGDE8.3-Permisos
- eEMGDE10 – CONTACTO
  - eEMGDE10.1 – Tipo de Contacto
  - eEMGDE10.2- Dato de Contacto

ENTIDAD “ACTIVIDAD”

METADATOS OBLIGATORIOS

- eEMGDE 1 – Categoría
- eEMGDE2 – Identificador
  - eEMGDE2.1 – Secuencia de Identificador
  - eEMGDE 2.2 – Esquema de Identificador: cuadro de clasificación funcional de una organización
- eEMGDE4 – Fechas
  - eEMGDE4.1 – Fecha Inicio
  - eEMGDE4.2 – Fecha fin (este sub-elemento se rellenará cuando finalice la existencia de una Entidad –actividad-).

METADATOS COMPLEMENTARIOS

- eEMGDE3 – NOMBRE
  - eEMGDE3.1 –Nombre Natural
- eEMGDE5 – DESCRIPCIÓN
- eEMGDE8-SEGURIDAD
  - eEMGDE8.3-Permisos

- eEMGDE22 –CLASIFICACIÓN
  - eEMGDE 22.1 – Código de clasificación
- eEMGDE 22.2 – Denominación de clase

ENTIDAD "RELACIÓN"

METADATOS OBLIGATORIOS

- eEMGDE 1 – Categoría
- eEMGDE2 – Identificador
  - eEMGDE2.1 – Secuencia de Identificador
  - eEMGDE 2.2 – Esquema de Identificador: vocabulario controlado de las relaciones en una organización, o la configuración del sistema de nombrado de relaciones de una aplicación dada.
- eEMGDE4 – Fechas
  - eEMGDE4.1 – Fecha Inicio
  - eEMGDE4.2 – Fecha fin (este sub-elemento se rellenará cuando finalice la existencia de una Entidad –relación-).
- eEMGDE6 – Entidad Relacionada
  - eEMGDE6.1 – ID de Entidad Relacionada.
  - eEMGDE6.2 – Esquema de ID de Entidad Relacionada.
  - eEMGDE6.3 – Rol de la relación, que podrá tener dos valores:

    "1": indica que la relación se lee desde la entidad.

    "2": indica que la relación se lee en dirección hacia la entidad

METADATOS COMPLEMENTARIOS

- eEMGDE5 – Descripción
- eEMGDE21-Trazabilidad

Índice de la Ponencia

I. ORIENTACIONES Y REQUISITOS PARA LA CONSTRUCCIÓN DE UN ESQUEMA DE METADATOS

I.1. QUE SON LOS METADATOS. JUSTIFICACIÓN DE SU NECESIDAD

Los metadatos han sido definidos en la norma ISO 15489 como “datos que describen el contexto, el contenido y la estructura de los documentos y su gestión a lo largo del tiempo”.

Contexto

Es el entorno y la red de relaciones en los que el documento ha sido creado y utilizado.

Se distinguen varios tipos de contexto:

- Jurídico-administrativo
- De procedencia (entidad productora)
- Procedimental (procedimiento que ha dado lugar al documento)
- Documental (fondo al que pertenece el documento)
- Tecnológico

Estructura

Son las reglas de representación de acuerdo con las cuales se comunica el contenido de un documento, su contexto administrativo y documental, y su autor.

Los metadatos permiten fijar el documento en su contexto corporativo y documentan su gestión a lo largo del tiempo. Los metadatos de los documentos sirven, pues, para identificarlo, autenticarlo y contextualizarlo, y no sólo en su punto de producción, porque se van acumulando para documentar su gestión a lo largo del tiempo. Por consiguiente, permiten (de acuerdo con el ICA o Consejo Internacional de Archivos) “localizar, representar y comprender el sentido de los documentos”.

La producción, captura y gestión de metadatos de gestión de documentos es esencial para permitir la identificación, comprensión y recuperación de los documentos y proteger las evidencias de su autenticidad, fiabilidad e integridad. Los metadatos se deberían de capturar de acuerdo con una norma de gestión de documentos concreta (en España de la NTI de Política de Gestión de Documentos Electrónicos), según estipulen los requerimientos normativos o de la organización.

Los metadatos no se han de conservar junto con el contenido, siempre y cuando estén vinculados o asociados de alguna manera. Sólo es obligatorio incorporar los metadatos al fichero del documento electrónico en el momento del intercambio. Los metadatos pueden almacenarse en sistemas externos al sistema de negocio en cuestión o pueden abarcar herramientas o documentación como por ejemplo esquemas o datos XML y modelos de clases que permitan comprender los documentos y mantenerlos comprensibles con el paso del tiempo.

En los entornos de bases de datos puede ser especialmente difícil distinguir el contenido de un documento de sus metadatos. Por ejemplo, los metadatos que evidencian que una persona ha accedido a un documento en una fecha o en una hora determinadas constituyen, también, un documento. A menudo, los metadatos de un sistema pertenecen al sistema en su conjunto. Dicho de otra forma, se aplican de una manera generalizada a todos los documentos del sistema, no a los documentos por separado; pueden residir en las reglas del sistema o en la documentación del sistema y no aplicarse a documentos concretos (fuente: ICA).

I.2. BENEFICIOS OBTENIDOS CON LA UTILIZACIÓN DE METADATOS

La descripción de documentos electrónicos mediante la incorporación de metadatos permite:

- Asegurar que **se registra en los documentos la información contextual** adecuada a los procesos.
- Ayudar a **descubrir y recuperar documentos** mediante la aplicación de vocabularios controlados, esquemas de valores y otros esquemas descriptivos normalizados.
- Mejorar la **difusión de la información**.
- **Controlar el acceso a los documentos**, señalando en el momento de su creación la categoría de seguridad o legal de los documentos.
- **Facultar el acceso o transferencia de documentos** entre organizaciones.
- **Hacer posible la ejecución de las acciones dictaminadas** sobre los documentos.
- **Asegurar que no se pierden los documentos esenciales** cuando se implantan nuevos sistemas.
- Asegurar la **preservación de la información a lo largo del tiempo.**
- **Estandarizar las descripciones** mediante: documentos tipo, series documentales, patrones tipo de expedientes, información en bases de datos.
- Ayudar a **planificar la migración de datos** y otras necesidades de conservación.
- Proporcionar una **referencia para evaluar la calidad de la gestión de documentos.**
- Integrar de manera eficaz la información acerca de documentos electrónicos en los **sistemas de control intelectual**.
- Asegurar la **interoperabilidad**.

I.3. REQUERIMIENTOS LEGALES PARA LA CONSTRUCCION DE UN ESQUEMA INSTITUCIONAL DE METADATOS

La norma ISO 23081, sobre "Metadatos para la gestión de documentos", define un esquema de metadatos como "*Plan lógico que muestra las relaciones entre los distintos elementos del conjunto de metadatos, normalmente mediante el establecimiento de reglas para su uso y gestión y específicamente relacionadas con la semántica, la sintaxis y la obligatoriedad de los valores*".

Otro concepto clave relacionado con el anterior es el de "Esquema de codificación", que se define de la siguiente manera en la norma ISO 23081: *Lista controlada de todos los valores aceptables en lenguaje natural o cadena de caracteres formateada con una sintaxis concreta, diseñados para su procesamiento automatizado.* Incluye reglas y/o formatos para la entrada de datos, tales como fechas, nombres de personas, etc.

De acuerdo con la NTI de Política de Gestión de Documentos electrónicos:

- Las **organizaciones garantizarán la disponibilidad e integridad de los metadatos** de sus documentos electrónicos.
- La implementación de los metadatos de gestión de documentos electrónicos para su tratamiento y gestión a nivel interno será **diseñada por cada organización en base a sus necesidades, criterios y normativa específica**.
- Los metadatos de gestión de documentos electrónicos se articularán en **esquemas de metadatos que responderán a las particularidades y necesidades específicas** de gestión de cada organización.
- El **e-EMGDE**, disponible en el Centro de Interoperabilidad Semántica, **podrá ser utilizado como referencia para la adecuación a los requisitos de interoperabilidad** en materia de gestión documental.

- e-EMGDE incluye los **metadatos mínimos obligatorios**, definidos en las *NTI de Documento electrónico y Expediente electrónico*, **así como otros metadatos complementarios** pertinentes en una política de gestión y conservación de documentos electrónicos.

I.4. EL DILEMA ENTRE LA CREACIÓN DE UN ESQUEMA DE METADATOS NUEVO O LA ADAPTACIÓN DE UN ESQUEMA NORMALIZADO

La cuestión clave para implantar un proyecto de metadatos es la siguiente: "¿Es necesario crear un esquema de metadatos nuevo o existen ya esquemas de metadatos que pueden adaptarse para su uso?". En las administraciones españolas, desde la aprobación de la NTI de Política de Gestión de Documentos Electrónicos, se dispone del esquema de metadatos e-EMGDE, basado en el utilizado en el Archivo Nacional de Australia, "*Australian Government Recordkeeping Metadata Standard Version 2.0*", y que incluye tablas de concordancia con los esquemas internacionales PREMIS e ISO 23081 (en este caso, sólo para los elementos de nivel superior).

En términos generales, y siguiendo las instrucciones de la ISO, es mejor que existan pocos esquemas de metadatos a nivel mundial. Usamos las normas para mejorar la interoperabilidad y reducir las diferencias innecesarias. Es mejor y más sencillo adoptar algo que ya existe, que está bien diseñado, y está apoyado globalmente. Si se construyera un esquema nuevo, eso implicaría la necesidad de gestionarlo y mantenerlo durante el tiempo de vida de los documentos. Esto incluye la actualización del esquema y el aseguramiento de la compatibilidad en el pasado y en el futuro, la aparición de metadatos sobre el esquema de metadatos, su catalogación y el resto de la infraestructura necesaria para mantener la implementación, etc.

Por los motivos expuestos, y dado que el esquema de metadatos recomendado por el ENI es e-EMGDE, partiremos del mismo para establecer un esquema institucional de metadatos para el Ministerio (que podría ser extrapolable a otros), que permita cumplir simultáneamente dos objetivos:

- soportar todas las transacciones que tienen lugar en los procesos de gestión documental identificados en la NTI de Política de Gestión de Documentos Electrónicos.
- Permitir a los diferentes organismos que lleven a cabo la adecuación al Esquema Nacional de Interoperabilidad con un esfuerzo de desarrollo moderado.

Siguiendo las directrices de la norma ISO/TC 46/SC 11/Archives/Record Management, es frecuente que las organizaciones requieran algún cambio específico en un esquema de metadatos. Los cambios más frecuentes son:

- Esquemas de codificación específicos para una organización. Ejemplos: listas de localizaciones de las oficinas, roles del personal, actividades internas específicas, etc.
- Inclusión de subelementos específicos para la organización.

Siempre que sea posible, se deberá evitar introducir ningún elemento nuevo, porque reduce la interoperabilidad. En consecuencia, cuando se crea un perfil de aplicación desde un esquema de metadatos, la mayor parte de los cambios, si los hubiera, se limitarían a introducir:

- Mejoras específicas (subelementos adicionales).
- Esquemas codificados específicos, por ejemplo listas controladas de términos, reglas sobre como introducir nombres, fechas, etc.

I.5. RECOMENDACIONES PARA LA ELABORACION DEL ESQUEMA INSTITUCIONAL DE METADATOS:

- Deberá estar integrado con las iniciativas de interoperabilidad y seguridad de la administración española (Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad).
- Seleccionar de e-EMGDE el conjunto de metadatos suficiente para cubrir todas las transacciones que tienen lugar en los procesos de gestión documental identificados

en la NTI de Política de Gestión de Documentos Electrónicos. Sólo serán capturados los metadatos de utilidad, para facilitar una adecuación al ENI menos costosa en tiempo y recursos.

- Estudiar qué elementos son obligatorios, cuáles son opcionales, y cuáles son recomendables. Si un elemento es obligatorio en e-EMGDE, éste deberá ser conservado, y se debe mantener su obligatoriedad.
- Evitar la introducción de elementos nuevos. Si fuera imprescindible introducir algún cambio, para asegurar la interoperabilidad este se limitaría a: subelementos, o listas controladas de términos.
- Se deberán minimizar las entradas en "texto libre". El principal beneficio de los elementos de texto libre es que estos proporcionan un lugar a los usuarios para añadir información que no encaja en otros elemento. Sin embargo, el texto libre presenta problemas importantes, como: variaciones en ortografía y uso de mayúsculas y minúsculas, variaciones en abreviaturas o formatos de fechas, los usuarios pueden evitar rellenar otros elementos y en su lugar introducir información desestructurada en un campo de texto libre, e incrementar costes operacionales para acceder y recuperar documentos. Asimismo, el texto libre puede conducir a que la información sea inutilizable por parte de sistemas automáticos.
- Estudiar autoridades homólogas de gestión documental y archivos, y otras administraciones que hayan aplicado o desarrollado esquemas de metadatos.
- Se deberán mantener adecuadamente los elementos que estén importados de otros esquemas de metadatos o vocabularios controlados (por ejemplo, coordenadas geoespaciales o fechas), mediante "tablas de equivalencias", y cuando cambien estos esquemas o vocabularios externos, se deberá actualizar en consonancia el esquema institucional de metadatos.
- A nivel técnico, el esquema de metadatos deberá concebirse teniendo en mente la posibilidad de implementarlo con un modelo Entidad/Relacional, que para evitar problemas de integridad deberá soportar directamente a nivel de base de datos (no a capas superiores) las relaciones de jerarquía y dependencia o condicionalidad, así como las restricciones de cardinalidad de e-EMGDE. Dada la complejidad de e-EMGDE, no es evidente conseguir un esquema con dichas características, pero debería ser posible.

Para concluir, es interesante plantearse el siguiente debate: ¿se usará el esquema para describir objetos en una aplicación de gestión documental (caso que hemos supuesto en esta ponencia, por ser el que cubre actualmente la NTI de Política de Gestión), o en una aplicación de archivo electrónico, o en un sistema de información del negocio, o en un servidor web, o en una base de datos transaccional? Los esquemas normalmente se construyen para un objetivo específico (por ejemplo gestión documental o archivado), pero conviene tener una visión amplia y conocer las posibilidades de aplicación o traslación a diferentes campos de uso.

II. NOCIONES DE e-EMGDE

El Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE), que se desarrolla en la NTI de Política de Gestión de Documentos Electrónicos, establece:

i. El modelo conceptual en el que se apoya el modelo de metadatos, sus propiedades y su lógica subyacente.

ii. Descripción de cada uno de los elementos y sub-elementos de metadatos, a través de la descripción de cada una de sus características: definición, propósito, obligatoriedad, etc.

iii. Los esquemas de valores necesarios para cumplimentar los valores de los elementos de metadatos pertinentes.

iv. Las referencias a las normas utilizadas como base, así como a otras normas de posible utilidad.

El e-EMGDE sigue una aproximación multi-entidad, y se aplica a diferentes tipos de entidad (documento, agente, actividad, regulación, relación), conforme al siguiente modelo E-R:

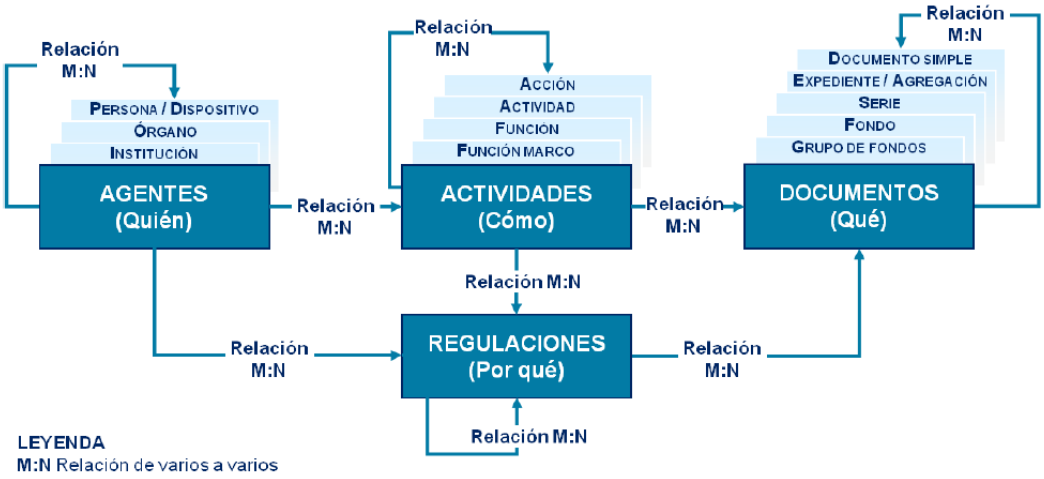


Figura 1

El esquema de metadatos consta de **23 elementos** (atributos de las entidades del modelo E/R), que para cada entidad **pueden ser Obligatorios, Condicionales u Opcionales**. Dependiendo del tipo de implantación se dividen en:

1. **OBLIGATORIOS** (esenciales): ***7 elementos***

   Categoría, Identificador, Fechas, Entidad Relacionada, Características técnicas, Firma, Tipo Documental, y Estado de elaboración.

2. **CONDICIONALES** (su uso depende del tipo de entidad que se esté describiendo y el contexto en que ésta funciona): ***11 elementos***

   Tipo de entidad, Nombre, Seguridad, Derechos de acceso, uso y reutilización, Contacto, Idioma, Calificación, Verificación de integridad, Trazabilidad y Clasificación.

3. **OPCIONALES** (pueden utilizarse bajo circunstancias en que se requiera una descripción más detallada): ***5 elementos*.**

   Descripción, Jurisdicción, Puntos de acceso, Ubicación y Prioridad.

– Parte de los elementos se subdividen en **sub-elementos**, hasta un total de 49. Estos a su vez pueden contener sub-sub-elementos (existen 14).

– Los sub-elementos no pueden usarse por sí solos, sino que tiene que existir el elemento de nivel superior.

III. PLANTEAMIENTO DE LA ESTRATEGIA DE IMPLANTACIÓN DE e-EMGDE

A pesar de su clara orientación multi-entidad, el esquema propuesto contempla y facilita su **implementación mono-entidad**, focalizada en los Documentos, en aquellas organizaciones que pretendan realizar una adecuación al Esquema Nacional de Interoperabilidad con un esfuerzo de desarrollo más moderado. Esta será la aproximación que propondríamos, de ser posible, para la adaptación de los gestores documentales del Departamento Ministerial a los requisitos del Esquema Nacional de Interoperabilidad.

No obstante, como se verá a lo largo de la presente ponencia, para cumplir con los requisitos de las NTI de Documento Electrónico, Expediente Electrónico, Copiado y Conversión, y Digitalización de Documentos, **es necesario contemplar algunos metadatos que en e-EMGDE obligan a disponer también de las entidades: Regulación, Agente, Actividad y Relación.**

Por tanto, se adoptará una **aproximación de e-EMGDE multi-entidad**, haciendo especial énfasis en la entidad "Documento", y limitando al mínimo imprescindible las informaciones recogidas en el resto de entidades.

Téngase en cuenta que, como se puede observar en el modelo E-R anterior de la Figura 1, la entidad "Documento" no se refiere únicamente a Documentos Electrónicos en sentido estricto, sino que también permite almacenar Grupos de Fondos, Fondos, Series Documentales, Expedientes o Agregaciones, y esta arquitectura está concebida para facilitar la herencia de metadatos o propiedades (por ejemplo, de una serie documental a los documentos que pertenezcan a ella), si así se estableciera en un organismo.

En el modelo de datos que implemente el SGDE, la entidad "Documento" contendrá auto-relaciones (relaciones de una entidad consigo misma), del tipo "contiene", para permitir la descripción de la pertenencia de un documento a:

- Clasificaciones Documentales (grupo de fondos, fondos, o series),
- Expedientes
- o Agregaciones de Documentos (que a diferencia de los expedientes, no están ligadas a un procedimiento administrativo).

En definitiva, las auto-relaciones de la entidad "Documento" permiten vincular los documentos que forman parte de una serie de documental, o los documentos que constituyen un expediente, soportando la estructura de clasificación documental que se representa en el siguiente diagrama:

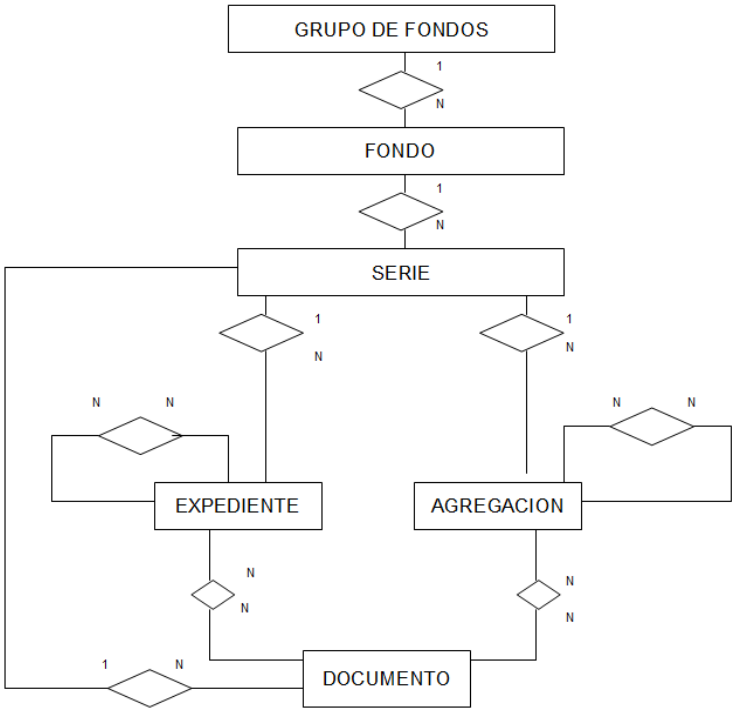


Figura 2

Nuestra estrategia de implementación implica que sólo será necesario soportar los metadatos obligatorios, así como los metadatos complementarios que se estimen convenientes para el Departamento Ministerial, y que apliquen a las 5 entidades de e-EMGDE: Documento, Agente, Actividad, Regulación y Relación.

III.1. METADATOS OBLIGATORIOS ENTIDAD DOCUMENTO

Se define "Documento" en eEMGDE como: *información estructurada en cualquier formato creada, recibida y mantenida como evidencia por una organización o persona en cumplimiento de obligaciones legales o para actuaciones de gestión.*

Los metadatos obligatorios de e-EMGDE para la entidad Documento son los siguientes:

Elemento	Descripción
Categoría (eEMGDE1)	Valor del tipo de entidad que se está describiendo (para la entidad Documento, podrá ser: Documento simple, Agregación, Expediente, Fondo, Serie, o Grupo de Fondos)
Identificador (eEMGDE2)	Identificador único asociado a una entidad – En el caso de los documentos, este metadato coincide con el metadato obligatorio homónimo de la NTI de Documentos Electrónicos. Si se trata de un expediente, este metadato coincide con el metadato obligatorio homónimo de la NTI de Expedientes Electrónicos. Este metadato consta de dos subelementos: – eEMGDE2.1 - Secuencia de identificador – eEMGDE2.2 – Esquema de identificador
Fechas (eEMGDE4)	Debe utilizarse este elemento siempre que se asignen fechas a una entidad. Permite recoger fechas asociadas a un evento concreto relacionado con la entidad que describe. – Consta de dos sub-elementos: “FECHA INICIO” y “FECHA FIN”, que recogen respectivamente la fecha de inicio de la existencia de un documento, y su fecha de destrucción o de fin de su existencia.
Características técnicas (eEMGDE14)	Información acerca de la forma lógica y otras características técnicas lógicas y físicas de un documento digital o digitalizado. Tiene los siguientes sub-elementos: – Soporte origen. – Nombre de formato. – Versión de formato. – Nombre de la aplicación de creación. – Versión de la aplicación de creación. – Registro de formatos (no aplica en nuestro caso) – Resolución – Tamaño
Firma (eEMGDE17)	Método para fijar las condiciones de fiabilidad y autenticidad de un documento. Está integrado por los siguientes sub-elementos: – Tipo de firma – Formato de firma – Rol de firma
Tipo Documental (eEMGDE18)	Modelo estructurado y reconocido que adopta un Documento, en el desarrollo de una competencia concreta, en base a una Regulación y cuyo formato, contenido informativo o soporte son homogéneos. – Este metadato coincide con el metadato obligatorio homónimo de la NTI de Documentos Electrónicos
Estado de elaboración (eEMGDE20)	Indicación del estado de la situación de elaboración de un documento, a saber, original o los distintos tipos identificados de copia. – Este metadato coincide con el metadato obligatorio homónimo de la NTI de Documentos Electrónicos

Así pues, deberán implementarse en los gestores documentales los siguientes **metadatos obligatorios** y sub-elementos asociados para la entidad Documento (donde se han excluido aquellos sub-elementos no obligatorios que a nuestro juicio no aportan valor, o no resultan

imprescindibles para la adecuación al ENI, como veremos en los apartados posteriores de esta ponencia):

- eEMGDE 1 – Categoría
- eEMGDE2 – Identificador
  - eEMGDE2.1 – Secuencia de Identificador
  - eEMGDE2.2 – Esquema de identificador
- eEMGDE4 – Fechas
  - eEMGDE4.1 – Fecha Inicio
  - eEMGDE4.2 – Fecha fin (éste sub-elemento se rellenará cuando finalice la existencia de una Entidad –documento- o de una Relación).
- eEMGDE14 – Características Técnicas
  - eEMGDE14.1 – Soporte origen
  - eEMGDE14.2 – Nombre de formato
  - eEMGDE14.3 - Versión de formato
  - eEMGDE14.4 – Nombre de la aplicación de creación
  - eEMGDE14.5 – Versión de la aplicación de creación
  - eEMGDE14.7 - Resolución
  - eEMGDE14.8 - Tamaño
- eEMGDE17 – Firma
  - eEMGDE17.1 – Tipo de Firma
  - eEMGDE17.2 – Formato de Firma
  - eEMGDE17.3 – Rol de Firma
- eEMGDE18-Tipo Documental
- eEMGDE20 – Estado de Elaboración
  - eEMGDE20.1 – Denominación del Estado
  - eEMGDE20.2 – Características de la Copia

III.2. METADATOS OBLIGATORIOS ENTIDAD REGULACIÓN

Se define “Regulación” en eEMGDE como: *marco normativo, incluidos los requisitos de gestión de documentos, tales como ordenamiento jurídico, normativa, política, etc. Las posibles categorías sobre este tipo de entidad son definidas por cada organización en función de sus necesidades y normativas específicas.*

Por la información que figura en distintos apartados de la documentación del Esquema de metadatos e-EMGDE, la entidad Regulación aplica no sólo a normativa, sino también a pro-

cedimientos administrativos (aquellas secuencias de trámites administrativos que terminan en una resolución declaratoria o denegatoria de derechos u obligaciones y son susceptibles de recurso.)

Elemento	Descripción
Categoría (eEMGDE1)	Valor del tipo de entidad que se está describiendo. Las posibles categorías para la entidad Regulación son definidas por cada organización en función de sus necesidades y normativas específicas. Las siete categorías que se prevén imprescindibles son: - normativa para la atribución de competencias en cuanto a la generación de copias auténticas. - otra normativa interna que regula una actividad. - normativa externa que regula una actividad. - Norma Técnica de Interoperabilidad. - otras normas de carácter general. - procedimiento administrativo interno (si tienen como destinatario a una unidad administrativa o empleado público). - procedimiento administrativo externo (si tienen como destinatario al ciudadano o a las empresas).
Identificador (eEMGDE2)	Identificador único asociado a una entidad Este metadato consta de dos subelementos: - eEMGDE2.1 - Secuencia de identificador - eEMGDE2.2 – Esquema de identificador
Fechas (eEMGDE4)	Debe utilizarse este elemento siempre que se asignen fechas a una entidad. Permite recoger fechas asociadas a un evento concreto relacionado con la entidad que describe - Consta de dos sub-elementos: “FECHA INICIO” y “FECHA FIN”, que recogen respectivamente la fecha de inicio de la existencia de una regulación, y su fecha de fin de existencia.

Así pues, deberán implementarse en los gestores documentales los siguientes **metadatos obligatorios** y sub-elementos asociados para la entidad Regulación (donde se han excluido aquellos sub-elementos no obligatorios que a nuestro juicio no aportan valor, o no resultan imprescindibles para la adecuación al ENI, como veremos en los apartados posteriores de esta ponencia):

- eEMGDE1 – Categoría
- eEMGDE2 – Identificador
  - eEMGDE2.1 – Secuencia de Identificador
  - eEMGDE2.2 – Esquema de identificador
- eEMGDE4 – Fechas
  - eEMGDE4.1 – Fecha Inicio
  - eEMGDE4.2 – Fecha fin (este sub-elemento se rellenará cuando finalice la existencia de una Entidad.

III.3. METADATOS OBLIGATORIOS ENTIDAD AGENTE

Se define “Agente” en e-EMGDE como: *Institución, persona física o jurídica responsable o involucrada en la creación, producción, custodia o gestión de documentos*.

Un agente sería el Productor, en terminología archivística.

Los metadatos obligatorios de e-EMGDE para la entidad Agente son los siguientes:

Elemento	Descripción
Categoría (eEMGDE1)	Valor del tipo de entidad que se está describiendo (para la entidad Agente, podrá ser: Institución, Órgano, Persona, o Dispositivo)
Identificador (eEMGDE2)	Identificador único asociado a una entidad Consta de dos subelementos: – eEMGDE2.1 - Secuencia de identificador – eEMGDE2.2 – Esquema de identificador
Fechas (eEMGDE4)	Fecha asociada a un evento concreto relacionado con la entidad que describe. – Consta de dos sub-elementos: “FECHA INICIO” y “FECHA FIN”, que recogen respectivamente la fecha de inicio de la existencia de un Agente, y su fecha de destrucción o de fin de su existencia.

Así pues, deberán implementarse en los gestores documentales los siguientes **metadatos obligatorios** y sub-elementos asociados para la entidad Agente (donde se han excluido aquellos sub-elementos no obligatorios que a nuestro juicio no aportan valor, o no resultan imprescindibles para la adecuación al ENI, como veremos en los apartados posteriores de esta ponencia):

- eEMGDE1 – Categoría
- eEMGDE2 – Identificador
  - eEMGDE2.1 – Secuencia de Identificador
  - eEMGDE2.2 – Esquema de Identificador: para una persona, se trataría del esquema del Número de Registro de Personal, y para una organización, el esquema del código de órgano.
- eEMGDE4 – Fechas
  - eEMGDE4.1 – Fecha Inicio
  - eEMGDE4.2 – Fecha fin (este sub-elemento se rellenará cuando finalice la existencia de una Entidad –agente-).

III.4. METADATOS OBLIGATORIOS ENTIDAD ACTIVIDAD

Se define “Actividad” en e-EMGDE como: *Responsabilidad ejecutada por o asignada a una entidad Agente*.

Los metadatos obligatorios de e-EMGDE para la entidad Actividad son los siguientes:

Elemento	Descripción
Categoría (eEMGDE1)	Valor del tipo de entidad que se está describiendo (para la entidad Actividad, podrá ser: Función Marco, Función, Actividad, Acción) Una "función marco" en un cuadro de clasificación se correspondería, por ejemplo, a funciones principales: gestión de personal. Una "función" derivaría de una función marco, por ejemplo contratación de personal. Una "actividad" se derivaría de una función, por ejemplo pruebas selectivas, y una "acción" de una actividad, por ejemplo evaluación de pruebas selectivas. En los cuadros de clasificación, si ponemos por caso el de la Universidad de Navarra, se establecen 4 categorías: Clase/Subclase/División/Serie. En otros modelos de cuadros de clasificación se cambian las denominaciones de categorías, pero se mantiene generalmente la división en 4 categorías. Es preciso determinar si la concordancia entre las cuatro categorías de la entidad Actividad y las categorías del Cuadro de Clasificación del Ministerio de Hacienda y Administraciones Públicas.
Identificador (eEMGDE2)	Identificador único asociado a una entidad Consta de dos subelementos: – eEMGDE2.1 – Secuencia de Identificador. – eEMGDE2.2 – Esquema de Identificador: cuadro de clasificación funcional de una organización.
Fechas (eEMGDE4)	Fecha asociada a un evento concreto relacionado con la entidad que describe. Consta de dos sub-elementos: "FECHA INICIO" y "FECHA FIN", que recogen respectivamente la fecha de inicio de la existencia de una Actividad, y su fecha de destrucción o de fin de su existencia.

Así pues, deberán implementarse en los gestores documentales los siguientes **metadatos obligatorios** y sub-elementos asociados para la entidad Actividad (donde se han excluido aquellos sub-elementos no obligatorios que a nuestro juicio no aportan valor, o no resultan imprescindibles para la adecuación al ENI, como veremos en los apartados posteriores de esta ponencia):

- eEMGDE1 – Categoría
- eEMGDE2 – Identificador
  - eEMGDE2.1 – Secuencia de Identificador
  - eEMGDE2.2 – Esquema de Identificador: cuadro de clasificación funcional de una organización
- eEMGDE4 – Fechas
  - eEMGDE4.1 – Fecha Inicio
  - eEMGDE4.2 – Fecha fin (este sub-elemento se rellenará cuando finalice la existencia de una Entidad –actividad–).

III.5. METADATOS OBLIGATORIOS ENTIDAD RELACIÓN

Se define “Relación” en e-EMGDE como: Asociación entre dos o más entidades que tiene relevancia en un contexto de gestión y/o de gestión de documentos.

Los metadatos obligatorios de e-EMGDE para la entidad Relación son los siguientes:

Elemento	Descripción
Categoría (eEMGDE1)	Valor del tipo de entidad que se está describiendo (para la entidad Relación, podrá ser: – Acción de gestión de documentos (como la clasificación, calificación, conservación o transferencia). – Relación de procedencia (como las relaciones de propiedad, sucesión o asociativas). Ambos tipos tienen un esquema de nombres definido en los Apéndices 6 y 7 de eEMGDE respectivamente, que son extensibles según las necesidades de la organización.
Identificador (eEMGDE2)	Identificador único asociado a una entidad Consta de dos subelementos: – eEMGDE2.1 – Secuencia de Identificador – eEMGDE 2.2 – Esquema de Identificador: vocabulario controlado de las relaciones en una organización, o la configuración del sistema de nombrado de relaciones de una aplicación dada.
Fechas (eEMGDE4)	Fecha asociada a un evento concreto relacionado con la entidad que describe. – Consta de dos sub-elementos: “FECHA INICIO” y “FECHA FIN”, que recogen respectivamente la fecha de inicio de la existencia de un Agente, y su fecha de destrucción o de fin de su existencia.
Entidad Relacionada (eEMGDE6)	Medio para identificar a otras entidades en una relación. Todas las descripciones de metadatos de relación implican a una entidad Relación, más otras dos entidades en cualquier combinación (por ejemplo, Agente-Documento). Este elemento permite describir el rol de cada entidad implicada en la relación y sirve para identificarlas (pero no para describirlas). – Consta de tres sub-elementos: – e-EMGDE6.1: ID de Entidad Relacionada. Figurará por duplicado, para cada una de las dos entidades diferentes a la entidad Relación que están implicadas en la relación – e-EMGDE6.2: Esquema de ID de Entidad Relacionada – e-EMGDE6.3: Rol de la relación, que podrá tener dos valores: “1”: indica que la relación se lee desde la entidad. “2”: indica que la relación se lee en dirección hacia la entidad

Así pues, deberán implementarse en los gestores documentales los siguientes **metadatos obligatorios** y sub-elementos asociados para la entidad Relación (donde se han excluido aquellos sub-elementos no obligatorios que a nuestro juicio no aportan valor, o no resultan imprescindibles para la adecuación al ENI, como veremos en los apartados posteriores de esta ponencia):

- eEMGDE 1 – Categoría
- eEMGDE2 – Identificador
  - eEMGDE2.1 – Secuencia de Identificador
  - eEMGDE 2.2 – Esquema de Identificador: vocabulario controlado de las relaciones en una organización, o la configuración del sistema de nombrado de relaciones de una aplicación dada.
- eEMGDE4 – Fechas
  - eEMGDE4.1 – Fecha Inicio
  - eEMGDE4.2 – Fecha fin (este sub-elemento se rellenará cuando finalice la existencia de una Entidad –relación-).
- eEMGDE6 – Entidad Relacionada
  - eEMGDE6.1 – ID de Entidad Relacionada.
  - eEMGDE6.2 – Esquema de ID de Entidad Relacionada.
- eEMGDE6.3 – Rol de la relación, que podrá tener dos valores:

    "1": indica que la relación se lee desde la entidad.

    "2": indica que la relación se lee en dirección hacia la Entidad.

III.6. METADATOS COMPLEMENTARIOS DE e-EMGDE

Los **metadatos complementarios** a incorporar en los gestores documentales serán aquellos que se identifiquen como necesarios para sustentar los Procesos de Gestión Documental establecidos en la NTI de Política de Gestión de Documentos Electrónicos, y que se identificarán en el apartado V de la presente ponencia.

III.7. OTRAS CONSIDERACIONES

En el plano organizativo, se deberá acordar en el ámbito de cada centro una propuesta respecto a qué sistema corresponde aportar la información correspondiente a cada metadato e-EMGDE: a la aplicación gestora del documento o del expediente electrónico, o bien al SGDE corporativo.

Como no podía ser de otra manera, hacemos constar que el conjunto de metadatos de e-EMGDE que se escoja para su implementación en el Departamento Ministerial, **deberá ser capaz de soportar todos los metadatos obligatorios de los Documentos Electrónicos y todos los metadatos obligatorios de los Expedientes Electrónicos** (definidos en la NTI de Documento Electrónico y la NTI de Expediente Electrónico respectivamente). Este es un requisito ineludible en cualquier plan de adecuación al ENI, y se refleja a continuación la correspondencia entre los metadatos mínimos obligatorios de documentos o expedientes electrónicos y los metadatos de e-EMGDE, tal y como se detalla en el Anexo a la NTI de Política de Gestión de Documentos Electrónicos:

DOCUMENTO ELECTRÓNICO	
Metadato	**Elemento / Sub-elemento e-EMGDE**
Versión NTI	**eEMGDE2.1 – Secuencia de identificador** (URI) de la Norma Técnica de Interoperabilidad de Documento electrónico, entendida como "Regulación", que a través de una "Relación" del tipo "documenta" está vinculada al "Documento".
Identificador	**eEMGDE2.1 – Secuencia de identificador.** Nota: Siendo el **eEMGDE2.2 – Esquema de identificador** del "Documento" = *ES_<Órgano>_<AAAA>_<ID_específico>*
Órgano	**2.1 – Secuencia de identificador** del "Agente" de tipo "Organización" que, a través de una "Relación" tipo "posee/controla/ es responsable de/ produce" está vinculado al "Documento". Nota: Siendo el **eEMGDE2.2 – Esquema de identificador** de la "Organización" = <Órgano>
Fecha de captura	**eEMGDE4.1 – Fecha de inicio** del Documento.
Origen	Elemento lógico que indicará el tipo de "Agente" que a través de una "Relación" de tipo "crea" está relacionado con el documento: - "0": Si es un ciudadano, el "Agente" será de tipo "Persona" con su identificador normalizado (*DNI, NIF, CIF, NIE* o similar). - "1": Si es una Administración, el "Agente" será de tipo "Organización" con su identificador normalizado (<*Órgano*>).
Estado de elaboración	Elemento que indicará el estado de elaboración del documento, siendo sus posibles valores: -Si "Original": **eEMGDE20.1 – Denominación del estado.** -Si existe una "Relación" de tipo "copia" entre el Documento y otro Documento que actúa de Original: **eEMGDE20.2.1 – Tipo de copia**, siendo **eEMGDE20.1 – Denominación del estado**="*Copia*".
Nombre de formato	**eEMGDE14.2 – Nombre de formato** lógico de cada fichero de contenido.
Tipo documental	**eEMGDE18 – Tipo documental** del Documento.
Tipo de firma	Si CSV, 'CSV'.
	Si Firma Electrónica basada en certificados: **eEMGDE17.1 - Tipo de firma.** Siendo **eEMGDE17- Firma** = '*Firma electrónica basada en certificados*'
Valor CSV	**eEMGDE16.2 - Valor** ="Valor CSV". Siendo: **eEMGDE16.1 – Algoritmo** = "*CSV*".
Definición generación CSV	**eEMGDE2.1 – Secuencia de identificador** de la "Actividad" que, mediante la "Relación" correspondiente, aplica a la generación del CSV del "Documento".

Figura 3

EXPEDIENTE ELECTRÓNICO	
Metadato	**Elemento / Sub-elemento e-EMGDE**
Versión NTI	**eEMGDE2.1 – Secuencia de identificador** (URI) de la Norma Técnica de Interoperabilidad de Expediente electrónico, entendida como "Regulación", que a través de una "Relación" del tipo "documenta" está vinculada al "Expediente".
Identificador	**eEMGDE2.1 – Secuencia de identificador.** Nota: Siendo el **eEMGDE2.2 – Esquema de identificador** del "Expediente"= *ES_<Órgano>_<AAAA>_<ID_específico>*
Órgano	**eEMGDE2.1 - Secuencia de identificador** del "Agente" de tipo "Organización" que, a través de una "Relación" tipo "posee/controla/ es responsable/produce de" está vinculado al "Expediente". Nota: Siendo el **eEMGDE2.2 – Esquema de identificador** de la "Organización" = *<Órgano>*
Fecha apertura del expediente	**eEMGDE4.1 – Fecha de inicio** del Expediente.
Clasificación	**eEMGDE2.1 – Secuencia de identificador** de la "Actividad" que, mediante la "Relación" correspondiente, aplica al "Expediente". Nota: Siendo el **eEMGDE2.2 – Esquema de identificador** de la "Actividad" = *<Esquema_procedimientos_organizacion>*
Estado	Elemento que indicará el estado del expediente, siendo sus posibles valores: - "Abierto": Si no existe **eEMGDE4.2 – Fecha de fin** del expediente. - "Cerrado": Si existe **eEMGDE4.2 – Fecha de fin** del expediente.
Interesado	- Si "ciudadano o persona jurídica": **eEMGDE2.1 – Secuencia de identificador** del "Agente" de tipo "Persona" que, a través de una "Relación" tipo "solicita" está vinculado al "Expediente". - Si "organización": **eEMGDE2.1 – Secuencia de identificador** del "Agente" de tipo "Organización" que, a través de una "Relación" tipo "solicita" está vinculado al "Expediente". Nota: Siendo el **eEMGDE2.2 – Esquema de identificador** de la "Organización" = *<Órgano>*
Función resumen foliado	**eEMGDE16.1 – Algoritmo** empleado para la generación de las huellas de los documentos incluidos en el expediente.
Tipo de firma	Elemento que indicará el tipo de firma del índice del expediente electrónico, siendo sus posibles valores: -Si CSV: **eEMGDE17.1 – Tipo de firma** = *'CSV'*. - Si Firma electrónica basada en certificados: **eEMGDE17.2 – Formato de firma** siendo **eEMGDE17.1 – Tipo de firma** = *'Firma electrónica avanzada basada en certificados'*.
Valor CSV	Si **eEMGDE17.1 – Tipo de firma** = *'CSV'*: **eEMGDE16.2 – Valor** ="*Valor CSV*".
	Siendo: **eEMGDE16.1 – Algoritmo** = "*CSV*". **eEMGDE17.1 – Tipo de firma** = *'CSV'*.
Definición generación CSV	**eEMGDE2.1 – Secuencia de identificador** de la "Actividad" que, mediante la "Relación" correspondiente, aplica a la generación del CSV del "Expediente". Nota: Siendo el **eEMGDE17.1 – Tipo de firma** = *'CSV'*.

Tabla 120. Correspondencia de los metadatos mínimos obligatorios de Expediente electrónico con el

Figura 4

Asimismo, el esquema institucional de metadatos deberá soportar, como requisito obligatorio, los **metadatos complementarios de Digitalización de Documentos, y de Conversión de Documentos**, cuya concordancia con el e-EMGDE se refleja a continuación:

DIGITALIZACIÓN DE DOCUMENTOS	
Metadato	**Elemento / Sub-elemento e-EMGDE**
Resolución	eEMGDE14.7 - Resolución.
Tamaño	eEMGDE14.8.2 - Tamaño Lógico. eEMGDE14.8.4 - Unidades.
Idioma	eEMGDE11 - Idioma.

Figura 5

CONVERSIÓN ENTRE DOCUMENTOS ELECTRÓNICOS	
Metadato	**Elemento / Sub-elemento e-EMGDE**
Identificador del documento origen	eEMGDE2.1 - Secuencia de identificador del "Documento" que, a través de una "Relación" tipo "convierte" indica el documento origen de la copia. Nota: Siendo el eEMGDE2.2 - Esquema de identificador del "Documento" origen= *ES_<Órgano_responsable>_<AAAA>_<ID_específico>*
Política de conversión	eEMGDE2.1 - Secuencia de identificador que identifique la Política, tratada como una "Regulación" que se relaciona con tipo "Conversión" con el "Documento". Nota: Siendo el eEMGDE2.2 - Esquema de identificador de la "Regulacion" = *<Esquema_regulaciones_organizacion>*

Figura 6

IV. PROCESOS DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS

Presentamos a continuación, a modo de síntesis, los principales requisitos en relación a los procesos de gestión documental que vienen establecidos en la NTI de Política de Gestión de Documentos Electrónicos o bien en su Guía de Aplicación

La gestión de documentos electrónicos se concretará en un programa de tratamiento específico para la gestión de documentos electrónicos de cada organización.

El programa de tratamiento consistirá en la articulación y posterior aplicación de una serie de procedimientos o **secuencia coordinada de procesos, técnicas y operaciones de gestión de documentos**.

El programa de tratamiento **se aplicará de manera contínua sobre el ciclo de vida de los documentos y expedientes electrónicos** para los que se garantizará su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad; permitiendo la protección, recuperación y conservación de los documentos y su contexto.

El **programa de tratamiento** incluye los siguientes procesos de gestión de documentos:

1. **Captura de documentos**, que incluirá la asignación de los metadatos mínimos obligatorios de la *NTI de Documento Electrónico*.

2. **Registro de documentos**, que proporciona evidencia de la entrada y la salida de un documento en la organización y es un requisito legal definido en la legislación de procedimiento administrativo (ley 30/92). El registro consiste en la introducción de una breve información descriptiva –asiento-, con el contenido definido en el artículo 38.3 de la ley 30/92, y la asignación de un identificador en el sistema (que forma parte de los metadatos mínimos obligatorios de documento electrónico, y queda por tanto cubierto por el proceso de captura de documentos). Además del tratamiento de documentos electrónicos recibidos, la ley 11/2007 permite digitalizar documentos en papel, de acuerdo con la *NTI de Digitalización de Documentos*.

3. **Clasificación de documentos** según criterios de actividad de acuerdo con el cuadro de clasificación funcional de cada organización. Incluirá los criterios de formación de expedientes y agrupaciones de documentos electrónicos según la *NTI de Expediente Electrónico*.

4. **Descripción de documentos:** permitirá la recuperación de los mismos y su contexto, y atenderá a la aplicación del esquema institucional de metadatos.

   La descripción de documentos se nutre de los metadatos para la gestión de documentos electrónicos definidos en cada organización para ajustarse a sus particularidades y necesidades específicas.

5. **Acceso a los documentos**, que contemplará la posible regulación institucional de dicha práctica, así como la trazabilidad de las acciones que se realizan sobre cada uno de ellos.

6. **Calificación de los documentos**, que incluye: determinación de los **documentos esenciales**, de los **plazos de conservación**, y **dictamen de la autoridad calificadora**.

   - Determinación de los documentos esenciales (para los que se recomienda medidas de protección reforzadas)
   - valoración de documentos y determinación de los plazos de conservación (para ello, se pueden crear comisiones calificadoras que determinen el valor legal, jurídico, fiscal, administrativo, archivístico y social de cada documento).
   - El dictamen puede definirse como la regulación de las transferencias o la eliminación de los documentos de los sistemas en uso, cuando los valores probatorios han prescrito y/o han transcurrido los plazos para su conservación.

7. **Conservación de los documentos,** en función de su valor y tipo de dictamen de la autoridad calificadora, a través de la definición de calendarios de conservación**.**

   - Ejemplos de situaciones que requieren métodos de conservación: cuando el soporte y formato de los documentos necesiten ser renovados, cuando es necesario migrar documentos de una estructura a otra, cuando con el estado actual de la técnica es imposible conservar la firma a largo plazo.

8. **Transferencia de documentos**, que incluirá las consideraciones para la transferencia entre repositorios así como las responsabilidades en cuanto a su custodia.

9. **Destrucción o eliminación de los documentos**, atendiendo a la normativa aplicable en materia de eliminación de Patrimonio Documental, y donde se aplicarán las medidas de seguridad relacionadas definidas en el ENS: “Borrado y destrucción” del capítulo **[mp.si]**, y “Limpieza de documentos” del capítulo **[mp.info]**

V. ANÁLISIS DE LOS PROCESOS DE GESTIÓN DE DOCUMENTOS A LO LARGO DE SU CICLO DE VIDA Y DETERMINACIÓN DEL CONJUNTO DE METADATOS PRECISO PARA GESTIONAR LAS DIFERENTES TRANSACCIONES

V.1. CAPTURA DE DOCUMENTOS:

a. DETERMINACIÓN DE LOS DOCUMENTOS QUE DEBERÍAN INCORPORARSE AL SGDE

La determinación de los documentos que deben incorporarse a un SGDE debería basarse en el análisis del marco reglamentario, de las necesidades de gestión y rendición de cuentas y del riesgo que supondría no incorporar los documentos o dejar constancia de su existencia.

Las decisiones acerca de la incorporación o no de los documentos al SGDE debe fundamentarse en un análisis previo de la actividad de la organización y de las responsabilidades que ésta asuma a lo largo del tiempo. La identificación de los documentos y de su plazo de conservación se materializará en un instrumento formal: el calendario de conservación.

Como ejemplo de documentos que no requieren una incorporación formal, se pueden citar aquellos que:

A. No obligan a una organización o individuo a emprender una acción determinada;

B. No documentan una obligación o responsabilidad; o

C. No contienen información relacionada con la actividad de la que la organización es responsable.

Los documentos se crean y se reciben en diferentes soportes y formatos mediante el uso de tecnologías que están en constante evolución. Un documento refleja un acto o actividad de una organización, es una constancia de tales actos o decisiones. Por tanto el contenido no es dinámico, pero sí lo pueden ser los metadatos no obligatorios. Los formatos en que son creados los documentos y sus metadatos evolucionan a lo largo del tiempo, y si deben conservarse esos documentos, es necesario garantizar que se preservarán en el formato en que estén, salvo que estos formatos deban ser migrados a lo largo del tiempo para garantizar su accesibilidad, o se decida transformarlos desde su inicio a un formato de preservación a largo plazo (como PDF/A).

Las actividades propias de una organización deberían fijarse en documentos asociados con metadatos que reflejen su contexto específico cuando impliquen acción o responsabilidad o documenten una acción, una decisión o un proceso de toma de decisiones.

b. REQUISITOS DE LA CAPTURA DE DOCUMENTOS

La finalidad de la incorporación de documentos a un SGDE es, según la ISO 15489:

- Establecer una relación entre el documento, su productor y el contexto en que se originó;
- Situar el documento y sus relaciones en el sistema de gestión;
- Asociarlo a otros documentos (expedientes, series y/o fondos)

Este proceso se realizará mediante la asignación de metadatos explícitos, asociados a un documento y almacenados en un repositorio e-EMGDE.

En primer lugar, el SGDE implementará los metadatos mínimos obligatorios de la NTI de documento electrónico y la NTI de Expediente Electrónico, cuya correspondencia con el e-EMGDE se describe en las tablas 119 y 120 del “Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE)”, y en las figuras 3 y 4 del presente documento.

Por otro lado, se deberán implementar en el proceso de Captura de Documentos los metadatos de e-EMGDE que soporten las siguientes acciones:

A. **Situar el documento en relación con el proceso de gestión** donde se originó o al cual se incorpora. Si el documento o expediente está asociado a un procedimiento administrativo, en esta fase se establecerá una relación de tipo “es controlado por” entre la instancia de “Documento” correspondiente al documento electrónico o expediente en cuestión, y una ocurrencia de una entidad “Regulación”, cuyo metadato eEMGDE 2.2-SECUENCIA DE IDENTIFICADOR apuntará a:

   - un registro de la tabla que contiene un duplicado del Sistema de Información Administrativa, la cual tendrá como clave primaria el valor del código identificativo del procedimiento administrativo.
   - o bien a un registro de la tabla que contendrá la relación de procedimientos de carácter interno del organismo que no estén recogidos todavía en el SIA (Sistema de Información Administrativa), en su caso.

   Si el documento o expediente está asociado a otras normativas (como normativas internas de atribución de competencias de digitalización, normas legales, etc), se

crearán tantas relaciones de tipo “es controlado por”, entre la instancia de “Documento” y las instancias de “Regulación” pertinentes, como sean necesarias.

Por otro lado, es preciso establecer una relación de tipo “asociada con” entre la instancia de “Documento” y la instancia de “Actividad” que establezca su alineación con el cuadro de clasificación documental.

Como una instancia de la entidad “Documento” puede estar asociada a otras instancias de “Documento” cuya categoría sea de tipo Grupo de Fondos, Fondo o Serie, se podría conocer tanto el procedimiento administrativo que origina o al cual se incorpora el documento, como su ubicación en el cuadro de clasificación documental.

Asimismo, se identificará la aplicación que ha creado el documento, que será reflejada en el metadato eEMGDE 14.4 de la entidad Documento, así como la versión de dicha aplicación, que se recogerá en el metadato eEMGDE 14.5, en su caso.

B. **Asociar a otros documentos formando parte de un expediente o agrupación documental**: en caso de que se conozca desde el momento de la captura del documento el expediente al que pertenece, se asociará la ocurrencia de la entidad “Documento” correspondiente a tal documento electrónico, a la instancia de la entidad “Documento” correspondiente a su expediente respectivo, mediante una relación de tipo “Contiene”. Por otro lado, si se desconoce el expediente al que pertenece un documento electrónico, o bien si se trata de un documento que no está englobado en un expediente, se asociará la ocurrencia de la entidad “Documento” a una ocurrencia correspondiente a una agrupación documental (Grupo de Fondo, Fondo, Serie, o Agregación), en su caso.

C. **Identificar los plazos de las acciones dictaminadas**: en la fase de captura del documento se generará el metadato eEMGDE13 “Calificación”, quedando habitualmente pendientes de completar los sub-elementos eEMGDE13.1 “Valoración” y eEMGDE 13.2 “Dictamen”. En cuanto al elemento “Valoración”, se le asignará el valor por defecto “Sin cobertura de calificación” en tanto no se disponga del dictamen de la autoridad calificadora.

   El SGDE permitirá verificar la validez de una firma electrónica en el momento de la captura del documento de archivo. Además, el SGDE deberá recoger información relativa a las firmas del documento en el metadato eMGDE17-“FIRMA” (con sus subelementos, referentes al Tipo de Firma, Formato de Firma y Rol de Firma). Asimismo, en el caso de que se utilice firma electrónica mediante CSV (código seguro de verificación), también se deberá emplear el metadato eMGDE16-“VERIFICACION DE INTEGRIDAD”, incluyendo en eMGDE16.2-“Valor” el valor del CSV y consignando en eMGDE16.1-“Algoritmo” la cadena “CSV”.

V.2. REGISTRO DE DOCUMENTOS:

De acuerdo con la legislación de procedimiento administrativo (ley 30/92), los órganos administrativos llevarán un **registro general en el que se hará el correspondiente asiento de todo escrito o comunicación** que sea presentado o que se reciba en cualquier unidad administrativa propia. También se anotarán en el mismo, la salida de los escritos y comunicaciones oficiales dirigidas a otros órganos o particulares.

El registro de un documento consiste en la introducción de una **breve información descriptiva (asiento), con el contenido definido en el artículo 38.3 de la ley 30/92, y la asignación de un identificador en el sistema** (que forma parte de los metadatos mínimos obligatorios de documento electrónico, y queda por tanto cubierto por el proceso de captura de documentos).

Existe un metadato opcional de e-EMGDE, eMGDE5-“DESCRIPCION”, que permite introducir información en texto libre relativa a una entidad. Proponemos incorporar este metadato en el repositorio e-EMGDE del Sistema de Gestión Documental, con la finalidad de permitir a las aplicaciones de gestión del Departamento Ministerial introducir, si procede, el apunte del asiento en Registro Electrónico correspondiente al documento. Si el documento no ha ingresa-

do a través de un Registro Electrónico, las aplicaciones gestoras podrán introducir cualquier información descriptiva en el metadato e-EMGDE5, como: resumen del texto, fecha de creación, autor, remitente, destinatario, etc. El título del documento (por ejemplo “Instancia de solicitud de licencia de obras”) se recogerá en el metadato eEMGDE3.1-Nombre natural.

Además del tratamiento de documentos electrónicos recibidos, la ley 11/2007 permite digitalizar documentos en papel, de acuerdo con la *NTI de Digitalización de Documentos*.

En caso de que se lleve a cabo una **digitalización de documentos** en papel presentados por ciudadanos coincidiendo con el proceso de registro, se cumplimentarán los siguientes metadatos (siempre que sea posible, de manera automática):

1. eEMGDE14.7, que se corresponde con la Resolución.
2. eEMGDE14.8, que se corresponde con el Tamaño.
3. eEMGDE11, que se corresponde con el Idioma.

Para concluir, es necesario indicar que el procedimiento de registro deberá **asegurar que no puedan llevarse a cabo operaciones relacionadas con el documento antes de que se haya completado el registro.**

V.3. CLASIFICACIÓN DE DOCUMENTOS:

De acuerdo con la Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos, la Clasificación de Documentos se efectuará según criterios de actividad, de acuerdo con el cuadro de clasificación funcional de cada organización, e incluirá los criterios de formación de expedientes y agrupaciones de documentos electrónicos según la NTI de Expediente Electrónico.

Un sistema de clasificación basado en las funciones de la organización puede proporcionar un marco sistemático para la gestión de documentos. La elaboración de un Cuadro de Clasificación de documentos (instrumento lógico que muestra la organización de los documentos en base a las funciones propias del organismo productor de los mismos) es imprescindible para las tareas de Conservación y Selección de documentos y sirve de sustento a los estudios de Valoración Documental. Asimismo, un Cuadro de Clasificación documental permitiría precisar rigurosamente las fases activa, semiactiva e inactiva de los documentos, con la ventaja añadida de que esto facilita la definición de una arquitectura de “data protection” (protección de datos), o backup-almacenamiento, acorde con la utilidad de los datos/documentos.

El cuadro de clasificación es una herramienta de apoyo para muchos de los procesos de gestión de documentos, como (ver norma ISO 15489):

A. el establecimiento de vínculos entre documentos individuales que reunidos proporcionan una representación continua de la actividad;
B. la garantía de que los documentos se denominan de manera coherente a lo largo del tiempo;
C. la ayuda a la recuperación de todos los documentos relacionados con una función o una actividad concretas;
D. la definición de niveles de seguridad y acceso adecuados para conjuntos de documentos;
E. la atribución de permisos de acceso a los usuarios para acceder a determinados grupos de documentos u operar en los mismos;
F. la distribución de la responsabilidad de la gestión de determinados grupos de documentos;
G. la distribución de los documentos para la realización de las tareas oportunas; y
H. el establecimiento de plazos y medidas de conservación y transferencia o destrucción de documentos.

Además, los cuadros de clasificación pueden complementarse con vocabularios controlados, adecuados a los documentos específicos de una organización, que fomentan la consistencia de los títulos y las descripciones, facilitando así la recuperación y el uso de los documentos.

Una vez determinado el Cuadro de Clasificación del Organismo, se deberá aplicar un proceso de clasificación funcional para cada documento que se incorpore al SGDE, utilizando para cada instancia de "Documento" que se incorpore al SGDE una vinculación con una instancia de "Actividad", que contendrá el código del cuadro de clasificación en el metadato eEMGDE22-Clasificación.

De acuerdo con la norma ISO 30301, el esquema de agrupación (cuadro de clasificación) de los documentos, que refleja la naturaleza, cantidad y complejidad de los procesos de trabajo de la organización, debe documentarse (incluyendo cambios en el tiempo) e implementarse como parte de los procedimientos de dichos procesos de trabajo.

V.4. DESCRIPCIÓN DE DOCUMENTOS:

Este proceso permitirá la recuperación de los documentos y su contexto, y atenderá a la aplicación del esquema institucional de metadatos. La descripción de documentos se nutre de los metadatos para la gestión de documentos electrónicos definidos en cada organización para ajustarse a sus particularidades y necesidades específicas.

Como indicamos anteriormente, la adopción de una estructura de metadatos para los documentos electrónicos permite:

- mejorar la recuperación de la información.
- mejorar la difusión de la información.
- asegurar la interoperabilidad entre sistemas.
- asegurar la preservación de la información a lo largo del tiempo.
- demostrar la conformidad con normas, por ejemplo las de gestión documental.

El Ministerio de Hacienda y Administraciones Públicas deberá establecer un catálogo institucional de metadatos compatible con el esquema e-EMGDE recomendado por el ENI, por motivos de interoperabilidad, así como por el hecho de que es más eficiente y sostenible la adopción de esquemas de metadatos normalizados que la creación de conjuntos de metadatos ad-hoc. La definición de dicho esquema institucional de metadatos es el objeto de esta ponencia.

Siguiendo la terminología de la ISO (International Standards Organization) en el ámbito de la gestión documental, el conjunto de elementos del esquema de metadatos e-EMGDE que sean seleccionados, así como las reglas o directrices que se establezcan para su uso, constituirán el "perfil de aplicación" de la Administración Presupuestaria.

Si bien en un sentido amplio se puede entender que la Descripción es el proceso en el que se asignan los metadatos de gestión documental, si tenemos en cuenta que en cada uno de los procesos que hemos desglosado (captura, clasificación, acceso, etc) se van a establecer unos metadatos específicos, resulta conveniente adoptar una concepción más acotada de la Descripción, que no presente solapamientos con el resto de procesos. En consecuencia, se engloban en el proceso de Descripción tanto los **estándares de descripción archivística multinivel** (como ISAD) - que aportan información sobre la temática y contenido de los documentos o agrupaciones documentales - como **metadatos técnicos informáticos y metadatos de preservación**.

Asimismo, de acuerdo con la norma ISO 30301, también están comprendidos dentro del proceso de descripción:

- documentar e implementar las **decisiones acerca de los metadatos que son necesarios** para identificar, gestionar y controlar los documentos en toda la organización, así como externamente.
- **Determinar el historial de eventos**: Se deben definir los procesos de gestión de documentos que deben registrarse en los metadatos vinculados al historial de even-

tos del documento. Se deben establecer los procedimientos para vincular el historial de eventos a los documentos y mantenerlo durante el mismo tiempo que los propios documentos. Por la especial importancia de la "Trazabilidad", como proceso esencial de la gestión de documentos, le dedicaremos un capítulo aparte.

En cuanto a la categoría de *metadatos técnicos informáticos*, se deberá emplear el metadato *eEMGDE14 – Características Técnicas* de la Entidad "Documento", que consta de los siguientes sub-elementos:

a. eEMGDE14.1 – Soporte origen
b. eEMGDE14.2 – Nombre de formato
c. eEMGDE14.3 - Versión de formato
d. eEMGDE14.4 – Nombre de la aplicación de creación
e. eEMGDE14.5 – Versión de la aplicación de creación
f. eEMGDE14.7 - Resolución
g. eEMGDE14.8 - Tamaño

En la categoría de *metadatos de preservación*, se deberán soportar en el Sistema de Gestión Documental los metadatos de la Entidad "Documento" relativos a:

- Fechas (e-EMGDE4)
- Firma (e-EMGDE17)
- Verificación de integridad (e-EMGDE16)

Si se considerara pertinente efectuar una descripción de la temática y contenido de los documentos electrónicos en el organismo, éste podría tener en cuenta a la hora de definir su propio modelo de descripción de documentos, las normas existentes para la descripción de entidades -tanto nacionales (NEDA) como internacionales (ISAD, ISAAR CPF, ISDF)-, como complemento al esquema e-EMGDE. Las descripciones, sea cual sea la taxonomía y el vocabulario empleado, se recogerán en e-EMGDE mediante el metadato eEMGDE12-PUNTO DE ACCESO.

V.5. ACCESO A LOS DOCUMENTOS:

Las organizaciones deben disponer de directrices formales que regulen a quién se le permite acceder a los documentos y en qué circunstancias.

El marco reglamentario en el que el Ministerio de Hacienda y Administraciones Públicas realiza sus actividades (en particular, la legislación sobre Protección de Datos de Carácter Personal, el Esquema Nacional de Seguridad, y la legislación sobre Patrimonio Histórico) establece una serie de principios generales sobre los derechos, condiciones y restricciones de acceso que deberían aplicarse en el funcionamiento de los sistemas de gestión de documentos.

Antes de proceder a la identificación de los metadatos, vamos a realizar algunas consideraciones acerca de la posible manera de abordar el proceso de acceso a los documentos.

A partir de la experiencia con los gestores documentales existentes, se deberán crear como mínimo en todos los centros tres perfiles de acceso, debiendo asignarse un perfil a cada documento: PUBLICO (disponible para todos los usuarios), RESTRINGIDO (disponible para aquellos que pertenezcan a una lista de control de acceso, que generalmente se establecerá por pertenencia a un departamento o servicio - por ejemplo los encargados de la tramitación de un procedimiento-, o por ser usuario de una aplicación de gestión), o ARCHIVOS (accesible para personal de archivos).

Por defecto, se podría decidir en un determinado organismo que cada aplicación gestora sólo podrá acceder en el Sistema de Gestión Documental a los documentos pertenecientes a los expedientes que gestiona, o bien a aquellos documentos que hayan sido declarados abiertos para acceso público.

Adicionalmente, se podrán establecer limitaciones al acceso, uso y reutilización para el usuario o receptor de documentos (por ejemplo, se podrá indicar que un determinado documento será accesible, pero sin derecho a reproducción, por motivos de propiedad intelectual), y las aplicaciones gestoras deberán alertar a los usuarios de estas limitaciones y ejecutar las acciones derivadas.

Llegados a este punto, se identifican a continuación los metadatos implicados en este proceso.

Los metadatos referentes a las condiciones de acceso, se reflejarán en el elemento eEMGDE9. Este consta de dos sub-elementos: "eEMGDE9.1-CONDICIONES DE ACCESO, USO Y REUTILIZACION" y "eEMGDE9.2-TIPO DE ACCESO".

A. eEMGDE9.1-CONDICIONES DE ACCESO, USO Y REUTILIZACION se usa "para proporcionar información acerca de la naturaleza de la limitación al acceso, uso y reutilización y de cualquier obligación en vigor para el usuario o receptor de los documentos". Este metadato no tiene un esquema de valores definido en e-EMGDE, pero algunos ejemplos de valores que podría tomar son: *Accesible sin derecho a reproducción*, *No accesible hasta la estabilización de la versión de la aplicación*, o *Reutilización autorizada con sujeción a condiciones generales*. A efectos de su implantación en el Sistema de Gestión Documental, deberá acordarse en el Grupo de Trabajo de Coordinación de Archivos el esquema de valores permitido para eMGDE9.1 en el Ministerio de Economía y Hacienda, así como las acciones a las que dará lugar cada valor.

B. eEMGDE9.2-TIPO DE ACCESO tiene el siguiente esquema de valores:

Código	Categoría	Comentario
A	Acceso libre	El documento está abierto al acceso público por aplicación de la normativa.
B	Acceso restringido	Determinado por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y normativa de desarrollo, pero también en Ley 30/1992, normativa sectorial (propiedad industrial, datos sanitarios, estadística, etc.). *Se aplica cuando el acceso es posible para algunas personas, pero no en general: interesados, por ser titular de un interés legítimo...*
B.1	Acceso reservado	Acceso reservado a los titulares de los datos, por contener datos que afectan a su seguridad, honor o intimidad, según artículo 37.2 Ley 30/1992.
B.2	Acceso limitado	Acceso limitado a sus titulares y a terceros con interés legítimo y directo, por contener datos nominativos que no afectan al honor ni la intimidad, según artículo 37.3 Ley 30/1992.
C	Acceso excluido	Determinado por la legislación aplicable: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y normativa de desarrollo, pero también Ley 30/1992, normativa sectorial (propiedad

Código	Categoría	Comentario
		industrial, datos sanitarios, estadística, etc.). *Se aplica a los documentos excluidos de la consulta pública por tratarse de materias protegidas que afectan a la seguridad y defensa del Estado o de las Administraciones Públicas.*
D	Documento sujeto a derechos de propiedad intelectual	Determinado por la Ley de Propiedad Intelectual.
E	Fuente accesible al público	Determinado por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y normativa de desarrollo.
F	Acceso regido por disposiciones específicas	Determinado por la Ley 30/1992 (artículo 37.6).

En la categoría B.2, merece ser destacado que quedan excluidos del acceso de terceros los documentos que figuren en procedimientos de carácter sancionador o disciplinario.

Como comentario aclaratorio, las fuentes accesibles al público son: el censo promocional, los repertorios telefónicos, las listas de personas pertenecientes a grupos profesionales, los diarios y boletines oficiales, y los medios de comunicación. Estos tipos de documentos no son objeto de esta política de gestión documental.

Por su parte, en la categoría F ("Acceso regido por disposiciones específicas") se encuentran:

- archivos sometidos a la normativa sobre materias clasificadas; documentos y expedientes que contengan datos sanitarios; archivos regulados por la legislación del régimen electoral; archivos que sirvan a fines exclusivamente estadísticos dentro del ámbito de la función estadística pública; el Registro Civil y el Registro Central de Penados y Rebeldes y los registros de carácter público regulados por una ley; el acceso a los documentos obrantes en los archivos de las Administraciones Públicas por parte de las personas que ostenten la condición de Diputado, Senador, miembro de una Asamblea legislativa de Comunidad Autónoma o de una Corporación Local; y la consulta de fondos documentales en los Archivos Históricos.

Las aplicaciones gestoras del Ministerio de Economía y Hacienda deberán tener en cuenta la Categoría de Acceso de un documento, lo que implica que en algunos casos no deberán permitir el acceso a los documentos o la obtención de información sobre los mismos.

También se deberá recoger en el SGDE el nivel de seguridad de un sistema de información de conformidad con el Esquema Nacional de Seguridad. En este sentido, se recogerá en el metadato **eEMGDE8.5** de la instancia de la entidad "Documento" el nivel de seguridad de un sistema de información (en la práctica este metadato se aplica a todos los documentos que participan en un sistema), de acuerdo con los criterios del Esquema Nacional de Seguridad. La disponibilidad de este metadato en el SGDE permitirá realizar automatismos en relación a: la obligatoriedad de utilizar certificados incluidos en dispositivos seguros de creación de firma, la necesidad de utilizar sellos de tiempo y no marcas de tiempo en las firmas longevas, y otras medidas derivadas del Esquema Nacional de Seguridad.

V.6. CALIFICACIÓN DE LOS DOCUMENTOS:

Este proceso incluye:

i. Determinación de los documentos esenciales.

ii. Valoración de documentos y determinación de plazos de conservación.

iii. Dictamen de la autoridad calificadora.

a. DETERMINACIÓN DE LOS DOCUMENTOS ESENCIALES

En primer lugar, es preciso diferenciar entre los documentos esenciales de un procedimiento administrativo y los documentos esenciales de una institución u organismo.

Abordemos en primer lugar la primera acepción: los documentos esenciales de un procedimiento administrativo. En función de su contenido, los documentos se dividen en: documentos esenciales (informes, dictámenes, resoluciones, etc), que son aquellos que recogen la información más cualificada del procedimiento administrativo, y documentos de enlace (oficios de remisión, notas internas, etc), cuya finalidad es servir de nexo y dejar constancia de los trámites realizados.

En cuanto a los documentos esenciales de una organización, según la norma MoReq (elaborada para el programa IDA, Interchange of data between Administrations del Consejo de Europa), los "*documentos de archivo esenciales son los absolutamente necesarios para la continuidad de la actividad de la organización, ya sea en cuanto a su capacidad de hacer frente a situaciones de emergencia o a catástrofes, ya en relación con la protección de sus intereses financieros y jurídicos. Por consiguiente, la identificación y la protección de estos documentos de archivo es de gran importancia en cualquier organización*." Asimismo, esta norma indica que "*el Sistema de Gestión de Documentos debe permitir la restauración de los documentos de archivo esenciales y los demás en operaciones separadas*".

De acuerdo con el modelo de política de gestión de Documentos Electrónicos del Esquema Nacional de Interoperabilidad, "Se entiende por documentos esenciales aquéllos que resultan indispensables para que la entidad pueda alcanzar sus objetivos, cumplir con sus obligaciones diarias de servicio, respetar la legalidad vigente y los derechos de las personas. La

categorización del sistema (ENS, Anexo I), el 'Análisis de riesgos [op.pl.1]' y la 'Calificación de la información [mp.info.2]' aportarán criterios para identificar documentos esenciales y las medidas de seguridad y nivel requerido aplicables."

En definitiva, los documentos esenciales a los que alude el ENI son los documentos esenciales de una institución.

Los documentos esenciales pueden requerir medidas de seguridad reforzadas, que prevengan su pérdida y faciliten su recuperación en situaciones de emergencia. En este sentido, para todos los documentos esenciales, se requieres la obtención de una copia electrónica auténtica. En función de un análisis de riesgos (medida [op.pl.1] del ENS), podrán implementarse otros medidas de protección para los documentos esenciales como: duplicación, efectuar copias diarias, creas tablas diferentes para documentos esenciales y documentos no esenciales.

Se propone reflejar el carácter de documento esencial o no esencial para una organización en el metadato eEMGDE13.1-VALORACION de le entidad "Documento". Este tiene un esquema de valores con cinco categorías posibles: Valor legal, Valor jurídico, Valor fiscal, Valor administrativo, Valor histórico o de investigación, Valor social. Recomendamos incluir una sexta categoría, "Valor esencial", con dos valores posibles: "SI" o "NO".

Con carácter general, para un documento dado, este metadato se heredará de la Serie documental a la que pertenezca.

b. VALORACIÓN DE DOCUMENTOS Y DETERMINACIÓN DE PLAZOS DE CONSERVACIÓN

El objetivo de la valoración es determinar, de entre todos los documentos emitidos por una organización en el curso de sus actividades, cuáles han de conservarse y durante cuánto tiempo, de manera que se garantice en el futuro la eficaz continuación de dichas actividades y la preservación de la memoria de la institución, así como el derecho de los ciudadanos al acceso a los documentos y a la información, según recoge la legislación, sin menoscabo de las restricciones que la normativa impone en función de la naturaleza de la información. La valoración de documentos es una tarea muy exigente, que debe ser realizada por un Archivero o Documentalista. La valoración es un proceso durante el cual no sólo se identifica el valor de los documentos, sino que se aumenta o disminuye ese valor en función del contexto, de la realidad social y del momento. Si bien existen diferentes enfoques en la determinación del valor de los documentos, hoy por hoy existe un consenso más o menos generalizado sobre la conveniencia de aplicar en el caso de la documentación electrónica una teoría funcional de valoración, basada en el análisis de las actividades y funciones que dieron lugar a la producción de los documentos, antes que en su contenido, pues éstas resultan más estables a lo largo del tiempo que las estructuras organizativas o las aplicaciones que generan los documentos. Entendemos que esta aproximación está alineada con la filosofía que subyace a la *NTI de Política de Gestión de Documentos Electrónicos*, que para otro proceso, el de la Clasificación de Documentos, prescribe también la modalidad de Clasificación Funcional, en detrimento de la Clasificación Orgánica o la Clasificación Por Materias.

Los Estudios de Valoración Documental son competencia del Grupo de Trabajo para la coordinación de archivos del Departamento, en virtud del artículo 13.2 del Real Decreto 1708/2011. Tras realizar un Estudio de Valoración Documental, el Grupo de Trabajo para la Coordinación de Archivos deberá elevar la correspondiente petición de dictamen a la Comisión Superior Calificadora de Documentos Administrativos. Este dictamen dará lugar a un informe de la Subsecretaría del Departamento, mediante resolución.

A nivel técnico, una vez culminado el estudio de Valoración Documental, y a partir de la Resolución correspondiente de la Subsecretaría, se procederá a almacenar en el Sistema de Gestión Documental la siguiente información para el Documento o Serie Documental en cuestión:

- **Valor del documento**, en el metadato eEMGDE13.1-VALORACION (por ejemplo, "Valor legal: Permanente, Valor fiscal: Cinco años".
- **Dictamen relativo a la conservación**, emitido por la autoridad calificadora, que se guardará en el metadato eEMGDE13-2-DICTAMEN, el cual consta a su vez de dos sub-elementos: eEMGDE13.2.1-TIPO DE DICTAMEN y eEMGDE13.2.2-ACCION DICTAMINADA.

La norma ISO 15489 establece unas directrices para la determinación de los plazos de conservación, que servirán de orientación al Grupo de Trabajo para la coordinación de archivos del departamento en sus tareas de valoración, conjuntamente con la Legislación sobre Patrimonio Histórico:

- *Las decisiones sobre los plazos de conservación en un Sistema de Gestión de Documentos se basan en la evaluación del marco reglamentario, de las necesidades de gestión y de rendición de cuentas y del riesgo. En un principio, en la toma de dichas decisiones deberían participar la unidad encargada de la actividad en cuestión, el responsable de la gestión de documentos que se haya designado y cualquier otra persona que se requiera, de conformidad con lo dispuesto en las políticas o normas de gestión de documentos externas e internas y con los requisitos específicos de los documentos relacionados con dicha actividad. Los requisitos legales o reglamentarios pueden exigir períodos de conservación mínimos o la aprobación por parte de un organismo competente, tal como una autoridad archivística o de auditoría y control. Los derechos y garantías de las partes interesadas se deberían tener en cuenta a la hora de determinar el período de conservación de los documentos. No se deberían tomar, de forma intencionada, decisiones que impidan el ejercicio del derecho de acceso.*

Asimismo, la norma ISO 15489 dispone que los documentos de conservación permanente son potencialmente aquellos que:

- *proporcionan información y pruebas sobre las políticas y las acciones de la organización;*
- *proporcionan información y pruebas sobre la interacción de la organización con aquellos a quienes presta sus servicios;*
- *documentan los derechos y las obligaciones de individuos y organizaciones;*
- *contribuyen a la elaboración de la memoria de la organización con fines científicos, culturales o históricos; y*
- *contienen información y pruebas relativas a actividades de interés para partes interesadas externas e internas.*

c. DICTAMEN DE LA AUTORIDAD CALIFICADORA

El “tipo de dictamen”, recogido en el sub-elemento eEMGDE13.2.1, tiene el siguiente esquema de valores:

Categoría	Descripción
Conservación permanente	Situación derivada de la fase de valoración que afecta a los documentos que han desarrollado valores históricos o de investigación y que en consecuencia no pueden ser eliminados.
Eliminación	Destrucción física de unidades o series documentales por el órgano responsable, empleando cualquier método que garantice la imposibilidad de su uso posterior.
Eliminación parcial	Proceso de destrucción física, una vez analizados sus valores, en el cual se acuerda la conservación de ejemplares a efectos testimoniales (muestreo).
Transferencia	Determinación del plazo de permanencia de los documentos en cada uno de los depósitos o repositorios que, en su caso, existan en la organización. Puede implicar el traspaso de las responsabilidades sobre el tratamiento y custodia de dicha documentación.
Muestreo	Conservación selectiva de documentos, cuya acción decidida es eliminación, a efectos meramente informativos.
Duplicación por esencial	Proceso de copia de unidades o series documentales en razón del carácter esencial de la información que contienen, de acuerdo con las actividades específicas de la organización.
Sin calificación	Equivalente a sin cobertura de calificación.
Revisión posterior	Situación en la que la decisión no puede ser tomada y se pospone.

El sub-elemento eEMGDE13.2.2-ACCION DICTAMINADA se utiliza para registrar la acción dictaminada que se pretende realizar de manera reglada sobre el documento, y concretará la acción que tiene que emprenderse sobre un documento una vez que ha pasado el período de tiempo especificado desde el evento desencadenante indicado. Ejemplos: *Transferir pasados cincos años desde su creación, Retener permanentemente, Destruir a los setenta y cinco años después de la fecha de nacimiento del empleado, Destruir a los tres años desde la finalización del contrato.*

Los documentos simples, expedientes, agregaciones y series pueden verse afectados, a lo largo de su ciclo de vida, por distintas decisiones hasta su eliminación o conservación permanente, en su caso, por lo que deberían describirse utilizando múltiples instanciaciones del sub-elemento eEMGDE13.2 – Dictamen (y por tanto, de sus sub-elementos eEMGDE13.2.1 y eEMGDE13.2.2).

V.7. CONSERVACIÓN DE LOS DOCUMENTOS

El SGDE debe permitir la asignación de normas de conservación a todos los documentos y expedientes del Cuadro de Clasificación, avisando mediante un proceso automatizado al administrador cuando se alcance la fecha en la que debe hacerse efectivo el destino establecido, en función de los dictámenes de los estudios de valoración.

En consonancia con la norma ISO 15489, la conservación de documentos se debe organizar de forma que se consiga:

A. Satisfacer las necesidades de gestión, presentes y futuras, mediante:

   1. la conservación de información relativa a decisiones y actividades presentes y pasadas como parte de la memoria administrativa para apoyar decisiones y actividades en el presente y en el futuro;

   2. la conservación de elementos de prueba de las actividades presentes y pasadas para cumplir las obligaciones de rendición de cuentas;

   3. la eliminación, lo antes posible y de manera sistemática y autorizada, de los documentos que ya no se necesiten; y

   4. la conservación del contexto del documento, lo que permitirá a futuros usuarios juzgar su autenticidad y fiabilidad, incluso en sistemas de gestión de documentos cerrados o que hayan sufrido importantes cambios.

B. Cumplir los requisitos legales, garantizando que se documenta, entiende e implementa la reglamentación aplicable a la gestión de los documentos producidos en el ejercicio de las actividades específicas, y

C. Satisfacer las necesidades presentes y futuras de las partes interesadas, tanto externas como internas, mediante:

   1. la identificación de los intereses legítimos y exigibles que las partes interesadas puedan tener en relación con la conservación de los documentos mediante un período de tiempo superior al requerido por la propia organización.

   2. la identificación y la evaluación de los beneficios legales, financieros, políticos, sociales y de cualquier otro tipo que se deriven de la conservación de los documentos al servicio de la investigación y de la sociedad en su conjunto; y

   3. el cumplimiento, en su caso, de las disposiciones reglamentarias de la autoridad archivística competente.

Se indican a continuación los metadatos de e-EMGDE referidos a la conservación, para las entidades Documento y Relación, que deberán ser soportados en el Sistema de Gestión Documental:

– Entidad Documento:

Identificador	eEMGDE2
Verificación de Integridad	eEMGDE16
Características técnicas	eEMGDE14
Fechas	eEMGDE4
Nombre	eEMGDE3
Ubicación	eEMGDE15
Firma	eEMGDE17
Derechos de acceso, uso y reutilización	eEMGDE9

– Entidad Relación:

Categoría	eEMGDE1
Nombre	eEMGDE3
Entidad Relacionada	eEMGDE6
Identificador	eEMGDE2
Fechas	eEMGDE4
Descripción	eEMGDE5
Trazabilidad	eEMGDE21

V.8. TRAZABILIDAD:

El control de la trazabilidad es un proceso esencial de la gestión de documentos en una organización, ya que es necesario para:

1. Identificar una acción pendiente de ejecución.
2. Permitir la recuperación de un documento.
3. Prevenir la pérdida de documentos.
4. Supervisar y mantener un sistema de auditoría de las operaciones relacionadas con los documentos.
5. Mantener la capacidad de identificar las tareas que originaron los documentos individuales cuando los sistemas se han fusionado o migrado.

El Esquema de Metadatos e-EMGDE dispone de un metadato específico para fines de Trazabilidad, denominado “eEMGDE21-TRAZABILIDAD”, que consta de los siguientes subelementos:

- **eEMGDE21.1 ACCIÓN**: indica el tipo de acción realizada sobre una o varias entidades del sistema (por ejemplo, Consulta, Modificación, Borrado, Alta, etc)

- Este sub-elemento sólo debe aplicarse en entornos mono-entidad. En una implementación multi-entidad (como la del Esquema Institucional de metadatos), se establece una relación con la entidad Actividad pertinente. Esta relación será de tipo “acción de gestión de documentos” (accede a, borra, cambia, copia, ejecuta, etc).

- **eEMGDE21.2 MOTIVO REGLADO**: razón por la que se lleva a cabo la acción expresada en eMGDE21.2 (por ejemplo, “en virtud del Real Decreto…” o “sin motivo reglado”).

    - Este sub-elemento sólo debe aplicarse en entornos mono-entidad. En una implementación multi-entidad (como la del Esquema Institucional de metadatos), se establece una relación con la entidad Regulación pertinente.

- **eEMGDE21.3 USUARIO DE LA ACCIÓN**: permite mantener una pista de auditoría inalterable de las personas que ejecutan las acciones realizadas en el sistema.

    - Este sub-elemento sólo debe aplicarse en entornos mono-entidad. En una implementación multi-entidad (como la del Esquema Institucional de metadatos), se establece una relación con la entidad Agente pertinente.

- **eEMGDE21.4 DESCRIPCIÓN**: su finalidad es ofrecer una finalidad más detallada en texto libre de la acción realizada sobre una determinada entidad (por ejemplo, “En 5 de agosto de 2012 el agente 12.345.687A, accedió al documento 1332007511, a las 12:15:25 horas, para modificar el campo Nombre”).

- **eEMGDE21.5 MODIFICACIÓN DE LOS METADATOS**: permite mantener una pista de auditoría inalterable, en texto libre, de las acciones realizadas en el sistema (por ejemplo, “Modificación realizada el 2 de junio de 2010 a las 12:14:23 por parte del usuario 172.16.0.15”). Sólo se utilizará cuando la acción haya producido alguna modificación en los metadatos del documento.

- **eEMGDE21.6 HISTORIA DEL CAMBIO**: permite rastrear los cambios sobre los metadatos de una entidad a lo largo del tiempo, y consta de dos sub-elementos:

    - **eEMGDE21.6.1 – NOMBRE DE ELEMENTO**

    - **eEMGDE21.6.2 – VALOR ANTERIOR**

Si bien estos metadatos no son obligatorios en el esquema e-EMGDE, recomendamos que se implementen (a excepción de aquellos que no se emplean en una implementación multi-entidad), ya que son necesarios para garantizar la calidad y seguridad de la gestión documental de un organismo, de acuerdo con la norma ISO15489.

El SGDE que gestione el repositorio de metadatos e-EMGDE, podrá implementar mediante *triggers* de base de datos y tablas de históricos los metadatos indicados anteriormente, con la excepción de:

- eEMGDE21.2 MOTIVO REGLADO, que deberá ser proporcionado por la aplicación gestora.
- eEMGDE21.4 DESCRIPCIÓN, que recomendamos sea automatizado, extrayendo información del resto de sub-elementos relacionados con la trazabilidad.
- eEMGDE21.5 MODIFICACIÓN DE LOS METADATOS, que recomendamos sea automatizado, obteniendo información del resto de sub-elementos relacionados con la trazabilidad.

En la implantación del metadato eEMGDE21-TRAZABILIDAD y la definición de los esquemas de valores permitidos para sus sub-elementos, se tendrán en cuenta las siguientes directrices de la norma ISO 15489, en cuanto a “Trazabilidad de las acciones” y “Trazabilidad de la ubicación”:

TRAZABILIDAD DE LAS ACCIONES: la trazabilidad de las acciones se puede implantar en un SGDE cuando se han establecido límites temporales internos o externos a la organización para la ejecución de las mismas. La trazabilidad de las acciones exige:

A. definir los pasos que han de darse en respuesta a las decisiones u operaciones recogidas en un documento;

B. asignar a una persona determinada la responsabilidad de las acciones emprendidas; y

C. registrar los plazos en los que tienen que efectuarse las acciones predefinidas y las fechas en las que dichas acciones han de ejecutarse.

La trazabilidad de las acciones sólo se puede implementar con eficacia si el material se registra en el SGDE antes de ser enviado a las personas designadas.

TRAZABILIDAD DE LA UBICACIÓN: se debería documentar el movimiento de documentos para garantizar que se puedan localizar siempre que sea necesario. Los mecanismos de trazabilidad pueden registrar el identificador del documento, el título, la persona o la unidad que lo posee y el momento o fecha en la que se realizó el movimiento.

El sistema debería dejar traza de la salida de documentos, la transmisión entre personas y la devolución del documento a su ubicación o almacenamiento "original", así como su destrucción o transferencia a cualquier otra organización autorizada externa, incluidas las autoridades archivísticas.

V.9. TRANSFERENCIA, DESTRUCCIÓN O ELIMINACIÓN DE DOCUMENTOS

Dado que los documentos son la plasmación de una actuación administrativa o de un hecho del que dan constancia, no podrán eliminarse los documentos hasta que se determine su destrucción, conservación o transferencia por dictamen del órgano competente.

La retirada de los documentos de los sistemas en uso sólo debería tener lugar si se garantiza que el documento ya no se necesita, que no queda ninguna labor pendiente de ejecución y que no existe ningún litigio o investigación, en el momento actual o pendiente de realización, que implique la utilización del documento como prueba.

La retirada de documentos puede englobar, de acuerdo con la norma ISO 15489:

A. la inmediata destrucción física, incluido el borrado o la sobreescritura;

B. la conservación durante un mayor período de tiempo en la unidad organizativa;

C. el traslado a un depósito o medio de almacenamiento apropiados bajo control de la organización;

D. la transferencia a otra organización que haya asumido la responsabilidad de la actividad mediante una reestructuración;

E. el traslado a un depósito gestionado en nombre de la organización por un proveedor independiente con el que se ha establecido un contrato adecuado;

F. la transferencia de responsabilidad de la gestión a otra autoridad competente, aunque el almacenamiento físico del documento siga realizándose en la organización que lo creó;

G. la transferencia al archivo histórico de la organización; o

H. la transferencia a una autoridad archivística externa.

La Evaluación y la Selección son los procedimientos mediante los cuales se determina el destino de los documentos (así como los plazos de tiempo límites para su conservación o destrucción) a partir de su valor. Asimismo, en el caso de los documentos desprovistos de interés a largo plazo, no podrá procederse directamente a su destrucción, sino que se deberá seguir un proceso que incluye un Estudio de Valoración Documental, y que involucra a la Comisión Superior Calificadora de Documentos Electrónicos y a la Subsecretaría del Departamento.

Como indicamos anteriormente, el metadato eEMGDE13-CALIFICACION almacenará la Valoración del Documento y el Dictamen relativo a su conservación. En el caso de los documentos para los que se pueda efectuar el estudio de Valoración Documental una sola vez, y reaplicar su dictamen en años sucesivos, los metadatos eEMGDE13.1 y eEMGDE13.2 podrán ser parametrizados por Serie Documental o aplicación gestora, con vistas a su cumplimentación automática.

Es preciso advertir que existirán categorías de documentos - como puede ser el caso de documentos que contengan datos de carácter personal, o documentos clasificados -, en los que habrá que estudiar si es posible la transferencia fuera del SGDE de la organización.

A estos efectos, se dispone de un metadato en e-EMGDE (eMGDE 8.4), que indica los niveles de protección de datos sensibles de carácter personal de los ficheros (Básico, Medio o Alto), de acuerdo con la Ley Orgánica 15/99, y normativa de desarrollo.

Asimismo, el metadato *eEMGDE 8.1.1-CLASIFICACION DE ACCESO* permite indicar si un documento es clasificado o reservado, poseyendo el siguiente esquema de valores:

Código	Clasificación	Comentario
A	Secreto	Categoría empleadas en la Ley de Secretos Oficiales.
B	Reservado	Categoría empleadas en la Ley de Secretos Oficiales.
C	Confidencial	Usado en tratados internacionales.
D	Clasificado	Genérico.
E	No clasificado	Cuando no existe una acción dictaminada de seguridad e interesa indicarlo.

La norma europea MoReq2, relativa a los requisitos de los Sistemas de Gestión de Documentos Electrónicos de Archivo (SGDEA), y que forma parte del Catálogo de Estándares del Esquema Nacional de Interoperabilidad, tiene un apartado referente a la “Modificación, borrado y disociación de datos de documentos de archivo”. En él se establecen, de manera resumida, los siguientes requerimientos para la disociación de datos:

- los documentos de archivo serán inmodificables, de manera que cuando se deba suministrar al exterior documentación que contenga información reservada o datos de carácter personal, se ha de poder facilitar el documento, suprimiendo la información confidencial, sin que ello afecte al archivo en cuestión. Ese proceso se denomina disociación de datos, y el Sistema de Gestión de Documentos Electrónicos de Archivo deberá almacenar **tanto el documento de archivo original como la copia sometida a dicho proceso, que se denominará “extracto”** del documento de archivo.

Es decir, siguiendo la terminología del ENI, cuando sea necesario aplicar un proceso de disociación habrá que mantener el documento electrónico original, y generar una “Copia electrónica parcial auténtica”.

Se enumeran a continuación los principios que deben regular la destrucción física de los documentos, de acuerdo con la norma ISO 15489:

- la destrucción siempre deberá contar con autorización;
- los documentos relacionados con litigios o investigaciones que se estén desarrollando en ese momento o que estén pendientes de realización no deberían destruirse;
- la destrucción de los documentos debería realizarse de manera que se preserve la confidencialidad de cualquier información que estos contengan;
- todas las copias de los documentos cuya destrucción esté autorizada, incluidas las copias de seguridad, las copias de conservación y las copias de seguridad electrónicas, deberían ser destruidas.

En relación al último punto, se deberá prestar especial atención al caso de las cintas, ya que al tratarse este soporte de un medio de acceso secuencial, no es materialmente posible borrar sólo una parte. En consecuencia, los datos que se vayan a borrar deberían encontrarse ya fuera del circuito de backup, y mantenerse únicamente como réplicas, puesto que son documentos que no se modifican.

Si estas replicas se almacenan en un soporte de cintas, se aconseja su conservación y partición por años (ya que los procesos de borrado se efectúan generalmente por intervalos temporales). En el caso del disco, no es necesaria esta división de los datos, por ser un medio de acceso aleatorio.

VI. DECLARACIÓN DEL CONJUNTO DE METADATOS DE GESTION DOCUMENTAL SELECCIONADOS DEL e-EMGDE

Como consecuencia del análisis efectuado en el apartado V, se reseñan a continuación los metadatos de gestión documental pertenecientes al Esquema Institucional de Metadatos, desglosados por Entidad:

VI.1. ENTIDAD “DOCUMENTO”

a. METADATOS OBLIGATORIOS

Deberán implementarse en los SGDE los siguientes **metadatos obligatorios** y sub-elementos asociados (donde se han excluido aquellos sub-elementos no obligatorios que a nuestro juicio no aportan valor, o no resultan imprescindibles para la adecuación al ENI):

- eEMGDE 1 – Categoría
- eEMGDE2 – Identificador
  - eEMGDE2.1 – Secuencia de Identificador
  - eEMGDE2.2 – Esquema de identificador
- eEMGDE4 – Fechas
  - eEMGDE4.1 – Fecha Inicio
  - eEMGDE4.2 – Fecha fin (éste sub-elemento se rellenará cuando finalice la existencia de una Entidad –documento- o de una Relación).
- eEMGDE14 – Características Técnicas
  - eEMGDE14.1 – Soporte origen
  - eEMGDE14.2 – Nombre de formato
  - eEMGDE14.3 - Versión de formato
  - eEMGDE14.4 – Nombre de la aplicación de creación
  - eEMGDE14.5 – Versión de la aplicación de creación
  - eEMGDE14.7 - Resolución
  - eEMGDE14.8 - Tamaño
- eEMGDE17 – Firma
  - eEMGDE17.1 – Tipo de Firma
  - eEMGDE17.2 – Formato de Firma
  - eEMGDE17.3 – Rol de Firma
- eEMGDE18-Tipo Documental
- eEMGDE20 – Estado de Elaboración
  - eEMGDE20.1 – Denominación del Estado
  - eEMGDE20.2 – Características de la Copia

b. METADATOS COMPLEMENTARIOS

Los **metadatos complementarios** a incorporar en el SGDE son aquellos que han sido identificados en el apartado V como necesarios para sustentar los Procesos de Gestión Documental establecidos en la NTI de Política de Gestión de Documentos Electrónicos. Esto es, teniendo en cuenta de que se trata de una implementación multi-entidad, se soportarán los siguientes metadatos complementarios y sub-elementos:

- eEMGDE3 – NOMBRE
  - eEMGDE3.1 –Nombre Natural
- eEMGDE5 - DESCRIPCIÓN
- eEMGDE8 – SEGURIDAD
  - eEMGDE8.1.1. – Clasificación de acceso
  - eEMGDE8.4- Sensibilidad Datos de Carácter Personal
  - eEMGDE8.5 – Clasificación ENS
- eEMGDE9 – DERECHOS DE ACCESO, USO Y REUTILIZACIÓN
  - eEMGDE9.1 – Condiciones de acceso, uso y reutilización
  - eEMGDE9.2 – Tipo de acceso
- eEMGDE11-IDIOMA
- eEMGDE12-PUNTO DE ACCESO
- eEMGDE13- CALIFICACIÓN
  - eEMGDE13.1 - Valoración
  - eEMGDE13.2 – Dictamen
- eEMGDE15 – UBICACIÓN
  - eEMGDE15.1 – Soporte
  - eEMGDE15.2 - Localización
- eEMGDE16 –VERIFICACIÓN DE INTEGRIDAD
  - eEMGDE16.1 – Algoritmo
  - eEMGDE16.2 - Valor
- eEMGDE21-TRAZABILIDAD
  - eEMGDE21.1 - Acción
  - eEMGDE21.2 – Motivo reglado
  - eEMGDE21.3 – Usuario de la acción
  - eEMGDE21.4 - Descripción
  - eEMGDE21.5 – Modificación en los metadatos
  - eEMGDE21.6 – Historia del cambio

VI.2. ENTIDAD “REGULACIÓN”

a. METADATOS OBLIGATORIOS

Deberán implementarse en los gestores documentales los siguientes **metadatos obligatorios** y sub-elementos asociados para la entidad Regulación (donde se han excluido aquellos sub-elementos no obligatorios que a nuestro juicio no aportan valor, o no resultan imprescindibles para la adecuación al ENI, de acuerdo con nuestro análisis del apartado V):

- eEMGDE1 – Categoría
- eEMGDE2 – Identificador
    - eEMGDE2.1 – Secuencia de Identificador
    - eEMGDE2.2 – Esquema de identificador
- eEMGDE4 – Fechas
    - eEMGDE4.1 – Fecha Inicio
    - eEMGDE4.2 – Fecha fin (este sub-elemento se rellenará cuando finalice la existencia de una Entidad.

b. METADATOS COMPLEMENTARIOS

- eEMGDE3 – NOMBRE
    - eEMGDE3.1 – Nombre Natural
- eEMGDE5 – DESCRIPCIÓN
- eEMGDE12 – PUNTOS DE ACCESO

VI.3. ENTIDAD "AGENTE"

a. METADATOS OBLIGATORIOS

Deberán implementarse en los gestores documentales los siguientes **metadatos obligatorios** y sub-elementos asociados para la entidad Agente (donde se han excluido aquellos sub-elementos no obligatorios que a nuestro juicio no aportan valor, o no resultan imprescindibles para la adecuación al ENI, de acuerdo con nuestro análisis del apartado V):

- eEMGDE1 – Categoría
- eEMGDE2 – Identificador
    - eEMGDE2.1 – Secuencia de Identificador
    - eEMGDE2.2 – Esquema de identificador
- eEMGDE4 – Fechas
    - eEMGDE4.1 – Fecha Inicio
    - eEMGDE4.2 – Fecha fin (este sub-elemento se rellenará cuando finalice la existencia de una Entidad.

b. METADATOS COMPLEMENTARIOS

- eEMGDE3 – NOMBRE
    - eEMGDE3.1 –Nombre Natural
- eEMGDE5 – DESCRIPCIÓN
- eEMGDE8-SEGURIDAD
    - eEMGDE8.3-Permisos
- eEMGDE10 – CONTACTO
    - eEMGDE10.1 – Tipo de Contacto
    - eEMGDE10.2- Dato de Contacto

VI.4. ENTIDAD “ACTIVIDAD”

a. METADATOS OBLIGATORIOS

Deberán implementarse en los gestores documentales los siguientes **metadatos obligatorios** y sub-elementos asociados para la entidad Actividad (donde se han excluido aquellos sub-elementos no obligatorios que a nuestro juicio no aportan valor, o no resultan imprescindibles para la adecuación al ENI, de acuerdo con nuestro análisis del apartado V):

- eEMGDE1 – Categoría
- eEMGDE2 – Identificador
  - eEMGDE2.1 – Secuencia de Identificador
  - eEMGDE2.2 – Esquema de Identificador: cuadro de clasificación funcional de una organización
- eEMGDE4 – Fechas
  - eEMGDE4.1 – Fecha Inicio
  - eEMGDE4.2 – Fecha fin (este sub-elemento se rellenará cuando finalice la existencia de una Entidad –actividad-).

b. METADATOS COMPLEMENTARIOS

- eEMGDE3 – NOMBRE
  - eEMGDE3.1 –Nombre Natural
- eEMGDE5 – DESCRIPCIÓN
- eEMGDE8-SEGURIDAD
  - eEMGDE8.3-Permisos
- eEMGDE22 –CLASIFICACIÓN
  - eEMGDE22.1 – Código de clasificación
  - eEMGDE22.2 – Denominación de clase

VI.5. ENTIDAD “RELACIÓN”

a. METADATOS OBLIGATORIOS

Deberán implementarse en los gestores documentales los siguientes **metadatos obligatorios** y sub-elementos asociados para la entidad Relación (donde se han excluido aquellos sub-elementos no obligatorios que a nuestro juicio no aportan valor, o no resultan imprescindibles para la adecuación al ENI, como veremos en los apartados posteriores de esta ponencia):

- eEMGDE1 – Categoría
- eEMGDE2 – Identificador
  - eEMGDE2.1 – Secuencia de Identificador
  - eEMGDE2.2 – Esquema de Identificador: vocabulario controlado de las relaciones en una organización, o la configuración del sistema de nombrado de relaciones de una aplicación dada.
- eEMGDE4 – Fechas
  - eEMGDE4.1 – Fecha Inicio
  - eEMGDE4.2 – Fecha fin (este sub-elemento se rellenará cuando finalice la existencia de una Entidad –relación-).

- eEMGDE6 – Entidad Relacionada
  - eEMGDE6.1 – ID de Entidad Relacionada.
  - eEMGDE6.2 – Esquema de ID de Entidad Relacionada.
  - eEMGDE6.3 – Rol de la relación, que podrá tener dos valores:

    "1": indica que la relación se lee desde la entidad.

    "2": indica que la relación se lee en dirección hacia la entidad

b. METADATOS COMPLEMENTARIOS

- eEMGDE5 – Descripción
- eEMGDE21-Trazabilidad

VII. REQUISITOS DE CUMPLIMENTACIÓN DE LOS METADATOS SELECCIONADOS.

Este capítulo de la ponencia es sólo un esbozo de los temas que se tratan en él, dado su alcance, y debería ser abordado posteriormente en un grupo de trabajo interdisciplinar.

VII.1. ANÁLISIS DE LAS LISTAS DE VALORES ASOCIADAS A DETERMINADOS METADATOS.

- eEMGDE1-"CATEGORIA": Valor del tipo de entidad que se está describiendo. Se ha definido en eEMGDE un esquema de valores para cada tipo de entidad, excepto para Regulación.

Las posibles categorías para la entidad Regulación son definidas por cada organización en función de sus necesidades y normativas específicas. Las siete categorías que se prevén imprescindibles son:

- normativa para la atribución de competencias en cuanto a la generación de copias auténticas.
- otra normativa interna que regula una actividad.
- normativa externa que regula una actividad.
- Norma Técnica de Interoperabilidad.
- otras normas de carácter general.
- procedimiento administrativo interno (si tienen como destinatario a una unidad administrativa o empleado público).
- procedimiento administrativo externo (si tienen como destinatario al ciudadano o a las empresas).

Por otro lado, para la entidad Actividad se han definido 4 categorías: Función Marco, Función, Actividad, Acción. Es necesario definir la concordancia de estas categorías con las del Cuadro de Clasificación del Ministerio de Hacienda y Administraciones Públicas.

- eEMGDE2.2 – "ESQUEMA DE IDENTIFICADOR":
  - para una entidad de tipo "Actividad", se corresponderá con el esquema del cuadro de clasificación funcional de una organización.

- para una entidad de tipo “Agente”, si éste es una persona, se trataría del esquema del Número de Registro de Personal, y para una organización, el esquema del código de órgano.

- eMGDE5-“DESCRIPCION”, que permite introducir información en texto libre relativa a una entidad. Proponemos incorporar este metadato en el repositorio e-EMGDE del Sistema de Gestión Documental, con la finalidad de permitir a las aplicaciones de gestión del Departamento Ministerial introducir, si procede, el apunte del asiento en Registro Electrónico correspondiente al documento. Si el documento no ha ingresado a través de un Registro Electrónico, las aplicaciones gestoras podrán introducir cualquier información descriptiva en el metadato e-EMGDE5, como: resumen del texto, fecha de creación, autor, remitente, destinatario, etc.

- eEMGDE8.3-Permisos: autorización o acreditación de un Agente o Actividad, que determina sus derechos e acceso, uso y reutilización de los documentos. Se deberá definir su esquema de valores permitido en el seno del Ministerio de Hacienda y Administraciones Públicas.

- eEMGDE9.1-CONDICIONES DE ACCESO, USO Y REUTILIZACIÓN se usa “para proporcionar información acerca de la naturaleza de la limitación al acceso, uso y reutilización y de cualquier obligación en vigor para el usuario o receptor de los documentos”. Este metadato no tiene un esquema de valores definido en e-EMGDE, pero algunos ejemplos de valores que podría tomar son: Accesible sin derecho a reproducción, No accesible hasta la estabilización de la versión de la aplicación, o Reutilización autorizada con sujeción a condiciones generales. A efectos de su implantación en el Sistema de Gestión Documental, deberá acordarse en el Grupo de Trabajo de Coordinación de Archivos el esquema de valores permitido para eMGDE9.1 en el Ministerio de Economía y Hacienda, así como las acciones a las que dará lugar cada valor.

- eEMGDE13.1-VALORACION. Este metadato tiene un esquema de valores con cinco categorías posibles: Valor legal, Valor jurídico, Valor fiscal, Valor administrativo, Valor histórico o de investigación, Valor social. Recomendamos incluir una sexta categoría, “Valor esencial”, con dos valores posibles: “SI” o “NO”.

- eEMGDE15.1-SOPORTE. Define el objeto físico sobre el que se almacena el documento. No está definido su esquema de valores en e-EMGDE. Algunos posibles valores serían: CD-ROM, DVD, cinta.

- eEMGDE17-FIRMA:

  - e-EMGDE17.1-TIPO DE FIRMA. El e-EMGDE indica únicamente que el esquema de valores se atendrá a lo definido en el Capítulo II “De la identificación y autenticación” de la Ley 11/2007, de 22 de junio. No obstante, es preciso identificar la relación concreta de valores que se emplearán, para evitar problemas de interoperabilidad. Ejemplos de posibles valores serían: claves concertadas, firma electrónica incorporada al Documento Nacional de Identidad, firma electrónica avanzada, firma electrónica reconocida, firma electrónica para la actuación administrativa automatizada, Firma electrónica del personal al servicio de las Administraciones Públicas.

  - e-EMGDE17.2-FORMATO DE FIRMA. El e-EMGDE indica únicamente que el esquema de valores se atendrá a lo definido en las NTI de Política de Firma Electrónica y de Certificados de la Administración y la NTI de Catálogo de Estándares. No obstante, es preciso identificar la relación concreta de valores que se emplearán, para evitar problemas de interoperabilidad. Ejemplos de posibles valores serían: PADES, CADES detached, CADES attached, XADES internally detached, XADES enveloped.

  - e-EMGDE17.3-ROL DE FIRMA. El e-EMGDE indica únicamente que el esquema de valores será “desarrollado a nivel local y puede incluir valores como válida, auténtica, refrenda, visa, representa, testimonia, etc” . No obstante, es preciso identificar la relación concreta de valores que se emplearán, para evitar problemas de interoperabilidad. Ejemplos de posibles valores serían: Valida, Refrenda, Testimonia, Autentica, Visa, Representa.

VII.2 EXISTENCIA O NECESIDAD DE VOCABULARIOS CONTROLADOS

Para la preparación de este apartado, se sugiere la intervención de personal con formación en archivística, que determinen, a partir de la relación de metadatos identificada en el apartado VI, los vocabularios controlados (como *thesaurus* o índices) más apropiados para la finalidad descrita en el apartado V.

ANEXO 1. NORMAS LEGALES

1. Ley 16/1985, de 25 de junio, de Patrimonio Histórico Español
2. Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común
3. Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
4. 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 documentos administrativos en soporte distinto al original.
5. Ley 59/2003, de 19 de diciembre, de firma electrónica.
6. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
7. Instrucción de la Secretaría General Técnica de 10 de julio de 2007 sobre eliminación de documentos en el Ministerio del Interior.
8. Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público
9. RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
10. RD 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007.
11. RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
12. RD 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad dentro del ámbito de la Administración Electrónica.
13. Resolución de 11 de junio de 2011, de la Secretaría de Estado para la Función Pública, por el que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico.
14. Resolución de 11 de junio de 2011, de la Secretaría de Estado para la Función Pública, por el que se aprueba la Norma Técnica de Interoperabilidad de Expediente Electrónico.
15. Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por el que se aprueba la Norma Técnica de Interoperabilidad de Digitalización de Documentos.
16. Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por el que se aprueba la Norma Técnica de Interoperabilidad de Copiado Auténtico y Conversión entre Documentos Electrónicos.
17. RD 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso.
18. Resolución de 28 de junio de 2012, de la Secretaría de Estado para la Función Pública, por el que se aprueba la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.
19. Guía de adecuación al Esquema Nacional de Interoperabilidad.
20. Documento Electrónico - Guía de aplicación de la Norma Técnica de Interoperabilidad.
21. Expediente Electrónico - Guía de aplicación de la Norma Técnica de Interoperabilidad.
22. Política de Gestión de Documentos Electrónicos - Guía de aplicación de la Norma Técnica de Interoperabilidad.
23. Digitalización de Documentos – Guía de aplicación de la Norma Técnica de Interoperabilidad.
24. Copiado Auténtico y Conversión entre Documentos Electrónicos – Guía de aplicación de la Norma Técnica de Interoperabilidad

ANEXO 2. BIBLIOGRAFÍA

- MoReq2 Specification. Comisión Europea. 2008.
- ISAD(G), Norma Internacional General de Descripción Archivística. Consejo Internacional de Archivos. 2000.
- Norma UNE-ISO 15489. 2006.
- Norma UNE-ISO 23081. 2008.
- Norma UNE-ISO 30300. 2011.
- Norma UNE-ISO 30301. 2011.
- Australian Government Recordkeeping Metadata Standard Implementation Guidelines. Versión 2.0. National Archives of Australia. 2011.
- Australian Government Recordkeeping Metadata Standard Implementation Guidelines: Exposure Draft. National Archives of Australia. 2010.
- Diccionario de terminología archivística. Ministerio de Educación cultura y Deporte. Accesible en: http://www.mcu.es/archivos/MC/DTA/Diccionario.html
- Modelo de Gestión Documental del Gobierno Vasco. Departamento de Justicia y Administración Pública. Gobierno Vasco. 2010.
- Orientación sobre la elaboración de un esquema de metadatos (Norma UNE-ISO 23081). AENOR 2010.

Ponencia nº 2

Planteamiento de firma electrónica en la política de gestión de documentos electrónicos del MINHAP

Carmen Conejo Fernández y Álvaro Tapias Sancho (Dirección General del Catastro)

Ponencia nº 2

Planteamiento de firma electrónica en la política de gestión de documentos electrónicos del MINHAP

Carmen Conejo Fernández y Álvaro Tapias Sancho (Dirección General del Catastro)

INTRODUCCIÓN

Se plantea el establecimiento de un marco de firma electrónica en el contexto de la política de gestión de documentos electrónicos del Ministerio. Este planteamiento, abarcará todo el ciclo de vida de los documentos electrónicos y se adaptará a las realidades existentes en los distintos Centros Directivos del Ministerio.

ANTECEDENTES Y LEGISLACIÓN

La normativa actual en administración electrónica contempla el uso de sistemas de firma electrónica avanzada basada en certificados y sistemas de firma electrónica no avanzada, tanto para documentos generados por las propias administraciones como para los documentos aportados por los ciudadanos de forma electrónica.

Son, en cada caso, los responsables de los procedimientos los que, dentro del marco de la Ley 11/2007, el Real Decreto 1671/2009 y el Real Decreto 4/2010 y sus Normas Técnicas, deben establecer y habilitar el sistema de firma electrónica a utilizar en la gestión de sus documentos electrónicos.

La Ley 11/2007 reconoce, en su artículo 18.1, dos sistemas de firma para la actuación administrativa automatizada: Sello electrónico basado en certificado electrónico y Código Seguro de Verificación, ambos vinculados a la administración actuante.

La misma ley, en su artículo 13.2, establece que los ciudadanos pueden utilizar como sistemas de firma el DNI electrónico, sistemas de firma avanzada u otros sistemas de firma, como claves concertadas o la aportación de información conocida por ambas partes.

Por último, en su artículo 19, la ley 11/2007 regula el uso de sistemas de firma electrónica del personal al servicio de la Administración Pública, permitiendo que las Administraciones doten a sus empleados de los sistemas necesarios y permitiendo, en todo caso, el uso del DNI.

El Real Decreto 1671/2009, regula con mayor detalle los sistemas de firma electrónica contemplados en la Ley 11/2007. Además de los mencionados anteriormente, el Real Decreto, contempla también en su artículo 20 el uso de Código Seguro de Verificación como sistema de firma electrónica del personal al servicio de las Administraciones Públicas.

Este Real Decreto establece también, en su artículo 24, el desarrollo de una política de firma electrónica de la Administración General del Estado, política aprobada por resolución del 19 de julio de 2011 de la Secretaría de Estado para la Función Pública.

Por último, es importante comentar, por su importancia dentro de la política de gestión de documentos electrónicos, la regulación que se ha hecho en el Esquema Nacional de Interoperabilidad del uso de la firma electrónica en el documento electrónico.

El Real Decreto 4/2010 y las normas técnicas que lo desarrollan, establecen que los documentos electrónicos susceptibles de incorporarse a un expediente electrónico deberán firmarse electrónicamente, bien con CSV o bien con firma electrónica basada en certificado

electrónico acorde a la norma técnica de política de firma electrónica y certificados y a los formatos establecidos en la norma técnica de documento electrónico.

SITUACIÓN DEL MINISTERIO

Actualmente, en el MINHAP, existen Centros Directivos que utilizan como sistema de firma electrónica para la actuación administrativa automatizada y para la firma del personal al servicio del Centro firma electrónica avanzada basada en certificado, tal y como se recomienda en la política de firma electrónica y certificados de la Administración General del Estado.

De la misma forma, también hay Centros Directivos, con alta producción documental, que utilizan Código Seguro de Verificación para la firma de los documentos electrónicos que gestionan, tanto en la actuación administrativa automatizada como para la firma del personal a su servicio. A algunos de estos documentos firmados con Código Seguro de Verificación se les añade también un Sello electrónico del organismo.

Por todo ello, el planteamiento de firma electrónica, dentro de la política de gestión de documentos electrónicos del MINHAP, debe recoger las realidades de todos los Centros Directivos del ministerio y, por tanto, deberá dar cabida a todos los sistemas de firma electrónica amparados por la ley que se estén utilizando actualmente en el MINHAP.

En todo caso, el planteamiento recomendará e impulsará la mejora de los sistemas de firma electrónica a emplear en el futuro, con el objetivo de garantizar una mejor conservación de los documentos y una mayor seguridad e interoperabilidad de las firmas electrónicas.

PLANTEAMIENTO DE FIRMA ELECTRÓNICA

Dentro de la política de gestión de documentos electrónicos del MINHAP, se recomendará la utilización, tanto para la actuación administrativa automatizada como para la firma electrónica del personal al servicio de un Centro Directivo, de la firma electrónica avanzada basada en certificado electrónico, tal y como se regula en la Política de Firma Electrónica y Certificados de la Administración General del Estado y en las Normas Técnicas de Interoperabilidad de Documento y Expediente Electrónico.

Los sistemas de firma electrónica avanzada deberán garantizar, en la medida de lo posible y de acuerdo a las normas mencionadas anteriormente, la longevidad de las firmas con objeto de asegurar la longevidad de dichas firmas.

En todo caso, será posible también la utilización del Código Seguro de Verificación como sistema de firma para la actuación administrativa automatizada y como firma del personal al servicio del Centro Directivo. En este caso, se recomienda la utilización complementaria del Sello Electrónico del Organismo con objeto de mejorar la interoperabilidad del documento y la verificación de la firma electrónica de forma automática sin necesidad de acceder a la sede electrónica del organismo emisor del documento.

En caso de que sea necesario transferir documentos electrónicos firmados con Código Seguro de Verificación a otro Centro Directivo encargado de la posterior conservación, el Centro Directivo emisor de los documentos podrá firmar dichos documentos con Sello de organismo con objeto garantizar la autenticidad, integridad y mejor conservación del documento.

ESCENARIOS DE USO DE LA FIRMA ELECTRÓNICA

La firma electrónica se utilizará, en el ámbito del MINHAP, en los siguientes escenarios relativos al ciclo de vida de los documentos electrónicos:

- En la captura del documento a través del registro electrónico de los diferentes organismos del MINHAP.
- En la generación y emisión de documentos fruto de la actuación administrativa automatizada del MINHAP.

- En la generación y emisión de documentos que requieren firma de empleado público.
- En la generación de copias electrónicas auténticas de documentos, tanto en formato electrónico como en soporte papel.
- En el intercambio de expedientes y documentos electrónicos con el ciudadano y entre órganos administrativos, incluyendo aquellos en los que se transfiere la competencia de conservación del documento.
- En la puesta a disposición en sede electrónica de un documento.
- En los proceso objeto de garantizar la conservación de los documentos.

En los escenarios descritos, se utilizarán los sistemas de firma establecidos en la legislación básica: Política de firma de la AGE basada en certificados, y en la legislación sectorial de cada uno de los Centros Directivos del Departamento.

Ponencia nº 3

Tratamiento global del Registro. Documento sobre el Registro como trámite y como procedimiento de gestión

Luis Romera Iruela y Rosa Martín Rey (Secretaría General Técnica)

Ponencia nº 3

Tratamiento global del Registro. Documento sobre el Registro como trámite y como procedimiento de gestión

Luis Romera Iruela y Rosa Martín Rey (Secretaría General Técnica)

I. LA PALABRA "REGISTRO" TIENE DOS SENTIDOS DIFERENTES, QUE ES NECESARIO DISTINGUIR:

a. Proceso de gestión del documento electrónico, íntimamente relacionado con el proceso de "Captura" del documento en el SGDEA. De acuerdo con la Norma ISO 15489, *consiste en la introducción de una breve información descriptiva o de metadatos sobre el documento* ***y la asignación de un identificador único*** *dentro del sistema. El registro formaliza la incorporación del documento al sistema.*

b. Registro como operación de control de los documentos emitidos o recibidos por un órgano administrativo con entidad suficiente para ser formalmente asentados, bien por formar parte de un procedimiento administrativo o por otros motivos que lo hacen conveniente.

La NTI de Política de Gestión de Documentos Electrónicos, por su parte, al referirse en su Apartado VI a los procesos de gestión de los documentos electrónicos, especifica:

> *2.- Registro legal de documentos, definido en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común que, además del tratamiento de documentos electrónicos recibidos, atenderá a la posibilidad de digitalizar documentos en soporte papel según lo establecido en la Norma Técnica de Interoperabilidad de Digitalización de Documentos.*

De esta manera, la NTI se aparta del concepto de "registro" como proceso de gestión para identificarlo más bien con la operación de control administrativo definido en la Ley 30/1992. Esta definición trae como consecuencia inmediata que el Modelo de Política de Gestión de Documentos Electrónicos se halle referido más a esta segunda acepción que a la primera.

Así, en el Párrafo 21 del Modelo, de dice:

El registro y tramitación de los documentos y expedientes electrónicos presentados en el registro electrónico de la entidad con descriptor […] se realizará conforme al siguiente procedimiento:

[Incluir el procedimiento de registro electrónico de los documentos o una referencia al mismo]

La NTI del modelo de datos para el intercambio de asientos registrales está orientada precisamente al intercambio, por lo que se limita a especificar ese procedimiento, sin entrar propiamente en la asignación de número, por lo que no serviría para el propósito que se pretende.

En el punto 9.3 del Anexo III de la mencionada NTI se dedica expresamente a una recomendación para la digitalización de documentos en oficinas integradas en SIR, incluyendo unas orientaciones prácticas que engloban incluso unas recomendaciones sobre cómo actuar en los casos de incidencias más frecuentes. En este sentido, sería conveniente elaborar un protocolo de actuación que regulara la actuación del personal de los registros en aspectos como la digitalización en el momento de su presentación por parte del ciudadano, con o sin devolución de los mismos al presentador o digitalización en diferido, en caso de que lo primero no sea posible, especificando el destino de los documentos en papel depositados, en este caso, por el ciudadano, en la oficina de registro.

Dentro de este punto, en su subdivisión 9.3.2, se describe el proceso de digitalización con un gráfico sacado de la NTI de Digitalización, a la que remite para el proceso de conformación de la copia mediante la adición de metadatos. Pero llegados a ese punto, la copia digitalizada, como documento electrónico que es, debe cumplir con la NTI de Documento electrónico, lo que implica la necesidad de asignar a la copia un identificador único, que no se contempla en la NTI de Intercambio de asientos registrales.

II. LA ASIGNACIÓN DE UN IDENTIFICADOR ÚNICO AL DOCUMENTO.

El primero de los metadatos obligatorios contemplado en la NTI de Documento Electrónico referido específicamente al documento es el de Identificador. Este metadato está sometido a una estructura determinada y, una vez asignado a un documento, le identifica de manera unívoca durante todo su ciclo de vida.

Este número debe, al menos en teoría, ser asignado al documento por el sistema de gestión de documentos electrónicos en el momento de su captura en el mismo.

Por otra parte, el sistema sólo debe capturar documentos terminados y, de alguna forma, "designados" para ingresar en él. Si se trata de documentos generados por un órgano administrativo, la asignación puede hacerse de forma automática con tal que el sistema pueda "leer" los datos correspondientes a idioma, fecha y órgano productor.

El problema es mayor cuando se trata de documentos presentados por el ciudadano que pueden llegar tanto por la vía del Registro Electrónico de Documentos como por vía presencial. En ambos casos será lo normal que se integren en un procedimiento, razón por la cual deberá serles asignado un identificador único. Es en este momento cuando debe plantearse la cuestión de "quién y en qué momento" asigna el identificador único a estos documentos.

La posibilidad más operativa sería que fuese asignado por el propio Registro, ya se tratase de documentos originariamente en soporte digital como si son producto de una digitalización por haberse presentado en papel. Encontramos aquí un problema relacionado con la estructura del identificador único que ha de recoger el código del órgano gestor, tal y como aparece en el Directorio Común y la asignación de este código supone el conocimiento exacto de cuál es el órgano que, específicamente, va a tramitar al procedimiento, lo que es casi de imposible aplicación en el momento inicial.

Una posible solución sería aplicar un código ficticio en el que se sustituyesen los dígitos correspondientes al órgano por ceros o por algún otro signo gráfico que denotara que son documentos de los ciudadanos ingresados a través de registro. Quedaría por solucionar la forma más adecuada de asignar un identificador único a los documentos aportados como adjuntos al principal, si bien esto último podría obviarse considerándolos como un todo indivisible al que se asignaría un único identificador.

III. METAINFORMACIÓN.

Finalmente quedaría por comentar lo referente a los metadatos de los documentos digitalizados a su presentación en el Registro.

La NTI de Intercambio de asientos registrales presenta un mapeo de metadatos correspondientes a los campos "Validez del documento" del segmento de Anexo de SICRES 3.0 y el metadato "Estado de elaboración" de la NTI de documento electrónico.

El problema puede plantearse con el hecho de que, de acuerdo con lo dispuesto en el artículo 50 del Real Decreto 1671/2009, que trata de la obtención de copias electrónicas a efectos de compulsa y recoge el procedimiento de obtención y validación de copias electrónicas de documentos presentados en papel por los ciudadanos en el caso de que los originales no deban obrar en el procedimiento. "Estas copias digitalizadas, serán firmadas electrónicamente mediante los procedimientos previstos en los artículos 18 y 19 de la Ley 11/2007, de 22 de junio y tendrán el carácter de copia compulsada o cotejada previsto en el artículo 8 del Real Decreto 772/1992, de 7 de mayo, sin que en ningún caso se acredite la autenticidad del documento original...". En ningún caso podría atribuirse a estas copias el carácter de copia auténtica, ya que, al no tener el Registro la facultas de discernir acerca de la autenticidad de los documentos presentados por el ciudadano, la copia que genera no cumple el primero de los requisitos de las copias auténticas, es decir, que el documento copiado sea original o una copia auténtica. Se produce aquí, pues, un conflicto con la NTI de Documento electrónico, ya que entre los valores del metadato "Estado de elaboración", no se recoge el valor de "Copia compulsada", por lo que habría que estudiar si procede proponer una modificación de los valores de este último metadato obligatorio para incluirlo.

Ponencia nº 4

Elaboración de un Repertorio de Series Documentales para el Departamento

Luis Romera Iruela y Rosa Martín Rey (Secretaría General Técnica)

Índice de la Ponencia

I. INTRODUCCIÓN

El Artículo 21 del R. D. 4/2010, de 8 de enero, por el que se aprueba el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica establece que:

> *"Las Administraciones públicas adoptarán las medidas organizativas y técnicas necesarias con el fin de garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida. Tales medidas incluirán:*
>
> *e) La clasificación, de acuerdo con un plan de clasificación adaptado a las funciones, tanto generales como específicas, de cada una de las Administraciones públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas."*

Por su parte, el artículo 10.1, del R.D. 1708/2011, de 18 de noviembre, al enumerar las funciones de los archivos centrales, establece entre ellas:

2.º Llevar a cabo el proceso de identificación de series y elaborar el cuadro de clasificación.

La necesidad de contar con un cuadro de clasificación funcional se desprende asimismo de lo dispuesto en la Norma Técnica de Política de Gestión de Documentos electrónicos, al contemplar en su Apartado VI.3, la Clasificación de los documentos como uno de los procesos de gestión de los mismos:

> *Clasificación de documentos, que incluirá los criterios de formación de expedientes y agrupaciones de documentos electrónicos según la Norma Técnica de Interoperabilidad de Expediente Electrónico, así como la clasificación funcional de acuerdo con el cuadro de clasificación de la organización.*

II. ¿QUÉ ES LA IDENTIFICACIÓN DE SERIES?

Una definición ya clásica de "Identificación" es que esta operación consiste en "la investigación y estudio de las categorías administrativas y archivísticas en que se descompone un fondo de archivo", entendiendo como fondo de archivo el conjunto de documentos generado por un órgano administrativo en el ejercicio de sus funciones.

En palabras menos técnicas, consistiría en la detección de las diferentes series documentales generadas por un órgano administrativo, determinando para cada una de ellas su triple contexto de producción orgánico, funcional y procedimental.

III. ¿PARA QUÉ SIRVE LA IDENTIFICACIÓN DE SERIES?

La identificación de las series documentales no solamente permite conocer el quién, cómo y para qué de la generación de los documentos, es decir, su contexto de producción sino que es la base de su posterior valoración, que permitirá determinar los periodos de conservación y acceso a los documentos. La fase de valoración permite dar cumplimiento a las medidas que, en relación con la conservación de los documentos a lo largo de su ciclo de vida, se establecen en el Artículo 21.1, apartados f), g) y h) del Real Decreto 4/2010, de 8 de enero, anteriormente mencionado. Estas medidas se refieren a los periodos de conservación de los documentos, al acceso a los mismos y a las medidas a implementar para que se garantice su conservación a largo plazo, se asegure su valor probatorio y su fiabilidad como evidencia electrónica de las actividades y procedimientos, así como la transparencia, la memoria y la identificación de los órganos de las

Administraciones públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas que ejercen la competencia sobre el documento o expediente.

IV. ASPECTOS PRÁCTICOS DE LA IDENTIFICACIÓN DE LAS SERIES DOCUMENTALES:

La determinación del contexto de producción que hemos mencionado anteriormente exige el estudio de:

- Los órganos productores de la documentación
- La competencia y las funciones de dichos órganos sobre su ámbito competencial
- Los procedimientos administrativos, los trámites en que se descomponen y los documentos resultantes de cada uno de ellos.
- La normativa que los regula (en su caso), aspecto básico para determinar los periodos de permanencia de sus valores primarios y, en consecuencia, los periodos mínimos de conservación

V. RESULTADOS DE LA IDENTIFICACIÓN Y DE LA CONSIGUIENTE VALORACIÓN DE LAS DIFERENTES SERIES DOCUMENTALES PRODUCIDAS EN EL DEPARTAMENTO

Los resultados de la identificación y la valoración de las series documentales son de dos tipos:

- Por una parte, nos permite elaborar el cuadro de clasificación. El cumplimiento de lo dispuesto en el Esquema Nacional de Interoperabilidad nos llevará, en este caso, a priorizar en su elaboración los aspectos funcionales.
- Por otra, habremos obtenido una base sólida para cumplir con los requisitos del proceso de gestión de Calificación de los documentos al que se refiere el Apartado VI.6 de la NTI de Política de gestión del documento electrónico en sus tres apartados:
    - Determinación de los documentos esenciales.
    - Valoración de documentos y determinación de plazos de conservación.
    - Dictamen de la autoridad calificadora.

VI. PROCEDIMIENTO A UTILIZAR Y SU JUSTIFICACIÓN

Como hemos visto más arriba, la identificación completa de una serie documental supone un estudio a fondo de su contexto de creación, por lo que es una tarea forzosamente lenta. Pero, por otra parte, un programa de gestión de documentos no puede ponerse en marcha sin contar con un cuadro de clasificación. Por ello, si queremos avanzar en este campo, es preciso contar con un repertorio de series documentales, aunque sea provisional, que nos permita iniciar dicho programa. No partimos de cero, sino que existen ya diferentes herramientas, ciertamente de diferente valor y contenido, cuyo examen nos permitirá, al menos, iniciar la tarea que se nos ha encomendado.

Partimos, por un lado, de dos instrumentos que recogen, aunque sea de modo parcial, las series documentales que se generan en el Departamento:

- El catálogo de procedimientos recogidos en el Sistema de Información Administrativa (SIA)
- Las series recogidas en ACTÚA

Ambos instrumentos son parciales, no coinciden necesariamente entre sí y solamente contemplan los expedientes sometidos a procedimiento.

Por ello, tenemos previsto utilizar la información recogida en la Encuesta sobre los archivos del Departamento, que entendemos que puede permitirnos detectar no solamente la documentación que responde a un procedimiento sino otra que puede referirse a expedientes cuya función es el estudio o la constancia de determinados datos en los órganos administrativos.

Esta recogida de datos debería complementarse con carácter previo o, al menos, simultáneo, con la construcción de un cuadro de grandes funciones, funciones y subfunciones, aunque fuera a un nivel muy básico.

Para cada una de las series documentales es preciso recoger una serie de aspectos mínimos, que podríamos concretar en:

- **Elaboración del Repertorio de series**, con determinación de:
  - Denominación de la serie
  - Fechas extremas
  - Órgano productor a lo largo del tiempo
  - Función a la que responde
  - Frecuencia de utilización por el órgano productor
  - Plazo de transferencia al A. Central
  - Periodo mínimo de conservación
  - Criterios de acceso a los documentos
  - Documentos fundamentales para el Departamento.
- **Estudios orientados a la valoración y al dictamen** de cada una de ellas
  - Datos obtenidos en la fase de repertorio y además:
  - Normativa regulatoria
  - Trámites del procedimiento y documentos básicos resultantes
  - Series complementarias
  - Plazos de conservación y acceso

Para todo este proceso, es preciso contar con la colaboración de los órganos administrativos productores de la documentación.

Por otra parte, conviene establecer un método de trabajo, para lo que parece aconsejable la selección de dos órganos o unidades administrativas con las que poder llevar a cabo un proyecto piloto, que se extendería posteriormente al resto de los del Departamento. Se seleccionarían órganos con contenido de gestión y órganos de carácter predominantemente consultivo o servicios horizontales, cuya tramitación es predominantemente interna, para cubrir todos los aspectos de la producción documental.

Este método permitiría además, la elaboración de un embrión de Cuadro de Clasificación, que se creciendo a medida que los estudios fueran extendiéndose a l resto de los órganos del Departamento.

Ponencia nº 5

Estrategia de conservación de documentos en repositorio, conforme al calendario de conservación

Alejandro Millaruelo Gómez (Intervención General de la Administración del Estado)

Resumen de la ponencia:

Estrategia de conservación de documentos en repositorio, conforme al calendario de conservación

Alejandro Millaruelo Gómez (Intervención General de la Administración del Estado)
Ponencia nº 5

LA CONSERVACIÓN COMO UN PROCESO DE GESTIÓN DOCUMENTAL

El Esquema Nacional de Interoperabilidad establece que las Administraciones públicas adoptarán las medidas organizativas y técnicas necesarias con el objeto de garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida. Entre estas medidas se encuentra la definición de una política de gestión de documentos que será de obligado cumplimiento por parte de las Administraciones públicas.

Por otro lado determina que el desarrollo e implantación de los procesos, técnicas y operaciones de gestión de documentos electrónicos se concretará en un programa de tratamiento específico para la gestión de documentos y expedientes electrónicos.

Este programa se aplicará de manera continua sobre todas las etapas o períodos del ciclo de vida de los documentos y expedientes electrónicos, para los que garantizará su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, lo que permitirá la protección, recuperación y conservación física y lógica de los documentos y su contexto.

En base a esto la conservación no debería verse como un proceso de gestión documental exclusivo de las últimas fases del ciclo de vida de los documentos electrónicos, sino como un proceso que abarca toda su existencia, permitiendo de esta forma aplicar medidas de preservación y conservación a los documentos electrónicos desde el momento de su captura por el sistema de gestión de documentos.

POR QUÉ SE DEBEN CONSERVAR LOS DOCUMENTOS ELECTRÓNICOS

En base al marco legal de aplicación, las Administraciones Públicas utilizarán las tecnologías de la información asegurando, entre otras cosas, la conservación de los datos e informaciones que gestionen en el ejercicio de sus competencias.

Cada Administración deberá facilitar, además, el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico.

Se establece asimismo que se deberán conservar en soporte electrónico todos los documentos electrónicos utilizados en actuaciones administrativas que formen parte de un expediente administrativo y aquellos que tengan valor probatorio de las relaciones entre los ciudadanos y la Administración, en el formato original o en cualquier otro que asegure su integridad.

En este sentido podrán realizarse operaciones de conversión para preservar la conservación, el acceso y la legibilidad de los documentos electrónicos archivados.

Los períodos mínimos de conservación de los documentos electrónicos se determinarán por cada órgano administrativo siendo de aplicación las normas generales sobre conservación del patrimonio documental con valor histórico y sobre eliminación de documentos de la Administración General del Estado y sus organismos públicos.

QUÉ DOCUMENTOS ELECTRÓNICOS SE DEBEN CONSERVAR

La ley define documento electrónico como aquella "información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado", entre cuyos componentes se encuentra su contenido, definido como el "conjunto de datos o información del documento".

Para ser considerados válidos los documentos electrónicos deberán contener información de cualquier naturaleza, estar archivada la información en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado y disponer de los datos de identificación que permitan su individualización.

Por otro lado se deberán determinar aquellos documentos considerados como esenciales, a los cuales se les procurará una especial protección en base a su relevancia en relación a las funciones que desarrolla una organización.

La ley también establece que toda la documentación electrónica generada o recibida por cualquier organismo de la Administración pública forma parte del Patrimonio Documental, sin perjuicio del momento de su generación, y que su eliminación deberá ser autorizada por la Administración competente. En ningún caso se podrán destruir tales documentos en tanto subsista su valor probatorio de derechos y obligaciones de las personas o los entes públicos.

Por último la NTI de Documento Electrónico se aplica exclusivamente a documentos administrativos electrónicos y a "cualquier otro documento electrónico susceptible de formar parte de un expediente electrónico", lo que excluye expresamente documentos electrónicos que por sus características no se ajusten a uno de estos dos tipos.

Así pues, conjuntos documentales como el correo electrónico, por ejemplo, podrían quedar fuera de la aplicación de las Normas Técnicas de Interoperabilidad, aunque constituya una evidencia de la actuación de las Administraciones públicas y a pesar de que la misma ley determina que toda documentación electrónica forma parte del Patrimonio Documental.

DÓNDE SE DEBEN CONSERVAR LOS DOCUMENTOS ELECTRÓNICOS

Dos conceptos fundamentales en el proceso de gestión documental son el valor de los documentos y su ciclo de vida.

En cuanto al valor se distingue uno primario, que es el que posee en función de la finalidad por la que ha sido creado y uno secundario, que puede adquirir o no a lo largo del tiempo.

El ciclo de vida, o conjunto de las etapas o períodos por los que atraviesa la vida del documento, puede dividirse en una fase activa o de uso frecuente, una semiactiva o de uso ocasional y una inactiva que correspondería con la pérdida de valor primario y adquisición plena de un valor secundario (histórico o informativo).

Por otro lado el Esquema Nacional de Interoperabilidad determina que "las Administraciones públicas crearán repositorios electrónicos, complementarios y equivalentes en cuanto a su función a los archivos convencionales, destinados a cubrir el conjunto del ciclo de vida de los documentos electrónicos". Asimismo define repositorio electrónico como el "archivo centralizado donde se almacenan y administran datos y documentos electrónicos, y sus metadatos".

A su vez el RD 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos establece "el desarrollo de archivos digitales o repositorios de documentos en soporte electrónico".

Dos conceptos estrechamente ligados a los repositorios son los de SGDE o Sistema de Gestión de Documentos Electrónicos y SGDEA o Sistema de Gestión de Documentos Electrónicos de Archivo.

El primero permite la creación, edición y compartición de documentos electrónicos en el seno de una organización, además de su modificación o borrado, con lo que pueden conservarse distintas versiones de un mismo documento.

Cuando el documento electrónico alcanza una versión definitiva debe ingresar en un SGDEA, el cual asegurará la accesibilidad, disponibilidad, integridad y autenticidad de los documentos electrónicos que se encuentran en él, independientemente de los soportes de almacenamiento o los formatos de los ficheros.

CÓMO ABORDAR EL PROCESO DE CONSERVACIÓN DE DOCUMENTOS ELECTRÓNICOS

Este proceso debería abordarse mediante una estrategia de conservación, que incluya, como mínimo, los actores involucrados; los principios de conservación (unidad del documento digital; ciclo de vida; valor de los documentos; independencia de formatos y soportes); los requisitos (el principal, disponer de un cuadro de clasificación; metadatos complementarios; determinación de los soportes y las aplicaciones documentales; calificación); la definición de un repositorio o archivo electrónico; la determinación de los riesgos y los planes de contingencia y acciones correctoras correspondientes; los métodos (backup, protección continua de la información); las medidas técnicas (numeración unívoca; índice de expediente electrónico; metadatos; control de acceso); los formatos aceptados; los procedimientos (transferencia; eliminación; cambio de formatos) y, por último, las herramientas (como los calendarios de conservación).

Índice de la Ponencia

ÍNDICE DE LA PONENCIA

V. CÓMO ABORDAR EL PROCESO DE CONSERVACIÓN DE DOCUMENTOS ELECTRÓNICOS.

Definición de un plan de preservación

a. Actores involucrados en el proceso de conservación
b. Descripción de los elementos a proteger y las medidas de protección implantadas
c. Análisis de riesgos
d. Medidas de prevención

VI. ANEXO 1. NORMAS LEGALES.

VII. ANEXO 2. BIBLIOGRAFÍA.

I. LA CONSERVACIÓN COMO UN PROCESO DE GESTIÓN DOCUMENTAL

Política de gestión de documentos electrónicos. El proceso de conservación.

El Esquema Nacional de Interoperabilidad, en su artículo 21, con el objeto de garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida, indica que las Administraciones públicas adoptarán las medidas organizativas y técnicas necesarias.

Una de estas medidas es la definición de una política de gestión de documentos que, junto con una serie de normas técnicas de interoperabilidad, será de obligado cumplimiento por parte de las Administraciones públicas (disposición adicional primera).

La Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos, en su apartado III.2, nos dice que la política de gestión de documentos electrónicos:

- Se integrará en el marco general de gestión de documentos y en el contexto de cada organización junto al resto de políticas implantadas para el desempeño de sus actividades.

- Aplicará los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como los estándares y buenas prácticas nacionales e internacionales aplicables a la gestión documental atendiendo a la Norma Técnica de Interoperabilidad de Catálogo de Estándares.

En su apartado V señala además que:

- El diseño, desarrollo e implantación de los procesos, técnicas y operaciones de gestión de documentos electrónicos se concretará en un programa de tratamiento específico para la gestión de documentos y expedientes electrónicos.

- Dicho programa de tratamiento se aplicará de manera continua sobre todas las etapas o períodos del ciclo de vida de los documentos y expedientes electrónicos para los que garantizará su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad; permitiendo la protección, recuperación y conservación física y lógica de los documentos y su contexto.

Por último, en su apartado VI, indica que entre los procesos de gestión de documentos electrónicos de una organización, se incluirá, entre otros, la conservación de los documentos, en función de su valor y tipo de dictamen de la autoridad calificadora, a través de la definición de calendarios de conservación.

La NTI señala, además, como herramienta básica para el proceso de conservación los calendarios de conservación, que dependerán, en gran medida, de otro proceso de gestión documental: la calificación, entre cuyas acciones la propia NTI incluye la valoración y la determinación de plazos de conservación de los documentos.

La conservación como un proceso que se desarrolla durante todo el ciclo de vida de los documentos.

La conservación no debería verse como un proceso de gestión documental exclusivo de las últimas fases del ciclo de vida de los documentos electrónicos, sino como un proceso que abarca toda su existencia.

Esta visión nos ayudará a diseñar una política de gestión de documentos electrónicos integral que podrá aplicarse desde el mismo momento de la captura de los documentos por el sistema de gestión.

Así pues, desde el principio sería posible aplicar medidas de preservación y conservación a los documentos electrónicos, con lo que aseguraríamos su accesibilidad, confidencialidad, integridad y disponibilidad.

Resumen

Una política de gestión de documentos es un requisito para garantizar la interoperabilidad en relación a la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida.

La conservación es uno más de los procesos de gestión documental

La herramienta básica de este proceso son los calendarios de conservación

El proceso de calificación proporcionará información para completar los cuadros de conservación.

Un programa de tratamiento específico para la gestión de documentos y expedientes electrónicos se aplicará sobre todo el ciclo de vida de los documentos electrónicos, y permitirá la protección, recuperación y conservación física y lógica de los documentos y su contexto.

La conservación es un proceso que se desarrolla durante todo el ciclo de vida de los documentos.

II. POR QUÉ SE DEBEN CONSERVAR LOS DOCUMENTOS ELECTRÓNICOS

A continuación se hace un repaso de la legislación y de cómo la conservación de los datos y documentos electrónicos que gestionan, en el ejercicio de sus competencias, es una de las obligaciones legales que corresponden a las Administraciones públicas.

Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos

Artículo 1.2. Objeto de la Ley

Las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

Hay que hacer notar que no se habla de documentos, sino de datos, informaciones y servicios. Es decir, que las Administraciones públicas están obligadas a conservar los datos que posean, sean del tipo que sean.

Artículo 6.2. Derechos de los ciudadanos.

b. A no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información siempre que, en el caso de datos de carácter personal, se cuente con el consentimiento de los interesados (...).

e. A obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan la condición de interesado.

f. A la conservación en formato electrónico por las Administraciones Públicas de los documentos electrónicos que formen parte de un expediente.

Las Administraciones públicas deben conservar datos y documentos que estén en su poder, puesto que uno de los derechos reconocidos de los ciudadanos es no aportar esos mismos datos y documentos.

En este sentido, el artículo 9.1, sobre transmisiones de datos entre Administraciones Públicas, hace hincapié en que "para un eficaz ejercicio del derecho reconocido en el apartado 6.2.b), cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico (...)".

La conservación en formato electrónico de los documentos electrónicos que formen parte de un expediente, es también otro de los derechos que la ley reconoce a los ciudadanos.

En cuanto al apartado e), el artículo 30.1, sobre copias electrónicas, nos recuerda textualmente que "las copias realizadas por medios electrónicos de documentos electrónicos emitidos por el propio interesado o por las Administraciones Públicas, manteniéndose o no el formato original, tendrán inmediatamente la consideración de copias auténticas con la eficacia prevista en el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que el documento electrónico original se encuentre en poder de la Administración (...)".

El artículo 30.3 también recalca el aspecto de conservación de los documentos electrónicos al señalar que "las Administraciones Públicas podrán obtener imágenes electrónicas de los documentos privados aportados por los ciudadanos, con su misma validez y eficacia, a través de procesos de digitalización que garanticen su autenticidad, integridad y la conservación del documento imagen (...)".

Artículo 31. Archivo electrónico de documentos.

1. Podrán almacenarse por medios electrónicos todos los documentos utilizados en las actuaciones administrativas.

2. Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones.

3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.

Dos aspectos importantes a señalar en relación a este artículo:

31.2 Los documentos electrónicos administrativos se conservarán en soportes digitales, en el formato original o en cualquier otro que asegure su integridad.

31.3 Los soportes digitales deberán contar con medidas de seguridad que garanticen, entre otras cosas, la conservación de los documentos almacenados

Por último, en el artículo 42, se vuelve a hacer énfasis en el aspecto de conservación al indicar que el "Esquema Nacional de Interoperabilidad comprenderá el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad".

RD 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007

Artículo 43. Copias electrónicas de los documentos electrónicos realizadas por la Administración General del Estado y sus organismos públicos.

4. Los órganos emisores de los documentos administrativos electrónicos o receptores de los documentos privados electrónicos, o los archivos que reciban los mismos, están obligados a la conservación de los documentos originales, aunque se hubiere

procedido a su copiado conforme a lo establecido en el presente artículo, sin perjuicio de lo previsto en el artículo 52.

La existencia de copias electrónicas auténticas no exime a las Administraciones públicas de la conservación de los documentos originales.

Artículo 51. Archivo electrónico de documentos.

1. La Administración General del Estado y sus organismos públicos vinculados o dependientes deberán conservar en soporte electrónico todos los documentos electrónicos utilizados en actuaciones administrativas, que formen parte de un expediente administrativo, así como aquellos otros que tengan valor probatorio de las relaciones entre los ciudadanos y la Administración.

2. La conservación de los documentos electrónicos podrá realizarse bien de forma unitaria, o mediante la inclusión de su información en bases de datos siempre que, en este último caso, consten los criterios para la reconstrucción de los formularios o modelos electrónicos origen de los documentos así como para la comprobación de la firma electrónica de dichos datos.

El artículo 51 establece la obligatoriedad de conservar en soporte electrónico los documentos administrativos y los que tengan un valor de prueba, independientemente de que se puedan incluir en bases de datos o se conserven de forma unitaria.

Artículo 52. Conservación de documentos electrónicos.

1. Los períodos mínimos de conservación de los documentos electrónicos se determinarán por cada órgano administrativo de acuerdo con el procedimiento administrativo de que se trate, siendo en todo caso de aplicación, con la excepción regulada de la destrucción de documentos en papel copiados electrónicamente, las normas generales sobre conservación del patrimonio documental con valor histórico y sobre eliminación de documentos de la Administración General del Estado y sus organismos públicos.

2. Para preservar la conservación, el acceso y la legibilidad de los documentos electrónicos archivados, podrán realizarse operaciones de conversión, de acuerdo con las normas sobre copiado de dichos documentos contenidas en el presente real decreto.

3. Los responsables de los archivos electrónicos promoverán el copiado auténtico con cambio de formato de los documentos y expedientes del archivo tan pronto como el formato de los mismos deje de figurar entre los admitidos en la gestión pública por el Esquema Nacional de Interoperabilidad.

El artículo 52 indica que serán los órganos administrativos los que determinarán los períodos mínimos de conservación en función del procedimiento administrativo. Además establece que, en aras de su conservación, los documentos electrónicos podrán cambiar de formato.

RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

Artículo 1. Objeto.

1. El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

Este artículo remarca el objetivo de este Real Decreto: la protección de la información mediante una serie de principios básicos y requisitos mínimos que aseguren el acceso, la inte-

gridad, la disponibilidad, la autenticidad, la confidencialidad, la trazabilidad y la conservación de los datos, informaciones y servicios.

Artículo 11. Requisitos mínimos de seguridad.

2. Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente. Esta política de seguridad se establecerá en base a los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

   j) Protección de la información almacenada y en tránsito.

La protección de la información almacenada y en tránsito es uno de los requisitos mínimos de seguridad.

Artículo 21. Protección de la información almacenada y en tránsito.

2. Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones públicas en el ámbito de sus competencias.

En este artículo se hace mención expresa a los documentos electrónicos producidos por las Administraciones públicas, y los procedimientos que aseguren su recuperación y conservación a largo plazo (nótese que no se hace referencia al conjunto de documentos electrónicos, ya sean públicos o privados, que las Administraciones gestionan, cuando estos comparten por ejemplo procedimiento administrativo).

RD 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad dentro del ámbito de la administración electrónica

Artículo 21. Condiciones para la recuperación y conservación de documentos.

1. Las Administraciones públicas adoptarán las medidas organizativas y técnicas necesarias con el fin de garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida. Tales medidas incluirán:

   a. La definición de una política de gestión de documentos en cuanto al tratamiento, de acuerdo con las normas y procedimientos específicos que se hayan de utilizar en la formación y gestión de los documentos y expedientes.

   b. La inclusión en los expedientes de un índice electrónico firmado por el órgano o entidad actuante que garantice la integridad del expediente electrónico y permita su recuperación.

   c. La identificación única e inequívoca de cada documento por medio de convenciones adecuadas, que permitan clasificarlo, recuperarlo y referirse al mismo con facilidad.

   d. La asociación de los metadatos mínimos obligatorios y, en su caso, complementarios, asociados al documento electrónico, a lo largo de su ciclo de vida, e incorporación al esquema de metadatos.

   e. El período de conservación de los documentos, establecido por las comisiones calificadoras que correspondan, de acuerdo con la legislación en vigor, las normas administrativas y obligaciones jurídicas que resulten de aplicación en cada caso.

   f. El acceso completo e inmediato a los documentos a través de métodos de consulta en línea que permitan la visualización de los documentos con todo el detalle de su contenido, la recuperación exhaustiva y pertinente de los documentos, la copia o descarga en línea en los formatos originales y la impresión a pa-

pel de aquellos documentos que sean necesarios. El sistema permitirá la consulta durante todo el período de conservación al menos de la firma electrónica, incluido, en su caso, el sello de tiempo, y de los metadatos asociados al documento.

g. La adopción de medidas para asegurar la conservación de los documentos electrónicos a lo largo de su ciclo de vida, de acuerdo con lo previsto en el artículo 22, de forma que se pueda asegurar su recuperación de acuerdo con el plazo mínimo de conservación determinado por las normas administrativas y obligaciones jurídicas, se garantice su conservación a largo plazo, se asegure su valor probatorio y su fiabilidad como evidencia electrónica de las actividades y procedimientos, así como la transparencia, la memoria y la identificación de los órganos de las Administraciones públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas que ejercen la competencia sobre el documento o expediente.

h. Transferencia, en su caso, de los expedientes entre los diferentes repositorios electrónicos a efectos de conservación, de acuerdo con lo establecido en la legislación en materia de Archivos, de manera que se pueda asegurar su conservación, y recuperación a medio y largo plazo.

i. Si el resultado del procedimiento de evaluación documental así lo establece, borrado de la información, o en su caso, destrucción física de los soportes, de acuerdo con la legislación que resulte de aplicación, dejando registro de su eliminación.

2. A los efectos de lo dispuesto en el apartado 1, las Administraciones públicas crearán repositorios electrónicos, complementarios y equivalentes en cuanto a su función a los archivos convencionales, destinados a cubrir el conjunto del ciclo de vida de los documentos electrónicos.

Este artículo 21 fija, por un lado, algunas medidas organizativas y técnicas orientadas a garantizar la interoperabilidad en relación a la conservación de los documentos durante su ciclo de vida, y por otro, establece la obligación de creación de repositorios electrónicos que equivalgan en funciones a los archivos convencionales y que cubran todo el ciclo de vida de los documentos electrónicos.

Artículo 22. Seguridad.

1. Para asegurar la conservación de los documentos electrónicos se aplicará lo previsto en el Esquema Nacional de Seguridad en cuanto al cumplimento de los principios básicos y de los requisitos mínimos de seguridad mediante la aplicación de las medidas de seguridad adecuadas a los medios y soportes en los que se almacenen los documentos, de acuerdo con la categorización de los sistemas.

2. Cuando los citados documentos electrónicos contengan datos de carácter personal les será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo.

3. Estas medidas se aplicarán con el fin de garantizar la integridad, autenticidad, confidencialidad, disponibilidad, trazabilidad, calidad, protección, recuperación y conservación física y lógica de los documentos electrónicos, sus soportes y medios, y se realizarán atendiendo a los riesgos a los que puedan estar expuestos y a los plazos durante los cuales deban conservarse los documentos.

4. Los aspectos relativos a la firma electrónica en la conservación del documento electrónico se establecerán en la Política de firma electrónica y de certificados, y a través del uso de formatos de firma longeva que preserven la conservación de las firmas a lo largo del tiempo.

En relación a los medios y soportes empleados para almacenar documentos electrónicos, con el objeto de asegurar su conservación, este artículo señala que se aplicará lo previsto

en el Esquema Nacional de Seguridad, y si contienen datos de carácter personal lo dispuesto en la Ley Orgánica 15/1999. Las medidas de seguridad tendrán en cuenta, además, los riesgos potenciales y el plazo de conservación de los documentos. Por otro lado la Política de firma electrónica y de certificados establecerá el papel de la firma electrónica en la conservación de los documentos, especialmente en el uso de formatos de firma longeva. Por último este artículo indica que, en caso de que la firma y los certificados no puedan garantizar la autenticidad de los documentos, ésta se asegurará a través de su conservación en repositorios electrónicos y por el uso de metadatos de gestión de documentos.

Artículo 23. Formatos de los documentos.

1. Con el fin de garantizar la conservación, el documento se conservará en el formato en que haya sido elaborado, enviado o recibido, y preferentemente en un formato correspondiente a un estándar abierto que preserve a lo largo del tiempo la integridad del contenido del documento, de la firma electrónica y de los metadatos que lo acompañan.
2. La elección de formatos de documento electrónico normalizados y perdurables para asegurar la independencia de los datos de sus soportes se realizará de acuerdo con lo previsto en el artículo 11.
3. Cuando exista riesgo de obsolescencia del formato o bien deje de figurar entre los admitidos en el presente Esquema Nacional de Interoperabilidad, se aplicarán procedimientos normalizados de copiado auténtico de los documentos con cambio de formato, de etiquetado con información del formato utilizado y, en su caso, de las migraciones o conversiones de formatos.

El artículo 23 establece que el documento se conservará en su formato original, aunque se remarca la preferencia por formatos normalizados y de estándar abierto. El objetivo es independizar los datos de su soporte. Cuando los formatos empleados queden obsoletos se emplearán procedimientos de copiado auténtico con cambio de formato.

RD 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso

Artículo 20. Condiciones para la recuperación y conservación del documento electrónico.

1. Los Departamentos Ministeriales y las entidades de derecho público vinculadas o dependientes de los mismos, adoptarán las decisiones organizativas y las medidas técnicas necesarias con el fin de garantizar la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida. Entre éstas:
    a. La identificación clara y precisa de cada uno de los documentos mediante un código unívoco que permita su identificación en un entorno de intercambio interadministrativo. (= artº 21.1 c RD 4/2010 ENI)
    b. La asociación de los metadatos mínimos obligatorios y, en su caso, complementarios asociados al documento electrónico. (= artº 21.1 d RD 4/2010 ENI)
    c. La inclusión, en el caso de los expedientes electrónicos, de un índice electrónico firmado por el órgano o entidad actuante que garantice la integridad del mismo y permita su recuperación. (= artº 21.1 b RD 4/2010 ENI)
    d. La recuperación completa e inmediata de los documentos a través de métodos de consulta en línea a los datos que permita la visualización de los documentos de modo que sean legibles e identificables. (= artº 21.1 g RD 4/2010 ENI)
    e. La adopción de medidas para garantizar la conservación de la memoria e identificación de los órganos que ejercen la competencia sobre el documento o ex-

pediente para que el ciudadano de hoy y del futuro pueda comprender el contexto en el que se creó. (= artº 21.1 h RD 4/2010 ENI)

f. El mantenimiento del valor probatorio de los documentos y expedientes y de las evidencias electrónicas como prueba de las actividades y procedimientos, así como la observancia de las obligaciones jurídicas que incumban a los servicios. (= artº 21.1 h RD 4/2010 ENI)

g. La transferencia de los expedientes electrónicos a los archivos históricos para la conservación permanente, de acuerdo con lo establecido en la normativa vigente, de manera que se pueda asegurar su conservación y accesibilidad a medio y largo plazo. (= artº 21.1 j RD 4/2010 ENI)

h. El borrado de la información, en su caso, o si procede la destrucción física de los soportes, de acuerdo con un procedimiento regulado y dejando registro de su eliminación. (= artº 21.1 k RD 4/2010 ENI)

i. La valoración y el establecimiento de las estrategias que se pueden aplicar para la conservación a medio y largo plazo de los documentos, tales como procedimientos de emulación, migración y conversión de formatos.

Observemos que este artículo 20.2 del RD 1708/2011 se inspira directamente en el artículo 21.1 del RD 4/2010 ENI (de hecho se titulan prácticamente igual), repitiendo buena parte de los puntos relacionados con la recuperación y conservación, aunque con una redacción algo distinta.

Artículo 21. Aplicación de las tecnologías de la información y comunicaciones en la gestión y tratamiento de los documentos.

Los Departamentos Ministeriales y sus organismos vinculados o dependientes promoverán en todo momento el uso de las tecnologías de la información y el conocimiento en el tratamiento archivístico de los documentos de su competencia y en todo lo relativo a las funciones de conservación, gestión, acceso y difusión que tiene encomendadas, mediante:

c. La aplicación de los principios básicos y los requisitos mínimos requeridos para una protección adecuada de la información con el fin de asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

Este artículo es prácticamente una reproducción del artículo 1.1 del RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Resumen

[Ley 11/2007] Las Administraciones Públicas utilizarán las tecnologías de la información asegurando, entre otras cosas, la conservación de los datos e informaciones que gestionen en el ejercicio de sus competencias.

[Ley 11/2007] Los ciudadanos tienen derecho a no aportar documentos o datos que obren en poder de las Administraciones públicas, a obtener copias electrónicas de los documentos de los procedimientos en los que tengan la condición de interesado y en que se conserven en formato electrónico por las Administraciones Públicas los documentos electrónicos que formen parte de un expediente.

[Ley 11/2007] Cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico.

[Ley 11/2007] Los documentos electrónicos administrativos se conservarán en soportes digitales, en el formato original o en cualquier otro que asegure su integridad.

[Ley 11/2007] Los soportes digitales deberán contar con medidas de seguridad que garanticen, entre otras cosas, la conservación de los documentos almacenados.

[RD 1671/2009] La existencia de copias electrónicas auténticas no exime de la conservación de los documentos originales.

[RD 1671/2009] Se deberán conservar en soporte electrónico todos los documentos electrónicos utilizados en actuaciones administrativas que formen parte de un expediente administrativo y aquellos que tengan valor probatorio de las relaciones entre los ciudadanos y la Administración.

[RD 1671/2009] La conservación de los documentos electrónicos podrá realizarse bien de forma unitaria o mediante la inclusión de su información en bases de datos.

[RD 1671/2009] Los períodos mínimos de conservación de los documentos electrónicos se determinarán por cada órgano administrativo siendo de aplicación las normas generales sobre conservación del patrimonio documental con valor histórico y sobre eliminación de documentos de la Administración General del Estado y sus organismos públicos.

[RD 1671/2009] Para preservar la conservación, el acceso y la legibilidad de los documentos electrónicos archivados, podrán realizarse operaciones de conversión.

[RD 1671/2009] Se empleará el copiado auténtico con cambio de formato de los documentos y expedientes del archivo tan pronto como el formato de los mismos deje de figurar entre los admitidos en la gestión pública por el Esquema Nacional de Interoperabilidad.

[RD 3/2010 ENS] La política de seguridad del organismo contemplará, entre otros requisitos mínimos, la protección de la información almacenada y en tránsito.

[RD 3/2010 ENS] Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones públicas en el ámbito de sus competencias.

[RD 4/2010 ENI] Medidas organizativas y técnicas necesarias que garanticen la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida:

- Definición de una política de gestión de documentos.
- Índice electrónico firmado en los expedientes.
- Metadatos obligatorios y complementarios.
- Período de conservación de los documentos.
- Acceso durante todo el período de conservación (al menos de la firma electrónica, incluido, en su caso, el sello de tiempo, y de los metadatos asociados al documento).
- Medidas para asegurar la conservación de los documentos electrónicos a lo largo de su ciclo de vida, asegurando su recuperación de acuerdo con el plazo mínimo.
- Transferencia de los expedientes entre los diferentes repositorios electrónicos a efectos de conservación.
- Si así se establece borrado de la información, o en su caso, destrucción física de los soportes.

[RD 4/2010 ENI] Se crearán repositorios electrónicos, complementarios y equivalentes en cuanto a su función a los archivos convencionales, destinados a cubrir el conjunto del ciclo de vida de los documentos electrónicos.

[RD 4/2010 ENI] A los soportes que almacenen documentos se les aplicarán las medidas de seguridad adecuadas, con objeto de cumplir los principios básicos y los requisitos mínimos de seguridad previstos en el Esquema Nacional de Seguridad.

[RD 4/2010 ENI] Se tendrán en cuenta los riesgos a lo largo del plazo de conservación a los que están expuestos los soportes que almacenen documentos electrónicos.

[RD 4/2010 ENI] En cuanto a la firma electrónica, uso de formatos de firma longeva que preserven la conservación de las firmas a lo largo del tiempo.

[RD 4/2010 ENI] Conservación de los documentos en su formato original.

[RD 4/2010 ENI] Preferencia de uso de formatos normalizados.

[RD 4/2010 ENI] Por obsolescencia del formato se aplicará un procedimiento de copiado auténtico de documentos con cambio de formato.

III QUÉ DOCUMENTOS ELECTRÓNICOS SE DEBEN CONSERVAR

Dato, documento electrónico, expediente electrónico y copia auténtica desde la perspectiva de la Ley 11/2007

La ley 11/2007 habla de documentos electrónicos, documentos electrónicos administrativos (en base al artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común) y expedientes electrónicos (definidos como el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan, artículo 32.1).

En cuanto al documento electrónico, en su artículo 30 distingue entre documento electrónico original, copia electrónica auténtica (de documentos emitidos por el propio interesado o por las Administraciones públicas) e imagen electrónica o documento imagen (referida sólo a documentos privados digitalizados), aunque son igualmente válidos siempre que se cumplan una serie de requisitos (firma electrónica, sello de tiempo, original en poder de la administración, etc.).

En el artículo 34, donde se definen los criterios para la gestión electrónica, se indica que se considerará "la supresión o reducción de la documentación requerida a los ciudadanos, mediante su sustitución por datos, transmisiones de datos o certificaciones (...)", sin aclarar expresamente la relación u origen de estos datos en relación a los documentos electrónicos.

En el artículo 35.3, que trata sobre la iniciación del procedimiento por medios electrónicos, señala que "con objeto de facilitar y promover su uso, los sistemas normalizados de solicitud podrán incluir comprobaciones automáticas de la información aportada respecto de datos almacenados en sistemas propios o pertenecientes a otras administraciones (...)".

En este caso es fácil deducir que los datos de los que habla podrían proceder de otros procedimientos, de datos que se almacenan en bases de datos y registros de la propia Administración, etc.

De hecho, en el apartado III de la Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico, entre los componentes que forman parte de un documento electrónico se encuentra su contenido, definido como el "conjunto de datos o información del documento".

El RD 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad dentro del ámbito de la administración electrónica, recoge en su glosario de términos una definición de dato:

- Una representación de hechos, conceptos o instrucciones de un modo formalizado, y adecuado para comunicación, interpretación o procesamiento por medios automáticos o humanos.

Finalmente, en el anexo de la ley se define documento electrónico como aquella "información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado".

No hemos de olvidar que en este mismo anexo se describe la interoperabilidad como "la capacidad de los sistemas de información y, por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos". La inter-

operabilidad pues, trabaja con datos, no expresamente con documentos, considerando obviamente aquellos como una parte integrante de éstos.

En esta línea el RD 1671/2009, de 16 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, en su artículo 41, establece las características que deberán cumplir los documentos electrónicos para ser considerados válidos:

- Contener información de cualquier naturaleza.
- Estar archivada la información en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.
- Disponer de los datos de identificación que permitan su individualización, sin perjuicio de su posible incorporación a un expediente electrónico.

Este mismo artículo añade, en relación a los documentos administrativos electrónicos, el requisito de "haber sido expedidos y firmados electrónicamente mediante los sistemas de firma previstos en los artículos 18 y 19 de la Ley 11/2007, de 22 de junio, y ajustarse a los requisitos de validez previstos en la Ley 30/1992, de 26 de noviembre".

En cuanto a las copias electrónicas de los documentos electrónicos realizadas por la Administración General del Estado y sus organismos públicos (artículo 43), estas tendrán la misma validez que el documento original si "no comportan cambio de formato ni de contenido".

Si por el contrario éste fuera el caso, para que adquiera la condición de copia auténtica, además de que el documento original se encuentre en poder de la Administración, debe incluir por un lado su carácter de copia entre los metadatos asociados y, por otro, que sea autorizada mediante firma electrónica conforme a los sistemas recogidos en los artículos 18 y 19 de la Ley 11/2007, de 22 de junio.

Documentos esenciales desde la perspectiva de la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos

Esta Norma Técnica de Interoperabilidad establece que uno de los procesos de gestión de documentos es la calificación, una de cuyas funciones primordiales es la determinación de los documentos esenciales para una organización. ¿Qué podemos entender por éstos?

En la Guía de Aplicación de la Norma Técnica de Interoperabilidad, en su punto 73, se nos aclara que "la determinación de los documentos esenciales sirve a los efectos de procurar una especial protección a aquellos documentos que tienen una singular relevancia en relación a las funciones que desarrolla una organización". Además la Guía propone que la gestión de los documentos esenciales se organice, a nivel de programa de tratamiento para la gestión de documentos electrónicos, en dos actividades.

La primera consistiría en "la obtención de una copia auténtica de acuerdo con lo especificado en la NTI de Procedimientos de copiado auténtico y conversión entre documentos electrónicos". La segunda en la "conservación de la copia auténtica obtenida en un servidor adecuado con el fin de minimizar los riesgos que pudieran ser producidos en caso de siniestro y con las medidas de seguridad adecuadas según el ENS".

Documento y Patrimonio Documental desde la perspectiva de la Ley 16/1985, de 25 de junio, de Patrimonio Histórico Español

Esta ley en su artículo 49.1 define documento como "toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos".

Si bien este artículo no añade más información ni contradice la definición que hemos visto hacían las Normas Técnicas de Interoperabilidad sobre documento electrónico, en cambio el apartado 2 del mismo artículo tiene unas implicaciones mayores: en él se señala que "forman parte del Patrimonio Documental los documentos de cualquier época generados, conservados o reunidos en el ejercicio de su función por cualquier organismo o entidad de carácter público (...)".

Así pues, toda la documentación electrónica generada o recibida por cualquier organismo de la Administración pública formaría parte del Patrimonio Documental, sin perjuicio del momento de su generación.

Además, en su artículo 55.1, la ley establece que "la exclusión o eliminación de bienes del Patrimonio Documental (...) deberá ser autorizada por la Administración competente". En el artículo 55.2 hace hincapié en que "en ningún caso se podrán destruir tales documentos en tanto subsista su valor probatorio de derechos y obligaciones de las personas o los entes públicos".

¿Qué tipos de documentos electrónicos deben contemplarse en una política de gestión de documentos?

La NTI de Documento Electrónico se aplica exclusivamente a documentos administrativos electrónicos y a "cualquier otro documento electrónico susceptible de formar parte de un expediente electrónico" (apartado II, ámbito de aplicación), lo que excluye expresamente documentos electrónicos que por sus características no se ajusten a uno de estos dos tipos.

La primera consecuencia de esta definición es la obligatoriedad de incluir en expedientes todo documento electrónico no administrativo, si queremos que su tratamiento se ajuste a la Norma Técnica. La segunda, y derivada de la primera, es el hecho de que todo documento electrónico deberá ir firmado electrónicamente.

Una tercera consecuencia es que se excluyen de la aplicación de la Norma Técnica aquellos documentos electrónicos que no formen parte de expedientes o que no estén firmados electrónicamente.

En relación a esto pueden emplearse las denominadas agrupaciones facticias, de forma que determinados documentos que no son producto de un trámite administrativo puedan incluirse en un expediente electrónico de tipo facticio, asegurando por tanto su conservación y permitiendo la aplicación de las normas de interoperabilidad.

Por contra, por citar un ejemplo, a los correos electrónicos recibidos y enviados por una organización pública en cumplimiento de sus funciones, salvo que se incluyeran en un expediente y se firmarán para garantizar su autenticidad e integridad, no se les aplicaría la NTI de Documento Electrónico.

Además, el hecho de que sólo a los correos "normalizados", es decir, incluidos en un expediente y firmados electrónicamente, se les pudiera aplicar la NTI y, por tanto, disponer de características adecuadas para la interoperabilidad de los datos, rompería su unidad al clasificarlos en función del tema del que tratan.

Esta distinción entre documentos ENI y no ENI perjudicaría, sin duda, las posibilidades de conservación a largo plazo de este tipo de conjuntos documentales, se consideren o no como series.

Algo similar podría decirse de aquellos datos que, recogidos por las Administraciones públicas en el ejercicio de sus competencias, no adquieren una forma documental definida, ya sea porque no corresponden a un procedimiento administrativo o porque responden a procedimientos internos.

Está claro, desde nuestra perspectiva, que debe buscarse la forma de integración de estos conjuntos documentales o de estos datos en un entorno donde la interoperabilidad sea un requisito fundamental para garantizar la conservación de la información independientemente de la forma que adopte.

Así pues, basándonos en los preceptos de la Ley 19/1985, cuando se trate de series o conjuntos documentales bien definidos, deberían incluirse en la política de gestión de documentos del organismo, buscando el modo de adaptarse a las normas técnicas de interoperabilidad.

Otro punto a parte es el del encaje de las series de datos "no documentales" que, aunque desde una perspectiva como la de la norma ISO 15489:1 y debido a que constituyen evidencias de la actividad pública, podrían integrarse en una política de gestión de documentos. En este caso habría que buscar el amparo de la ley para poder incluirlas o descartarlas por completo (aunque uno de los modos “sencillos” de incluirlas es darles categoría de documento electrónico).

Recordemos finalmente que esta norma ISO define documento como "aquella información producida, recibida y conservada como evidencia y con finalidades informativas por parte

de una persona u organización, de acuerdo con las obligaciones legales o en el desarrollo de sus actividades".

Resumen

Documento que se ajusta al ENI:

- Documento administrativo electrónico y documento electrónico que forme parte de un expediente.

Documentos esenciales:

- Aquellos documentos que tienen una singular relevancia en relación a las funciones que desarrolla una organización.

Todos los documentos electrónicos, generados o recibidos por las Administraciones públicas en el ejercicio de sus competencias forman parte del Patrimonio Documental.

No se podrán destruir tales documentos en tanto subsista su valor probatorio de derechos y obligaciones de las personas o los entes públicos.

Su eliminación deberá ser autorizada por la Autoridad competente.

Existen documentos electrónicos excluidos de la aplicación del ENI.

Existen series de datos no documentales que son evidencia de la actividad de la Administración.

IV DÓNDE SE DEBEN CONSERVAR LOS DOCUMENTOS ELECTRÓNICOS

El ciclo de vida de los documentos y su valor

Dos conceptos fundamentales en el proceso de gestión documental de conservación son, por una lado, el del ciclo de vida de los documentos y, por otro, el de su valor.

Se distinguen dos tipos de valores de los documentos:

1. **Valor primario**, que es el que posee un documento en función de la finalidad por la que ha sido creado. En este caso pueden distinguirse varios tipos de valores primarios: administrativo, jurídico, legal, contable, fiscal, etc..
2. **Valor secundario**, que es el que algunos documentos adquieren con el paso del tiempo, y que puede ser de tipo informativo o histórico.

Es necesario conocer el valor que tienen los documentos a lo largo del tiempo (mediante el proceso documental de valoración) con objeto de confeccionar los calendarios de conservación, que veremos más adelante.

En cuanto al ciclo de vida de los documentos electrónicos, en el glosario del RD 4/2010, de 8 de enero por el que se regula el Esquema Nacional de Interoperabilidad, se define este concepto como el

"conjunto de las etapas o períodos por los que atraviesa la vida del documento, desde su identificación en un sistema de gestión de documentos, hasta su selección para conservación permanente, de acuerdo con la legislación sobre Archivos de aplicación en cada caso, o para su destrucción reglamentaria."

Este concepto es un concepto clásico de la archivística que fue desarrollado en los Estados Unidos en los años 30 y 40 del siglo XX. En su origen contemplaba tres etapas o fases, a saber:

1. Fase activa

a. Corresponde con la creación y captura del documento y con el período de tramitación del procedimiento del que forma parte.

b. Posee un valor primario, y su consulta es frecuente.

c. A nivel de archivo estaríamos hablando de los archivos de gestión o administrativos.

2. Fase semiactiva

a. Una vez que el período de tramitación ha concluido y pasado cierto tiempo, que será diferente para las distintas series documentales, la consulta del documento se vuelve inexistente o infrecuente.

b. Corresponde con el momento en que el documento va perdiendo su valor primario (aunque sigue manteniendo su valor probatorio de derechos y obligaciones) y en contraposición puede ir, aunque no siempre, adquiriendo un valor secundario. Su consulta se vuelve infrecuente o inexistente.

c. Esta fase corresponde con los archivos centrales e intermedios.

3. Fase inactiva

a. Cuando un documento ha perdido por completo su valor primario, por lo que ya no será consultado en relación a este valor, diremos que se trata de documentación en fase inactiva.

b. Si el valor secundario del documento justifica su conservación permanente será transferido a los denominados archivos históricos. En caso contrario se procederá a su expurgo o eliminación, aunque en determinados casos se conserve una pequeña muestra de la serie documental, como referencia.

c. Esta fase corresponde con el archivo histórico.

El RD 1708/2011, de 18 de noviembre, por el que se establece el sistema Español de Archivos, en su artículo 15.3, se hace eco del ciclo de vida en tres fases, al indicar que "los calendarios de conservación, determinarán para cada serie o agrupación documental, las fases de actividad, semiactividad o inactividad administrativa y delimitarán los períodos de permanencia de los documentos en cada uno de los tipos de archivo definidos según el ciclo vital."

Ahora bien, existe una segunda aproximación que distingue también tres fases de ciclo de vida de un documento electrónico, aunque en este caso no se basan en la frecuencia de su uso o su valor sino en la continuidad de procesos.

Así en la Guía de aplicación de la Norma Técnica de Interoperabilidad de Expediente Electrónico, en sus puntos 26 y 28, se dice que "a pesar de que la NTI de Expediente Electrónico no incluye una descripción del ciclo de vida del expediente como tal (...) esta guía describe, a tal fin, las diferentes fases de un ciclo de vida genérico (...) en tres fases: 'Apertura', Tramitación' y 'Conservación y selección'."

En la misma Guía se detalla, en relación a estas tres fases, que "dentro de este ciclo, la formación del expediente, entendida como el proceso mediante el cual se crea el expediente y su índice y se produce la incorporación ordenada y sucesiva de documentos, tiene lugar a lo largo de las fases de 'Apertura' y 'Tramitación'. Concluida la tramitación, el expediente se cierra y pasa a 'Conservación y selección' para, según corresponda, su archivado o destrucción."

Si tomamos este modelo de ciclo de vida y lo aplicamos a los distintos tipos de archivo, tendríamos que las fases de apertura y tramitación podrían corresponder con el archivo de gestión y la fase de conservación con el central y, si fuera el caso, con los archivos intermedio e histórico.

Repositorios electrónicos

En el artículo 21.2 del RD 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad, se determina que "las Administraciones públicas crearán repositorios electrónicos, complementarios y equivalentes en cuanto a su función a los archivos convencionales, destinados a cubrir el conjunto del ciclo de vida de los documentos electrónicos".

En el glosario de términos del RD se define repositorio electrónico como el "archivo centralizado donde se almacenan y administran datos y documentos electrónicos, y sus metadatos".

Asimismo el artículo 21 del RD 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos, en su apartado b), establece que "los Departamentos Ministeriales y sus organismos vinculados o dependientes promoverán en todo momento el uso de las tecnologías de la información y el conocimiento en el tratamiento archivístico de los documentos de su competencia y en todo lo relativo a las funciones de conservación, gestión, acceso y difusión que tiene encomendadas, mediante (...) el desarrollo de archivos digitales o repositorios de documentos en soporte electrónico (...)".

SGDE vs. SGDEA

Un SGDE o Sistema de Gestión de Documentos Electrónicos es un sistema de tratamiento documental que permite la creación, edición y compartición de documentos electrónicos en el seno de una organización. Permite la modificación o borrado de los documentos, con lo que pueden conservarse distintas versiones de un mismo documento, así como almacenar documentación de apoyo que se considere necesaria para la tramitación.

Cuando el documento electrónico alcanza una versión definitiva, en cuanto adquiere una característica de originalidad y, por tanto, no se admiten modificaciones, éste debe ingresar en un SGDEA o Sistema de Gestión de Documentos Electrónicos de Archivo.

El SGDEA deberá asegurar la accesibilidad, disponibilidad, integridad y autenticidad de los documentos electrónicos que se encuentran en él, independientemente de los soportes de almacenamiento o los formatos de los ficheros.

Otras características específicas de un SGDEA son, entre otras:

- Proporcionar funcionalidades de consulta y búsqueda de información.
- Permitir la asignación de metadatos complementarios o de gestión documental.
- Gestionar fondos y series documentales.
- Soportar formatos de conservación a largo plazo (como PDF/A o firmas longevas).
- Permitir copias electrónicas auténticas con cambio de formato.
- Gestionar transferencias a repositorios electrónicos distintos o expurgos de los documentos.

El repositorio o archivo electrónico que veíamos en el apartado anterior formaría parte de un SGDEA.

Sistema de Archivos de la Administración General del Estado

El RD 1708/2011, de 18 de noviembre, por el que se establece el sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso, en sus artículos 6 y 7 define por un lado el Sistema de Archivos de la Administración General del Estado como

> "el conjunto de sistemas archivísticos departamentales, órganos, archivos y centros de la Administración General del Estado y de sus organismos públicos, que actúan de manera coordinada con la finalidad de garantizar la correcta gestión de los fondos, colecciones, documentos y otras agrupaciones documentales producidos o reunidos en el ejercicio de sus competencias y facilitar el acceso de los ciudadanos a los mismos".
>
> Y por otro establece la composición del Sistema de Archivos, formado por:
>
> "los archivos, centros, servicios y, en su caso, sistemas archivísticos de los departamentos ministeriales, y de sus organismos públicos existentes y los que en el futuro puedan crearse reglamentariamente".

El mismo RD, en su artículo 8, enumera las clases de archivos en función del ciclo de vida de los documentos:

- Archivos de oficina o de gestión.
- Archivos generales o centrales de los Ministerios y de los organismos públicos dependientes de los mismos.
- Archivo intermedio.
- Archivos históricos.

Los archivos de oficina o de gestión, tal como señala el artículo 9 del RD, "son aquellos archivos existentes en todos los órganos y unidades administrativas para la custodia de los documentos en fase de tramitación o sometidos a continua utilización y consulta administrativa".

Una de las responsabilidades, entre otras, del archivo será, "transferir los documentos al Archivo central, en la forma y tiempo establecidos en el correspondiente calendario de conservación elaborado de manera conjunta con el Archivo Central, una vez agotado su plazo de permanencia en la unidad productora".

Por otro lado el artículo 10 del mismo RD establece que los archivos generales o centrales de los Ministerios son los encargados de "la custodia de los documentos, una vez finalizada su tramitación y transcurridos los plazos establecidos por la normativa vigente o en los calendarios de conservación"., responsabilizándose además de, entre otras tareas, de:

- "proporcionar el asesoramiento técnico necesario a las unidades y a su archivo de gestión, con el fin de conseguir la correcta conservación y tratamiento técnico de los documentos de archivo, de acuerdo con las normas específicas que correspondan a cada serie documental";
- "llevar a cabo el proceso de identificación de series y elaborar el cuadro de clasificación";
- "llevar a cabo procesos de valoración documental, a fin de elevar las correspondientes propuestas de eliminación, o en su caso, de conservación permanente de documentos";
- "realizar las transferencias preceptivas y periódicas de documentos al archivo intermedio, acompañadas de su correspondiente relación de entrega".

Los archivos intermedio e histórico no son objeto de estudio al depender del Ministerio de Cultura y exceder de los límites de esta ponencia.

El artículo 14 señala que "con carácter general, los Archivos integrados en el Sistema (...) en todas las fases del ciclo vital de los documentos (...)" deberán "garantizar la integridad, autenticidad, fiabilidad, disponibilidad, confidencialidad y conservación de los documentos y expedientes electrónicos recibidos o almacenados, según lo establecido por la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en los Esquemas Nacionales de Seguridad e Interoperabilidad, y demás normativa de desarrollo".

El artículo 20 de este RD, en el que se detallan las condiciones para la recuperación y conservación del documento electrónico, establece en su apartado 1 que "las disposiciones del presente Real Decreto relativas a los documentos integrantes del Sistema de Archivos de la Administración General del Estado, serán de aplicación también a los documentos en soporte electrónico, con las especialidades derivadas de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, de los Esquemas Nacionales de Seguridad e Interoperabilidad, y demás normativa de desarrollo".

V CÓMO ABORDAR EL PROCESO DE CONSERVACIÓN DE DOCUMENTOS ELECTRÓNICOS

Como hemos visto en los capítulos anteriores, el proceso de conservación debe aplicarse de manera continua a lo largo de todo el ciclo de vida de los documentos electrónicos, para asegurar su recuperación, tal como señala el Esquema Nacional de Interoperabilidad en su artículo 21.

Obviamente no puede contemplarse de forma aislada de otros procesos de gestión documental. De hecho existen algunos requisitos, derivados de estos mismos procesos, que facilitarán su desarrollo e implementación, a saber:

- Disponer de un **cuadro de clasificación** basado en las funciones del organismo. Este es, probablemente, un requisito crucial para abordar el proceso de conservación, ya que permite la organización de los documentos y expedientes electrónicos y, especialmente, la determinación de qué datos (o documentos) serán objeto de un tratamiento diferenciado para ser conservados.

- **Calificación del valor** de las series documentales, que ayudará a ubicar los documentos electrónicos en los soportes de almacenamiento más adecuados, tanto en relación a su coste como a sus características de rendimiento.

- Determinar los **documentos esenciales** y las medidas de protección aplicables.

Por otro lado, asociado al cuadro de clasificación es indispensable contar con un **calendario de conservación**, definido en el RD 1708/2011, de 18 de noviembre, por el que se establece el sistema Español de Archivos, como

> "el instrumento de trabajo fruto del proceso de valoración documental, en el que se recoge el plazo de permanencia de los documentos de archivo en cada una de las fases del ciclo vital para su selección, eliminación o conservación permanente y, en su caso, el método y procedimiento de selección, eliminación o conservación en otro soporte."

Asimismo, para determinar el entorno concreto y el alcance de este proceso, sería recomendable identificar los sistemas de información que manejan documentos electrónicos y los sistemas de almacenamiento, soportes y tecnologías involucrados.

Con el objetivo de cumplir adecuadamente los preceptos del Esquema Nacional de Interoperabilidad, las organizaciones públicas deberían contar con un **plan de preservación** de los documentos electrónicos, basado en:

a. Un análisis de los riesgos que pueden amenazar su conservación a largo plazo, teniendo en cuenta las características de los soportes de almacenamiento, los formatos de los documentos, el software, el hardware, los tipos de datos (estructurados o no) y las medidas de protección disponibles.

b. Y en la adopción de medidas preventivas que reduzcan el nivel de riesgo.

Además la posibilidad de que estas mismas organizaciones tengan que realizar funciones de archivo central, intermedio o, incluso, histórico, durante un período de tiempo más o menos largo, confiere a este plan de preservación una importancia y urgencia mayores que las que hubiera tenido de no ser así.

Este plan debería garantizar principalmente la accesibilidad, autenticidad, disponibilidad, integridad, inteligibilidad, y legibilidad de los documentos electrónicos a lo largo de su ciclo de vida, frente a riesgos que hemos clasificado en cinco grupos:

En primer lugar, los derivados de la continua evolución de la tecnología y la consiguiente obsolescencia de la misma.

En segundo lugar, los que son consecuencia de un mal funcionamiento o de un uso erróneo de la tecnología, y que pueden ocasionar la pérdida o degradación de los documentos electrónicos, total o parcialmente.

En tercer lugar, los que proceden de una posible descontextualización de los documentos electrónicos.

En cuarto lugar, los que forman parte del ámbito de la seguridad de las TI y que pueden suponer una alteración intencionada de los documentos electrónicos o su misma desaparición (accesos no permitidos, ataques, robo de soportes, etc.).

En quinto y último lugar, aquellos que directa o indirectamente derivan del aumento constante del volumen de documentos y en paralelo de los costes necesarios para asegurar el entorno adecuado de conservación.

Para cada uno de estos grupos de riesgos cada organización debería definir y detallar en el plan de preservación, las medidas concretas para prevenirlos, minimizar su impacto y garantizar la conservación de los documentos electrónicos. En este sentido sería fundamental seguir una política de prevención antes que una política de corrección, para lo que sería recomendable evaluar periódicamente los riesgos y comprobar que las medidas preventivas se ajustan a los mismos.

Definición de un plan de preservación

Un plan de preservación a largo plazo de los documentos digitales de una organización debería incluir como mínimo los siguientes aspectos:

a. Actores involucrados en el proceso de conservación

b. Descripción de los elementos a proteger y las medidas de protección implantadas

c. Análisis de riesgos

d. Medidas de prevención

a. Actores involucrados en el proceso de conservación

Se indicarían los distintos actores involucrados (personal técnico, de administración, empresas colaboradoras, dirección), etc., sus funciones y responsabilidades.

b. Descripción de los elementos a proteger y las medidas de protección implantadas

Se trataría principalmente de elaborar una relación de los elementos involucrados en el seno de la organización en el proceso de conservación (documentos electrónicos, cuadro de clasificación, soportes de almacenamiento, software, hardware, etc.), describir sus características más relevantes, detallar la interdependencia que existe entre ellos (especialmente de cara a sufrir una contingencia) y, finalmente, indicar las medidas de protección ya adoptadas o disponibles.

Estos elementos podrían ser los siguientes:

- Los sistemas de información de la organización;
- las aplicaciones;
- los distintos procedimientos administrativos;
- las correspondientes series documentales;
- el calendario de conservación;
- los documentos considerados esenciales;
- los formatos empleados en los documentos electrónicos;
- si se trata de datos estructurados (bases de datos) o no;
- los sistemas de ficheros empleados;
- los sistemas informáticos que dan soporte a los procesos de negocio;
- los sistemas de almacenamiento y los soportes utilizados en función del ciclo de vida de los documentos;
- las políticas de backup y la retención de los datos salvaguardados;
- los sistemas de redundancia de datos (réplicas);
- y cualquier otro elemento que se considere relevante de cara a la conservación.

Esta descripción sería la base para realizar posteriormente un análisis de riesgos.

c. Análisis de riesgos

Teniendo en cuenta los cinco grupos de riesgos que hemos señalado con anterioridad y los elementos a proteger y la relación entre ellos, se deberían determinar los posibles riesgos y el grado de ocurrencia de los mismos. Este análisis serviría para determinar las medidas necesarias para prevenirlos o minimizar sus posibles efectos, y evaluar la conveniencia de las ya implantadas.

A continuación se describe, a modo de ejemplo, una parte de los riesgos a los que están sometidos los documentos electrónicos y que pueden comprometer directa o indirectamente su conservación a largo plazo:

En cuanto a la obsolescencia

- De los soportes de almacenamiento
  - Sería necesario disponer de un catálogo de soportes, con indicación de su vida útil supuesta en condiciones óptimas y su antigüedad.
- De los formatos
  - Sería importante conocer los errores o defectos conocidos de cada formato empleado.
- Del software
  - Sería recomendable contar con la información acerca del historial de cambio de versiones y de la evolución prevista por los propios fabricantes.
- Del hardware
  - Se debería conocer, por ejemplo, la antigüedad del hardware, la posibilidad de disponer de piezas de recambio y la existencia de contratos de soporte y mantenimiento.

En cuanto a errores o fallos de la tecnología

- Degradación de los soportes
  - Su causa puede deberse a una manipulación incorrecta de los mismos, a un almacenamiento que no se atiene a las indicaciones del fabricante en cuanto condiciones ambientales, al desgaste, etc.
- Corrupción o pérdida de datos
  - Determinados errores o la combinación de una serie de ellos podrían ocasionar alteraciones de la secuencia de bits en la que se almacenan los documentos electrónicos, lo que perjudicaría su legibilidad.
- Fallo en los soportes o en el hardware
  - En este sentido sería recomendable contar con el historial de fallos y errores de los soportes o el hardware, y sus causas.
  - Asimismo sería importante conocer el MTBF (*mean time between failures*, o tiempo medio entre fallos) de cada soporte, especificado por el fabricante del mismo.
- Errores en las aplicaciones
  - Ya sean éstas de desarrollo propio o aplicaciones comerciales, contando con la existencia en este caso de errores conocidos, deberían registrarse los errores sufridos y sus posibles causas.

En cuanto a la descontextualización de los documentos

- Ausencia de metadatos adecuados para la contextualización de los documentos electrónicos.

En cuanto a la seguridad

- Ataques (internos o externos) que modifiquen o eliminen documentos electrónicos.
- Virus que puedan alterar los documentos o sus metadatos asociados.
- Robo (de soportes, especialmente en tránsito).

En cuanto al aumento de documentos y los costes asociados

- Falta de espacio de almacenamiento.

- Rendimiento no ajustado a las necesidades de acceso de los sistemas de almacenamiento.
- Incapacidad de realizar copias de seguridad debido al volumen de los datos a salvar o exceder la ventana de backup (período de tiempo durante el cual se establece que se llevarán a cabo las copias de seguridad, sin que estas afecten al rendimiento de los sistemas o a las aplicaciones).

d. Medidas de prevención

Una vez que se conocen los elementos a proteger y su interdependencia y los riesgos a los que están sometidos, sería indispensable determinar las medidas de prevención necesarias para asegurar la conservación de los documentos electrónicos a largo plazo (o, al menos, el tiempo que se haya estipulado que deban conservarse), comprobar si están o no disponibles y evaluar si funcionan como se espera que lo hagan.

Existen una serie de medidas genéricas de prevención, que se detallan en la norma ISO/TR 18492:2005 "Conservación a largo plazo de información electrónica basada en documentos", o en las recomendaciones recogidas en la guía creada por el Grupo de Trabajo del Subcomité de Gestión de documentos y archivos de ISO, responsable de la conservación de documentos electrónicos en el ámbito de la gestión documental (ISO - TC 46/SC 11 / WG 7).

En general, parte de las medidas recogidas en esta ponencia se basarían en alguno de estos tipos:

- Refresco o renovación (copia entre dos mismos tipos de soportes, sin cambio en los datos).
- Migración (copia a otro tipo de soporte, sistema o formato).
- Replicación (creación de un duplicado de los datos, como medio de protección ante la pérdida o degradación de los mismos).
- Emulación (reproducir las funcionalidades de un sistema o soporte obsoleto).
- Encapsulación (los documentos contienen en sí mismos todos los elementos que forman un objeto digital, por ejemplo, los metadatos, las firmas asociadas y el propio documento).
- Empleo de estándares abiertos no propietarios.

Un segundo conjunto de medidas tendrían que ver con conceptos propios de los sistemas informáticos, como la alta disponibilidad, la redundancia de elementos para evitar los denominados puntos únicos de fallo, etc.

A continuación se detallan a modo de ejemplo, para cada tipo de riesgo identificado, una serie de medidas que podrían incluirse en un plan de preservación.

En cuanto a la obsolescencia

- De los soportes de almacenamiento
  - Refresco o renovación: realizar copias en el mismo tipo de soporte, antes de llegar al final de su vida útil.
  - Migración: hacer una copia del contenido de un soporte a otro tipo distinto, o de un sistema de almacenamiento a otro.
- De los formatos
  - Migración a un formato considerado longevo, especialmente en documentos de conservación permanente.
  - Uso de estándares y formatos abiertos, en vez de formatos propietarios.
- Del software
  - Actualización de las versiones, según las recomendaciones de los fabricantes.

- Migración a otro tipo de software. Podría provocar cambios en los formatos de los documentos, lo que alteraría su integridad.
- Emulación: es una alternativa complicada y, seguramente, de elevado coste.
- Con objeto de que la obsolescencia del software no comprometa la conservación a largo plazo de los documentos electrónicos, podría ser recomendable reducir su dependencia de aplicaciones o bases de datos con estándares propietarios, al menos en la fase semiactiva o inactiva de la documentación, independizándolos de las mismas. A continuación se describen una serie de consideraciones en relación a este tipo de medidas:

  - Almacenar los documentos electrónicos en una base de datos presenta, en principio, unas ventajas funcionales:

    - Simplifica la administración.
    - Facilita la salvaguardia de los datos, puesto que existen procedimientos y herramientas de backup específicamente orientados para estos entornos.
    - Permite una transaccionalidad más sencilla.
    - No hay necesidad de mantener enlaces externos entre los registros de la base de datos y los ficheros, con los riesgos potenciales de pérdida o modificación de rutas, renombrado accidental de ficheros, posibles agujeros de seguridad, etc.
    - Los sistemas gestores de bases de datos (DBMS) proporcionan funcionalidades como la gestión de la integridad, control de accesos, trazabilidad, etc.

  - Por el contrario:

    - El almacenamiento exclusivo de los documentos electrónicos en bases de datos con estándares propietarios supone un riesgo para la conservación a largo plazo de estos documentos, debido a la obsolescencia segura del software.
    - Igualmente al tratarse de sistemas propietarios la migración de los documentos a otro software puede resultar una operación costosa en recursos o difícil técnicamente, lo que podría comprometer la conservación de los mismos documentos almacenados.
    - Un tamaño excesivo de la base de datos que contiene los documentos electrónicos perjudicaría el rendimiento y la realización de copias de seguridad y podría comprometer su recuperación ante un desastre.
    - En este caso para reducir el tamaño y el tiempo de las copias de seguridad, al menos las que se realizan con más frecuencia, podrían emplearse métodos como el particionamiento de la base de datos:

      ✓ Las tablas que contienen documentos de un determinado rango de fechas se convierten en tablas de sólo lectura y, por tanto, inmodificables.

      ✓ Las copias de seguridad podrían excluir estas tablas, reduciendo el volumen de los datos que a salvar.

      ✓ Adicionalmente estas particiones podrían almacenarse en soportes o sistemas de almacenamiento más económicos.

  - Una alternativa al almacenamiento de los documentos electrónicos en bases de datos podría ser su almacenamiento en sistemas de ficheros, independientes de estas mismas bases de datos.

- En este caso las bases de datos contendrían la ruta donde efectivamente se almacenan los documentos electrónicos.

- Este sistema podría tener algunas ventajas frente al uso de bases de datos:
  - Independizaría efectivamente a los documentos de las bases de datos con estándares propietarios, lo que a largo plazo podría facilitar la conservación de esos documentos.
  - Podría emplearse un tipo de soporte de almacenamiento más económico (por ejemplo, discos duros de gran tamaño).
  - Aunque depende de muchos factores, el acceso a los documentos podría llegar a ser más rápido.
  - En función de la configuración de los sistemas gestores de bases de datos (DBMS), podría hacerse un uso más eficiente de la memoria, al necesitar menos para la recuperación de los documentos.
  - Podría reducirse el tamaño de las copias de seguridad, al reemplazarlas por otros sistemas de protección propios de sistemas de almacenamiento como son las réplicas.
- En todo caso, se nos presentarían varias alternativas:
  - Almacenar los documentos electrónicos firmados junto con sus metadatos en bases de datos como “Internal Binary Large Objects” (i-BLOB). Los i-BLOB son objetos de datos binarios de gran tamaño, que se almacenan directamente en tablas de la base de datos. Participan en el modelo transaccional típico de las bases de datos, garantizando las propiedades ACID (atomicidad, consistencia, aislamiento y durabilidad). El uso de este tipo de objetos binarios puede ocasionar la redundancia de los datos, al guardar varias veces un mismo objeto.
  - Almacenar los metadatos en bases de datos y los documentos electrónicos firmados como “External Binary Large Objects” (e-BLOB). Los e-BLOB son objetos de datos binarios de gran tamaño que, al contrario que los i-BLOB, se almacenan en archivos del sistema de ficheros fuera de las tablas de la base de datos. Son más eficientes para operaciones de lectura de objetos de tamaño muy grande. Asimismo su uso limita la posible redundancia de los objetos binarios puesto que permite referencias únicas a los mismos. No forman parte sin embargo de las transacciones de la base de datos, por lo que deberá ser el sistema de ficheros el que proporcione las garantías de integridad y el resto de propiedades ACID.
  - Almacenar los metadatos en bases de datos y los documentos electrónicos firmados en sistemas de ficheros, manteniendo en aquellas únicamente los enlaces a los documentos. Este sistema tendría, frente a los dos anteriores, las ventajas y desventajas expuestas más arriba, y permitiría independizar el almacenamiento de los documentos electrónicos de los formatos propietarios de las bases de datos.
  - Almacenar los metadatos y los documentos electrónicos firmados conjuntamente en sistemas de ficheros (como un objeto digital) y mantener una copia de los metadatos y el enlace a los documentos en la base de datos. Esta alternativa, variación de la anterior, facilitaría la realización de búsquedas. En este caso podría incluso llegar a guardarse en un campo de la base de datos el texto plano del documento.
  - De todas formas, para seleccionar la alternativa más adecuada que garantice una serie de factores como la facilidad de administración, un rendimiento óptimo en cuanto a las necesidades de acceso, unas medidas de seguridad adaptadas a la naturaleza de la información

contenida en los documentos, y la integridad y conservación de esos documentos, habría que considerar su ciclo de vida y la fase de archivo en la que se encontrarían en cada momento.

- Así pues, podría emplearse una estrategia que combine, para distintos series de documentos o fracciones de estas mismas series, cualquiera de las alternativas señaladas.

– Del hardware

  - Migración, a otro hardware que, como hemos visto con el software, podría suponer cambios en los formatos de los documentos electrónicos.
  - Emulación (aunque sería la opción menos recomendable por su coste y las complicaciones que supondría mantener sistemas que emulen las funcionalidades de otros sistemas).

En cuanto a errores o fallos de la tecnología

– Sistemas RAID que aseguren los datos frente a fallos de los discos duros.

– Redundancia de los documentos mediante replicación:

  - La unidad mínima de replicación sería un volumen que contenga documentos electrónicos.
  - Hay que indicar que un soporte de tipo cinta magnética corresponde a un volumen, mientras que en un sistema de almacenamiento (con discos duros) pueden existir centenares o miles de volúmenes.
  - En este sentido hay que recalcar la necesidad de tener bien localizados y ubicados los soportes, sean del tipo de sean, que contienen documentos electrónicos.
  - En la misma línea podría ser recomendable no mezclar documentos electrónicos y otros tipos de datos no relacionados con ellos en los mismos soportes.
  - La replicación, por otro lado, se realizaría siempre entre soportes de la misma naturaleza, en cuanto tipo y capacidad.
  - Para realizar las réplicas se emplearían las utilidades que suelen incorporar los mismos sistemas de almacenamiento o software especializado que permita hacerlas.
  - La réplica, según su ubicación, podría ser de dos tipos:
    - Remota, cuando su destino es un sistema de almacenamiento diferente situado en un edificio o ciudad distintos.
    - Local, cuando es el mismo sistema de almacenamiento el que alberga las réplicas.
  - Ambas formas de replicación no son incompatibles, por lo que en función de los recursos disponibles, del valor de los documentos electrónicos y de la necesidad de minimizar los posibles riesgos, podría ser recomendable combinarlas.
  - Aun así sería preferible disponer, como mínimo, de una réplica remota.
  - Otro aspecto a determinar sería el número de réplicas que se consideran necesarias y su periodicidad. En este sentido habría que tener presente que las réplicas en disco, al ser más rápidas que las que se hacen a cinta magnética, por ejemplo, suelen reescribirse.

– Utilización de sistemas de almacenamiento de alta disponibilidad (doble controladora activo-activo, fuentes de alimentación redundadas, memoria caché con espejo (mirror), etc.) que eviten puntos únicos de fallo y reduzcan las posibilidades de pérdidas de información.

– Técnicas de backup que permitan la recuperación de los documentos electrónicos a un estado previo.

- Almacenamiento de soportes de cinta magnética en condiciones ambientales controladas (armarios ignífugos, humedad, temperatura, etc., según recomendaciones de los fabricantes de los mismos soportes).
- Para documentos electrónicos digitalizados, en su fase semiactiva o inactiva, contar con un conjunto denominado "fichero maestro", en un formato considerado longevo (como TIFF, por ejemplo), a partir del cual se obtendrían las copias de consulta.
- Realizar comprobaciones periódicas de los distintos soportes, especialmente los de cinta magnética, para asegurarse de que mantienen todas sus propiedades y no presentan ningún tipo de degradación previa al final de su vida útil esperada.

En cuanto a la descontextualización de los documentos electrónicos

- Uso de metadatos específicos de conservación, que aseguren la contextualización de los documentos electrónicos. En este sentido podría emplearse un estándar como los metadatos de preservación PREMIS.
- Considerar los documentos electrónicos como objetos digitales, mediante el encapsulamiento de los metadatos y los documentos en una misma estructura (por ejemplo, un fichero XML).
- Para documentos en fase semiactiva o inactiva almacenados en sistemas de ficheros, reproducción a este nivel del cuadro de clasificación de la organización.

En cuanto a la seguridad

- Control de accesos.
- Control de soportes.

En cuanto al aumento de documentos y los costes asociados

- Almacenamiento en capas (*tiers*) o jerárquico
  - En función del número de accesos a los documentos se emplearían tipos de discos distintos, estableciendo un nivel jerárquico de mayor a menor rendimiento y de menor a mayor espacio de almacenamiento. De esta forma los documentos menos accedidos se ubicarían en discos más lentos y grandes y, por tanto, más económicos.
  - El sistema en tier o niveles aseguraría asimismo el rendimiento necesario en función de las necesidades de acceso a los documentos.
- Sistemas RAID adecuados a la naturaleza de los datos (RAID-1+0 para documentos muy accedidos o críticos; RAID-5 o RAID-6, que son más económicos, para documentos menos accedidos, por ejemplo).
- Uso de técnicas de deduplicación en copias de seguridad a disco, con el objetivo de que el espacio necesario para el almacenamiento de las copias sea menor.
- Utilización de cintas magnéticas de gran capacidad para almacenar documentos en fase semiactiva (archivo central o intermedio), montando, por ejemplo, sistemas de ficheros en este tipo de soportes o empleándolos simplemente como sistema de backup o conservación permanente.
- Sistemas de archivado para reducir las licencias necesarias de copias de seguridad y permitir la utilización de sistemas de almacenamiento de gama inferior a los empleados para los documentos más accedidos.
  - En este sentido se dispondrían de métodos como el particionamiento de las bases de datos y el empleo de tablas de sólo lectura (ver medidas en relación a la obsolescencia del software), que reducen el volumen de las copias de seguridad y el tiempo necesario para realizarlas y permitirían emplear, si se considera oportuno, soportes de almacenamiento más económicos.

VI ANEXO 1. NORMAS LEGALES

1. Ley 16/1985, de 25 de junio, de Patrimonio Histórico Español
2. Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común
3. Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
4. 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 documentos administrativos en soporte distinto al original.
5. Ley 59/2003, de 19 de diciembre, de firma electrónica.
6. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
7. Instrucción de la Secretaría General Técnica de 10 de julio de 2007 sobre eliminación de documentos en el Ministerio del Interior.
8. Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público
9. RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
10. RD 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007.
11. RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
12. RD 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad dentro del ámbito de la Administración Electrónica.
13. Resolución de 11 de junio de 2011, de la Secretaría de Estado para la Función Pública, por el que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico.
14. Resolución de 11 de junio de 2011, de la Secretaría de Estado para la Función Pública, por el que se aprueba la Norma Técnica de Interoperabilidad de Expediente Electrónico.
15. RD 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso.
16. Resolución de 28 de junio de 2012, de la Secretaría de Estado para la Función Pública, por el que se aprueba la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.
17. Guía de adecuación al Esquema Nacional de Interoperabilidad.
18. Documento Electrónico - Guía de aplicación de la Norma Técnica de Interoperabilidad.
19. Expediente Electrónico - Guía de aplicación de la Norma Técnica de Interoperabilidad.
20. Política de Gestión de Documentos Electrónicos - Guía de aplicación de la Norma Técnica de Interoperabilidad.

VII ANEXO 2. BIBLIOGRAFÍA

Administración de documentos y archivos. Textos fundamentales. Coordinadora de Asociaciones de Archiveros. José Ramón Cruz Mundet (director). Madrid, 2011.

Archivística, archivo, documento de archivo… Necesidad de clarificar los conceptos. Francisco Fuster Ruiz. Anales de documentación, nº 2. Págs. 103-120. 1999.

Dark data is more important than big data. Big Data Debate. Francis Pedraza. 2013.

Diccionario de terminología archivística. Ministerio de Educación cultura y Deporte. Accesible en: http://www.mcu.es/archivos/MC/DTA/Diccionario.html

Digital Preservation Guidance Note 2. Selecting Storage Media for Long-Term Preservation. The National Archives. United Kingdom. 2008.

El documento electrónico: un enfoque archivístico. María de Hontanares Redondo Herranz. 2009.

El Glossari "comparat" d'arxivística. Ajuntament de Sant Boi de Llobregat. 2011.

Entender PREMIS. Priscilla Caplan. Library of the Congress. 2009. Traducción de Mª Luisa Martínez Conde, Ministerio de Cultura.

Establecimiento de Políticas y Mecanismos de Conservación de Documentos Electrónicos a Largo Plazo. Sociedad Informática del Gobierno Vasco. 2008.

Gestión de los documentos digitales: estrategias para su conservación. Jordi Serra Serra. En "El profesional de la información", 2001.

La conservación a largo plazo de documentos electrónicos: normativa ISO y esfuerzos nacionales e internacionales. 2009. Alejandro Delgado Gómez.

La Norma ISO 15489, un marc sistemàtic de bones pràctiques de gestió documental a les organitzacions. José Alberto Alonso, Montserrat García Alsina y M. Rosa Lloveras i Moreno. Revista Ítem, nº 7, págs. 41-70. 2007.

La seguretat i la preservació dels documents electrònics d'arxiu signats. Nacho Alamillo i Domingo. Revista Lligall nº 31, páginas 82 a 104. 2010.

Los Archivos Municipales y la Administración Electrónica 1988-2008. Actas de las XVII Jornadas de Archivos Municipales. Madrid. 2008.

Manual de Gestión de Archivos Administrativos. Diputación de Valladolid. Carlos Alcalde Martín-Calero. 2007.

Modelo de Gestión Documental del Gobierno Vasco. Departamento de Justicia y Administración Pública. Gobierno Vasco. 2010.

Reference model for an open archival information system (OAIS). Recommended practice. The Consultative Committee for Space Data Systems. 2012.

STORAGE CONCEPTS-Storing and Managing Digital Data. HDS Academy. Edited by Peter Manijak. Martin Stewart an Pavel Vild. 2012.

Ponencia nº 6

Tratamiento y gestión del correo electrónico como documento electrónico

Álvaro Reig González (Instituto Nacional de Administración Pública) y
Alejandro Millaruelo Gómez (Intervención General de la Administración del Estado)

Resumen de la ponencia:

Tratamiento y gestión del correo electrónico como documento electrónico

Álvaro Reig González (Instituto Nacional de Administración Pública) y
Alejandro Millaruelo Gómez (Intervención General de la Administración del Estado)
Ponencia nº 6

INTRODUCCIÓN

El término correo electrónico designa tanto un medio de comunicación y transmisión de información, como un sistema de mensajería que emplea medios electrónicos y hace uso de redes de comunicaciones, como los mensajes que se envían o reciben en ese sistema.

Los mensajes de correo electrónico se pueden categorizar como documento electrónico basándonos en las definiciones de documento y documento electrónico que hacen la ley 16/1985, de 25 de junio, de Patrimonio Histórico Español, el RD 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad dentro del ámbito de la administración electrónica, y el RD 1671/2009, de 16 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007.

Por otro lado, los mensajes de correo electrónico tienen unas características propias que los pueden diferenciar de otros documentos electrónicos, a saber: su uso privado y oficial y su uso interno o externo a la organización, el hecho de que su preservación no esté garantizada, su empleo como contenedor de otros documentos, su contenido informativo (que puede ser múltiple), la falta de garantía de autenticidad e integridad de los mensajes, los formatos propietarios en cuanto a su almacenamiento, el riesgo de que sea considerado un medio informal de comunicación y el uso de un lenguaje menos formalizado que en otro tipo de documentos, la existencia de múltiples destinatarios y su limitación de tamaño.

VISIÓN TÉCNICA DE UN SISTEMA DE CORREO ELECTRÓNICO

En cuanto a la arquitectura está formado por servidores de entrada o salida (Mail Transfer Agent o MTA), por clientes de correo (Mail User Agent o MUA) y el mensaje propiamente dicho.

En cuanto a protocolos estándar destacan SMTP (protocolo de envío que emplean los clientes de correo) y POP/IMAP (protocolo de recepción usado por los clientes de correo). Otros elementos a considerar son las listas de distribución, el buzón de correo electrónico y las cabeceras de correo electrónico.

EL CORREO ELECTRÓNICO EN EL MARCO LEGAL ESPAÑOL

El correo electrónico considerado como un medio de comunicación no está regulado específicamente por ninguna norma española. Existen sin embargo varias referencias a su uso, no siempre directas, en diversas normas: la Constitución, la Ley 30/1992 Régimen Jurídico de las administraciones públicas, la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, la Ley 11/2007 de acceso de los ciudadanos a los servicios públicos, el RD 1671/2009 por el que se desarrolla parcialmente la ley 11/2007 y el RD 3/2010 por el que se regula el Esquema Nacional de Seguridad.

EL CORREO ELECTRÓNICO Y SU CONSIDERACIÓN COMO DOCUMENTO DE ARCHIVO

Para asegurar la conservación a largo plazo de los correos electrónicos, garantizando la accesibilidad, confidencialidad, integridad y disponibilidad de los mismos es necesario contar con una estrategia de conservación.

Esta estrategia definirá qué mensajes deberán ser conservados a largo plazo (los que formen parte de expedientes, tengan un contenido informativo único o sean evidencia de las actividades de la organización), distinguirá tres grupos de correos (personales, oficiales a con-

servar a largo plazo, resto de correos oficiales) y establecerá el tratamiento a aplicar a cada uno de estos grupos, determinará el valor de los correos desde el momento de su creación o recepción e indicará los metadatos necesarios para asegurar su conservación, fijará los sistemas de firma electrónica y cifrado de datos necesarios para asegurar su integridad y autenticidad y, finalmente, establecerá los datos necesarios para la contextualización de los mensajes.

SUGERENCIAS EN EL ÁMBITO DEL MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

El otro aspecto que permitirá asegurar la conservación a largo plazo de los correos electrónicos es una política de gestión del correo electrónico, que se aplicaría desde el momento de la creación o recepción de los mismos.

Esta política tendrá en cuenta las implicaciones desde el punto de vista de la privacidad, la adaptación al ENI de los mensajes de correo electrónicos a conservar (en cuanto a metadatos, formatos normalizados, tratamiento de anexos y conversión de formato) y las implicaciones desde el punto de vista organizativo, como la posibilidad de automatización de determinados procesos como la captura de metadatos o el proceso de calificación, el procedimiento de firma aplicable y otro conjunto de normas como son las políticas de uso (privado u oficial), las recomendaciones de redacción de los mensajes (pie, cabecera, etc.), las normas para la redacción del campo asunto, tratamiento de temas (uno por mensaje), gestión de la bandeja de entrada, eliminación de mensajes, reenvío de mensajes, normas de seguridad, etc.

Por último se analizan algunas posibles soluciones técnicas para la selección de los mensajes, en función de sistemas que requieran o no intervención humana.

Ponencia nº 6

Tratamiento y gestión del correo electrónico como documento electrónico

Álvaro Reig González (Instituto Nacional de Administración Pública) y Alejandro Millaruelo Gómez (Intervención General de la Administración del Estado)

Índice de la Ponencia

ÍNDICE DE LA PONENCIA

I. INTRODUCCIÓN

Qué entendemos por correo electrónico

El término correo electrónico designa tanto un medio de comunicación y transmisión de información, como un sistema de mensajería que emplea medios electrónicos y hace uso de redes de comunicaciones, como los mensajes que se envían o reciben en ese sistema[1].

Como medio de comunicación es una herramienta indispensable para el trabajo del personal al servicio de las Administraciones públicas.

Como sistema de mensajería su uso está extendido en todos los organismos públicos, mediante aplicaciones de correo electrónico como Outlook. De hecho a día de hoy probablemente el conjunto de empleados públicos dispone de una cuenta de correo personal. Aunque no sea la aplicación que soporta el peso fundamental de las atribuciones que tiene encargadas cada organización, constituye en la mayoría de los casos una de las aplicaciones críticas cuya indisponibilidad tiene unas consecuencias más visibles en el trabajo diario.

Por último como mensaje se puede categorizar como documento electrónico.

Así la ley 16/1985, de 25 de junio, de Patrimonio Histórico Español, en su artículo 49.1 define **documento** como "toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos".

En el anexo del RD 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad dentro del ámbito de la administración electrónica, se define **documento electrónico** como aquella "información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado".

Asimismo en el RD 1671/2009, de 16 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, en su artículo 41, establece las características que deberán cumplir los documentos electrónicos para ser considerados válidos:

- Contener información de cualquier naturaleza.
- Estar archivada la información en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.
- Disponer de los datos de identificación que permitan su individualización, sin perjuicio de su posible incorporación a un expediente electrónico.

La norma ISO 15489:1, por su lado, define documento como "cualquier información creada, recibida y mantenida como evidencia e información por una organización o persona, en la consecución de sus obligaciones normativas o en las transacciones comerciales".

Así pues, basándonos en estas definiciones podríamos considerar que los correos electrónicos, entendidos como mensajes, son documentos electrónicos.

[1] *El correu electrònic: un problema a resoldre*, Teresa Banús Giménez y Marta Cortez Longares, revista Lligall nº 25, 2006.

Otras características de los correos electrónicos considerados como documentos, derivadas del uso del correo electrónico entendido como sistema de comunicación

1. Uso privado y oficial

Existe un uso privado combinado con un uso público u oficial: los sistemas de correo almacenan indistintamente correos de índole privada junto con otros que son consecuencia de las actividades de los empleados públicos en el ejercicio de sus funciones.

2. Doble función del correo

Si nos ceñimos exclusivamente a su uso oficial, independientemente del asunto que traten, en función de los emisores o destinatarios de los mensajes de correo electrónico, podríamos distinguir entre un uso interno o externo a la organización. En el primero el correo electrónico tiene como origen y destino cuentas de correo de la misma organización; en el segundo pueden ser de la misma organización y de otros organismos públicos, o de ciudadanos.

3. La preservación no está garantizada por el propio sistema

Salvo que medien sistemas de archivado, los correos pueden ser eliminados o conservados por el emisor una vez enviados y, por supuesto, conservados o eliminados también por el receptor o receptores.

4. El correo como contenedor de otros documentos

Los mensajes de correo electrónico pueden emplearse como soporte de transmisión de otros documentos o anexos, cuyo tratamiento merecería un estudio aparte.

5. Su contenido informativo puede ser múltiple

En cuanto al contenido, éste puede tener un uso informativamente complejo, al tratar varios asuntos en un mismo mensaje.

6. No está garantizada la autenticidad e integridad de los mensajes

Por sí mismas las aplicaciones de correo no garantizan la autenticidad e integridad de los mensajes de correo electrónico, salvo que se empleen firma electrónica y/o cifrado de datos.

7. La conservación depende de formatos propietarios

Aunque el transporte, el acceso a los buzones y las direcciones siguen protocolos estándar (SMTP para el primero, POP3 e IMAP para el segundo y X.400 para el tercero, por ejemplo), el almacenamiento de los mensajes de correo electrónico se basa en formatos propietarios que, con el paso del tiempo, pueden quedar obsoletos.

8. Las aplicaciones de correo constituyen por sí mismas un SGDE

Las aplicaciones de correo se pueden considerar como Sistemas de Gestión de Documentos Electrónicos específicos, con lo que su relación e integración con los sistemas propios de cada organización no es automática.

9. El correo se considera un medio informal de comunicación

Uno de los riesgos en cuanto a su conservación es que, dadas sus características (valor primario efímero, uso privado combinado con un uso oficial, dificultad para garantizar la autenticidad e integridad de los mensajes, etc.) las propias organizaciones consideran los correos electrónicos como un subconjunto documental menos valioso que otros tipos de documentos electrónicos.

10. Uso de un lenguaje informal

La inmediatez que proporcionan los sistemas de correo electrónico favorece el uso de un lenguaje menos formal que en otro tipo de documentos.

11. Destinatarios múltiples

Una de sus características más notables es que un mensaje puede enviarse a más de un destinatario, lo que puede generar múltiples respuestas. El último mensaje de una serie de este tipo (con un asunto común) constituye el resumen de todos los mensajes enviados.

12. Limitación de tamaño

Las aplicaciones de correo electrónico suelen limitar el tamaño máximo del mensaje de correo o el tamaño de los anexos. No es un medio que sirva para transmitir documentos de cualquier tamaño.

II. VISIÓN TÉCNICA DE UN SISTEMA DE CORREO ELECTRÓNICO.

Dada la dependencia de los mensajes de correo electrónico de las aplicaciones y sistemas de correo, hemos considerado necesario hacer un repaso de las características generales de estos sistemas.

Arquitectura

Si bien la arquitectura y funcionamiento del correo electrónico es técnicamente complejo, se va a ofrecer una visión simplificada con objeto de alcanzar un público más amplio.

En el proceso de envío y recepción de correos electrónicos intervienen varios elementos, entre los que destacan los siguientes:

- Servidores de entrada o salida (Mail Transfer Agent, MTA). Son servicios que se encargan de enviar o recibir los correos para sus usuarios. Cada organización suele tener al menos uno de entrada y otro de salida

- Clientes de correo (Mail User Agent, MUA). Software con el que interactúa el usuario final. Se conecta con los servidores MTA de la organización del usuario para recuperar y enviar correos. Pueden ser aplicaciones de escritorio (Microsoft Outlook, Mozilla Thunderbird), aplicaciones web (Gmail, Yahoo) o aplicaciones móviles (Gmail para Android, Gmail para iPhone).

- Correo electrónico. El mensaje propiamente dicho, con toda la información necesaria para asegurar el envío.

Protocolos

Los elementos descritos anteriormente utilizan varios protocolos para transmitir datos entre ellos. Destacan los siguientes:

- SMTP: Protocolo de envío de correo. Utilizado por

  - Los clientes de correo (MUA) para enviar un correo electrónico al servidor de correo (MTA) de su organización.

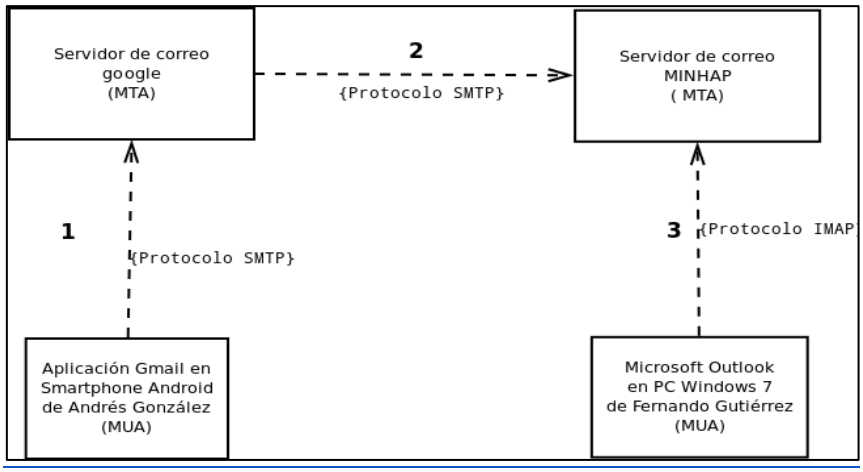
  - El servidor de correo de la organización del emisor (MTA) para hacer llegar el correo electrónico al servidor de correo de la organización del receptor (MTA).

- POP / IMAP[2]. Protocolos de recepción de correo. Utilizados por un cliente de correo (MUA) para visualizar sus mensajes de correo electrónico, almacenados en el servidor de correo de su organización (MTA).

Ejemplo de envío de correo

Con objeto de clarificar los conceptos expuestos anteriormente, se va a realizar un diagrama explicativo de un caso de uso típico: un usuario envía un correo desde su correo electrónico personal (andres.gonzalez@gmail.com) al correo profesional de su compañero (fernando.gutierrez@minhap.es) utilizadando un smartphone:

[2] El servidor de correo electrónico Microsoft Exchange puede utilizar protocolos diferentes en función de la versión.



Los pasos son:

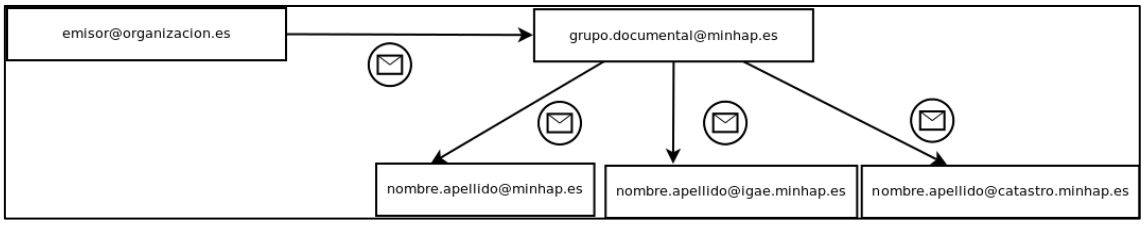
1. Andrés González redacta un correo electrónico en su smartphone utilizando Gmail y hace clic en “Enviar”. La aplicación Gmail (MUA) se comunica con el servidor de correo del emisor (en este caso, el servidor de correo de Google, MTA) utilizando el protocolo SMTP para hacerle llegar el correo electrónico.
2. A su vez, el servidor de correo electrónico del emisor utiliza el protocolo SMTP para hacerle llegar el correo electrónico al servidor de correo electrónico del receptor, en este caso el servidor del correo electrónico del Ministerio de Hacienda y Administraciones Públicas.
3. Por último, Fernando Gutiérrez abre su cliente de correo Microsoft Outlook (MTA), que se conecta al servidor de correo de la organización utilizando el protocolo IMAP. Al encontrar nuevo correo electrónico, éste es descargado a Microsoft Outlook para que su destinatario pueda leerlo.

Otros elementos a considerar

De cara al estudio de la conservación documental hay que tener en cuenta otros elementos:

1. Lista de distribución

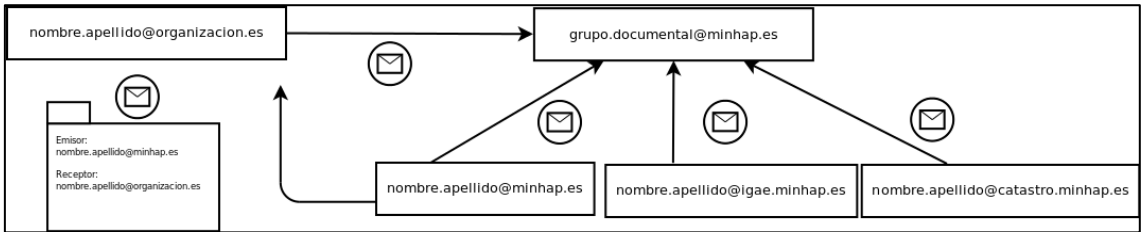
Dirección de correo electrónico que reenvía todos los correos recibidos a uno o más usuarios. De este modo, un grupo de trabajo puede proporcionar a terceros una única dirección y tener la garantía de que todos los miembros del equipo de trabajo recibirán todos los correos electrónicos. Sin embargo, si alguno de los miembros responde a un correo electrónico recibido a través de la lista se utilizará su dirección personal como remitente.



2. Buzón de correo electrónico

Dirección de correo electrónico compartida por varios usuarios. Existen dos diferencias principales con una lista de distribución.

- Los usuarios deben acceder al buzón para leer el correo electrónico, mientras que la lista de distribución reenviar automáticamente los mensajes recibidos a la cuenta personal de cada usuario.
- Los usuarios también pueden enviar correos utilizando la dirección del buzón como remitente



3. Cabeceras de correo electrónico

Un mensaje de correo electrónico consta de una serie de cabeceras (metadatos) necesarias para el buen funcionamiento del sistema. Algunas de las más conocidas son:

- Dirección del emisor (from)
- Dirección del destinatario (sender)
- Asunto (subject)
- Direcciones de los usuarios en copia (cc)
- Direcciones de los usuarios en copia oculta (bcc)

Sin embargo, existen muchas cabeceras que sería necesario tener en cuenta a la hora de definir un esquema de conservación del correo electrónico como soporte documental.

III. EL CORREO ELECTRÓNICO EN EL MARCO LEGAL ESPAÑOL

El correo electrónico y la ausencia de regulación específica

El correo electrónico considerado como un medio de comunicación no está regulado específicamente por ninguna norma española. Existen sin embargo varias referencias a su uso, no siempre directas, en diversas normas que iremos detallando a continuación.

Constitución española

En su artículo 18, apartado 3, nuestra constitución establece que "se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial." Esta protección se reconoce independientemente del contenido de la comunicación, e incluye la identidad de los interlocutores[3]. La interceptación de las comunicaciones por un tercero ajeno a ellas es un delito tipificado en el Código Penal.

Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las administraciones públicas y de procedimiento administrativo común

La ley 30/1992 establece en su artículo 19 que "las comunicaciones entre órganos podrán efectuarse por cualquier medio que asegure la constancia de su recepción".

En el artículo 38.1 se indica que "los órganos administrativos llevarán un registro general en el que se hará el correspondiente asiento de todo escrito o comunicación que sea presentado o que se reciba en cualquier unidad administrativa propia. También se anotarán en el mismo, la salida de los escritos y comunicaciones oficiales dirigidas a otros órganos o particulares." Este registro además deberá "instalarse en soporte informático" (artículo 38.3).

[3] Constitución española. Sinopsis artículo 18. Ascensión Elvira Perales y Ángeles González Escudero. Congreso de los Diputados. 2011.

Por otro lado en el artículo 45.5 se señala que "los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por ésta u otras leyes".

Por último se establece que las resoluciones y actos administrativos se notificarán a los interesados "por cualquier medio que permita tener constancia de la recepción por el interesado o su representante, así como de la fecha, la identidad y el contenido del acto notificado" (artículo 58.1 y 59.1).

Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y RD 1707/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999

La Ley Orgánica establece en su artículo 2 que se aplicará "a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado", definiendo en su artículo 3 datos de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificables".

En este sentido una dirección de correo electrónico personalizada se considerará un dato de carácter personal[4]. No hay que confundir este hecho con el uso privado del correo: al tratarse de una cuenta de correo corporativo serán las normas de uso del organismo las que permitirán o no su empleo con fines particulares.

Al contrario, una cuenta genérica no se considerará un dato de carácter personal.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico y Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información

En estas normas se regula el uso del correo electrónico por parte de las empresas con fines de comunicación comercial y de contratación por vía electrónica.

Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos

En su artículo 6 "se reconoce a los ciudadanos el derecho a relacionarse con las Administraciones Publicas utilizando medios electrónicos (…)", a seleccionar de entre los "que en cada momento se encuentren disponibles" el que van a emplear, y a elegir "las aplicaciones o sistemas para relacionarse con las Administraciones Públicas siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos".

En cuanto a las comunicaciones electrónicas el artículo 27.2 establece que "las comunicaciones a través de medios electrónicos serán válidas siempre que exista constancia de la transmisión y recepción, de sus fechas, del contenido íntegro de las comunicaciones y se identifique fidedignamente al remitente y al destinatario de las mismas".

Finalmente en el anexo de la ley se define medio electrónico como el "mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras".

RD 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos

En su artículo 27, que trata sobre la creación de registros electrónicos, este RD señala que "en ningún caso tendrán la consideración de registro electrónico los buzones de correo electrónico corporativo asignado a los empleados públicos o a las distintas unidades u órganos".

[4] Manual de buen uso del correo electrónico. Guía para las personas trabajadoras para la protección de la privacidad en el uso del correo electrónico. Autoritat Catalana de Protecció de Dades. Generalitat de Catalunya. 2013.

Por otro lado en su artículo 35.1 establece que “los órganos y organismos públicos de la Administración General del Estado habilitarán sistemas de notificación electrónica (…)”, basados en los siguientes medios electrónicos, a saber: una dirección electrónica, “sistemas de correo electrónico con acuse de recibo que deje constancia de la recepción”, “comparecencia electrónica en la sede” y “otros medios de notificación electrónica que puedan establecerse, siempre que quede constancia de la recepción por el interesado en el plazo”.

En cuanto a la utilización de sistemas de correo electrónico como medio de notificación el artículo 39 indica que “se podrá acordar la práctica de notificaciones en las direcciones de correo electrónico que los ciudadanos elijan siempre que se genere automáticamente y con independencia de la voluntad del destinatario un acuse de recibo que deje constancia de su recepción y que se origine en el momento del acceso al contenido de la notificación”.

RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

Este RD hace una mención específica al correo electrónico, en la medida de protección de los servicios 5.8.1 (protección del correo electrónico):

El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

a) La información distribuida por medio de correo electrónico, se protegerá, tanto en el cuerpo de los mensajes, como en los anexos.

b) Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.

c) Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:

   1. Correo no solicitado, en su expresión inglesa "spam".
   2. Programas dañinos, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.
   3. Código móvil de tipo "applet".

d) Se establecerán normas de uso del correo electrónico por parte del personal determinado. estas normas de uso contendrán:

   1. Limitaciones al uso como soporte de comunicaciones privadas.
   2. Actividades de concienciación y formación relativas al uso del correo electrónico.

IV. EL CORREO ELECTRÓNICO Y SU CONSIDERACIÓN COMO DOCUMENTO DE ARCHIVO

La conservación de los mensajes de correo electrónico

Como documentos y evidencia de las funciones ejercidas por las Administraciones públicas los correos electrónicos deberían conservarse, no obstante las particularidades que vimos en la introducción y que les caracterizan.

Por otro lado, el proceso de conservación, para garantizar la accesibilidad, confidencialidad, integridad y disponibilidad de los documentos debería aplicarse a todo el ciclo de vida de los correos electrónicos. Esto supondrá en primer término que existan unas normas claras, conocidas por todos los empleados de cada organización, acerca de la creación, tratamiento, gestión, conservación y eliminación de los correos electrónicos y, en segundo lugar, que se haya definido una estrategia de conservación que contemple los actores involucrados, los principios de conservación, los requisitos, el archivo electrónico donde se almacenarán los correos, los riesgos y los correspondientes planes de contingencia y acciones correctoras, los métodos, medidas técnicas y procedimientos que aseguren la conservación, los formatos admitidos y las herramientas de las que dispone el organismo.

Así pues, en este capítulo trataremos la estrategia de conservación y en el siguiente abordaremos la necesidad de contar con una política de gestión de los correos electrónicos y plantearemos, en este sentido, una serie de sugerencias.

Qué mensajes deberíamos conservar a largo plazo

Como documentos los correos electrónicos disponen de un valor primario, que responderá al motivo por el que fueron redactados o elaborados. Pero este valor primario, a diferencia de lo que pasa con, por ejemplo, los documentos públicos administrativos, es en muchos casos **efímero**.

Una de las preguntas esenciales en relación al correo electrónico en cuanto mensaje o documento, es acerca de su conservación. ¿Deben conservarse todos los correos enviados o recibidos por una organización en el ejercicio de sus funciones, más allá de su valor primario?

En este sentido no debemos olvidar que la ley 16/1985 de Patrimonio Histórico Español, en su artículo 49.2, establece que "forman parte del Patrimonio Documental los documentos de cualquier época generados, conservados o reunidos en el ejercicio de su función por cualquier organismo o entidad de carácter público (...)", por lo que toda la documentación electrónica generada o recibida por cualquier organismo de la Administración pública formaría parte del Patrimonio Documental, sin perjuicio del momento de su generación.

Además, en su artículo 55.1, esta ley señala que "la exclusión o eliminación de bienes del Patrimonio Documental (...) deberá ser autorizada por la Administración competente". En el artículo 55.2 hace hincapié en que "en ningún caso se podrán destruir tales documentos en tanto subsista su valor probatorio de derechos y obligaciones de las personas o los entes públicos".

Por todo esto parece que la conclusión es que se deberían conservar a largo plazo, al menos, los correos electrónicos que sean producto de las competencias ejercidas por el organismo. En este conjunto podríamos incluir:

- los correos recibidos que forman parte de expedientes en curso;
- los que siendo generados por la misma organización forman parte también de un expediente o procedimiento;
- los que tienen un contenido informativo único;
- y, en general, los que son una evidencia de las funciones y actividades propias del organismo.

Dos fases de conservación de los correos electrónicos

Aunque el valor primario de muchos correos electrónicos sea efímero o no cumplan los requisitos que hemos visto en el apartado anterior, su valor puede ser importante durante un plazo determinado de tiempo, por lo que deberán conservarse igualmente.

Atendiendo al ciclo de vida de los documentos (fases activa, semiactiva e inactiva) a su valor (primario o secundario) y a su uso (privado u oficial), cabría dividir el conjunto de los correos electrónicos de una organización, en un momento dado, en tres grupos:

- Correos personales.
- Correos oficiales que deban conservarse a largo plazo.
- Resto de correos oficiales.

En cuanto al primer grupo, una buena práctica consistiría en la eliminación de los correos personales de la bandeja de entrada una vez leídos, para evitar el uso de espacio de almacenamiento corporativo o sobrecargar los sistemas de salvaguarda.

En cuanto al resto de correos se podría hablar de dos fases de conservación:

- Una primera fase en la que los correos electrónicos se conservarían durante un determinado plazo de tiempo, atendiendo a su valor primario inmediato. Como método de conservación deberían emplearse métodos de backup para los buzones de correo personales, con una retención acorde con el plazo fijado de utilidad. Si fuera necesario podrían establecerse retenciones distintas si se considerase que determi-

nados buzones almacenan correos cuyo valor es mayor. Durante esta fase sería recomendable, además, contar con sistemas de archivado que permitieran conservar los correos electrónicos independientemente de los buzones, con una retención mayor que la de los backups. Estos sistemas de archivado permiten almacenar los correos en sistemas de almacenamiento con prestaciones menores que los sistemas que emplean los buzones, resultando por tanto más económicos, dado el volumen de datos que son capaces de tratar. Además suelen ser sistemas que almacenan los anexos una sola vez, independientemente del número de mensajes. Una vez transcurrido el tiempo determinado de conservación los correos serían eliminados.

- Una segunda fase que, en realidad, es paralela a la anterior, no secuencial, en la que los correos electrónicos que deban conservarse a largo plazo, aquellos que cuentan con un valor primario importante por ser parte de expedientes o trámites administrativos, por tener un contenido informativo único o por ser evidencia de las actividades del organismo, pasarían a formar parte del sistema de gestión de documentos electrónicos de archivo de la organización. Así pues, estos correos se almacenarían en dos entornos distintos, uno el propio sistema de correo electrónico y otro el SGDEA. Decimos que es una fase que transcurre en paralelo porque la captura de estos correos debería hacerse desde el momento de su creación y envío, con objeto de garantizar su conservación a largo plazo. Por otro lado, sería necesario realizar un cambio de formato para asegurar esta conservación, y se les debería aplicar una serie de requisitos para que fuesen considerados documentos electrónicos válidos (firma electrónica, cifrado, etc.).

Determinación del valor de los correos electrónicos.

Con objeto de asegurar la conservación a largo plazo de los mensajes de correo electrónico, es necesario determinar su valor, a ser posible, desde el momento de su creación. Como hemos visto en los apartados anteriores, existen una serie de criterios que se pueden adoptar para calificar estos documentos (formar parte de expedientes, disponer de un valor informativo único y ser evidencia de funciones del organismo).

El uso de metadatos adecuados facilitará este proceso de calificación, por lo que los correos electrónicos no deberían dejarse de lado en el momento de definir los metadatos necesarios para la gestión documental. Algunos de los metadatos podrán obtenerse de la cabecera del mensaje, pero otros podrán procederán de otras fuentes, por ejemplo, los propios servidores de correo. Sería recomendable minimizar la intervención manual en este proceso, aunque probablemente será imposible evitarla del todo.

Cómo garantizar la integridad, la confidencialidad y la autenticidad de los mensajes de correo electrónico

Para garantizar la integridad, la confidencialidad y la autenticidad de los mensajes de correo electrónico, especialmente de los que forman el grupo que se conservará a largo plazo, disponemos de los mecanismos de firma electrónica y el cifrado de los datos.

Los correos electrónicos a los que no se les apliquen estas técnicas deberían excluirse de la conservación a largo plazo, puesto que no sería posible garantizar su autenticidad ni su integridad.

Contextualización de los mensajes de correo electrónico

Es importante, de cara a su conservación a largo plazo, no perder el contexto en que se crean o reciben los mensajes de correo electrónico.

Así, los correos que forman una cadena secuencial de mensajes deberían conservarse íntegramente, con lo que el último de la cadena permitiría la conservación de todos ellos. Los anexos y sus modificaciones deberían conservarse asimismo, como evidencia.

También es recomendable asociar las direcciones de correo electrónico personalizadas con los datos identificativos de las personas (nombre, apellidos y cargo dentro de la organización).

Por supuesto los correos electrónicos que formen parte de expedientes deberían contener las indicaciones necesarias para que puedan ser asociados a ellos o a los trámites adminis-

trativos correspondientes. Una de las formas más simples de asociación es incluir estos correos electrónicos como parte de los expedientes.

Otro método para asegurar la contextualización sería emplear el registro electrónico con determinados correos.

V. SUGERENCIAS EN EL ÁMBITO DEL MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

Necesidad de una política de gestión del correo electrónico

Con objeto de asegurar la conservación a largo plazo de los correos electrónicos, además de contar con una estrategia de conservación, cuya definición hemos visto en el capítulo anterior, sería necesario disponer de una **política de gestión del correo electrónico** a nivel de la organización, en la que se plasmaría de forma concreta esa misma estrategia.

Esta política recogería el conjunto de buenas prácticas asociadas al uso del correo electrónico en sus tres acepciones: como medio de comunicación, como aplicación de mensajería y como documento electrónico.

Especialmente esta política debería contemplar especialmente la creación o recepción de correos electrónicos y su gestión posterior, puesto que sólo entendiendo el proceso de conservación como un proceso que abarca todo el ciclo de vida de los documentos, sentaremos las bases necesarias para su conservación a largo plazo.

Esta política tendría en cuenta, además, como mínimo, implicaciones legales, de seguridad, técnicas y organizativas involucradas en el proceso de gestión y conservación de los mensajes de correo electrónico.

Implicaciones desde el punto de vista de la privacidad y los datos de carácter personal

Dado que todo correo electrónico puede acabar almacenado en el sistema de gestión documental de la organización, sería muy conveniente elaborar un plan de comunicación para informar a los usuarios de tal circunstancia, y que sean conscientes de la necesidad de eliminación de los correos de índole personal de la bandeja de entrada en cuanto sea posible.

Además, sería necesario analizar el impacto de la normativa vigente en el uso de las cuentas de correo electrónico corporativas (Ley Orgánica de Protección de Datos de Carácter Personal y sentencias del Tribunal Constitucional, especialmente el recurso de amparo nº 2907/2011 de 7 de octubre de 2013), puesto que son instrumentos de la organización puestos al servicio de los empleados con objeto de facilitar las funciones encomendadas.

Implicaciones desde el punto de vista del Esquema Nacional de Seguridad

Siguiendo las recomendaciones que hace específicamente el Esquema Nacional de Seguridad se determinarían las medidas de protección adecuadas para la información contenida en los mensajes y para el establecimiento de conexiones seguras, incluyendo asimismo aquellas dirigidas a reducir el riesgo ante correos no deseados, programas dañinos y otras amenazas similares.

El ENS recomienda también limitar el uso privado del correo corporativo.

Implicaciones desde el punto de vista del Esquema Nacional de Interoperabilidad

Como documentos electrónicos integrados en el sistema de gestión de documentos electrónicos de archivo de la organización, los mensajes de correo que deban conservarse a largo plazo tendrían que ajustarse al Esquema Nacional de Interoperabilidad y, en especial, a la NTI de Documento Electrónico.

En este sentido algunos de los aspectos a tener en cuenta serían los siguientes:

- Metadatos.
- Formatos normalizados.
- Tratamiento de los anexos.
- Conversión de formatos.

En cuanto a los metadatos:

- En relación a los metadatos obligatorios, cabría definir, por ejemplo, en cuanto a tipo documental los de "correo electrónico" y "anexo de correo".
- En cuanto al metadato mínimo obligatorio "estado de elaboración" se indicaría el valor "copia electrónica auténtica con cambio de formato".

En cuanto a los formatos normalizados:

- Se seguiría lo dispuesto en la NTI de Catálogo de Estándares.
- Se tendrían en cuenta asimismo los formatos de los anexos, haciendo hincapié en la normalización de los mismos.

En cuanto al tratamiento de los anexos:

- Cada archivo adjunto debería ser tratado como un documento electrónico, lo que plantea el problema de cómo asociarlos a los mensajes de correo electrónicos. En este sentido habría que definir el procedimiento de asociación.
- Se establecerían normas acerca de la conveniencia de conservación de los anexos modificados sucesivamente (por ejemplo, en una cadena de mensajes).

En cuanto a la conversión de los formatos:

- Se seguiría lo dispuesto en la NTI de Procedimientos de Copiado Auténtico y de Conversión entre documentos electrónicos.
- Los correos seleccionados para su conservación a largo plazo deberían ajustarse a las recomendaciones acerca de la copia auténtica con cambio de formato.
- Habría que tener en cuenta asimismo los anexos y la posibilidad de realizar una copia auténtica con cambio de formato.

Implicaciones desde el punto de vista organizativo

Algunas implicaciones desde el punto de vista organizativo tienen que ver con el grado de automatización de los procesos que asegurarán la conservación a largo plazo de determinados correos electrónicos.

Así, por ejemplo:

- Automatización de los metadatos (qué metadatos podrán extraerse de la cabecera de los mensajes u obtenerse de los propios servidores de correo).
- Mecanización del proceso de calificación (mediante el uso de claves concertadas en el campo asunto, por ejemplo, basándose en determinados contenidos de los mensajes, etc.).

Si estos procesos no pueden ser completamente automatizados debería contarse con la intervención de personas especializadas en estas tareas.

Otra de las implicaciones a este nivel deriva del proceso de firma electrónica y las responsabilidades consiguientes.

Un tercer grupo de implicaciones a nivel organizativo se relacionan con políticas de uso (privado u oficial), recomendaciones de redacción de los mensajes (pie, cabecera, etc.), normas para la redacción del campo asunto, tratamiento de temas (uno por mensaje), gestión de la bandeja de entrada, eliminación de mensajes, reenvío de mensajes, etc.

Posibles soluciones desde el punto de vista técnico a la selección de los mensajes de correo electrónico que deban conservarse a largo plazo

A continuación se plantean una serie de posibles soluciones técnicas para el proceso de selección de los mensajes de correo electrónico.

a. Sistemas que no requieran la intervención del usuario

Funcionamiento a través del indexado de correos electrónicos para seleccionar, en función de parámetros especificados y/o sistemas de inteligencia artificial, aquellos que deben ser guardados.

A pesar de su teórica validez jurídica[5], podría descartarse por la dificultad de vencer la resistencia de los usuarios a la hora de ponerla en práctica, además de la complejidad técnica del software necesario y su elevado coste.

b. Sistemas que requieran la intervención del usuario

En este tipo de sistemas, el usuario selecciona los correos que considera relevantes y los envía de manera manual para su procesado. Al contar con la participación del usuario éste puede especificar los metadatos, aumentando la precisión de la categorización.

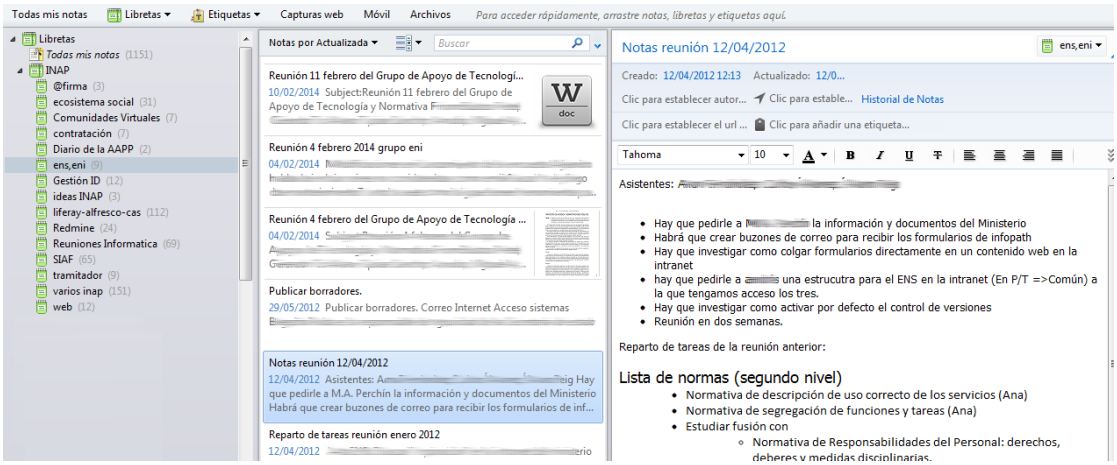
Aplicaciones integradas con el cliente de correo electrónico

Desarrollo de extensiones para los clientes de correo electrónico seleccionado, permitiendo al usuario rellenar un formulario con metadatos antes de enviar el correo electrónico para su procesado.

A la hora de realizar el envío físicamente, se proponen dos posibles soluciones mostrando dos ejemplos de aplicaciones con un comportamiento parecido.

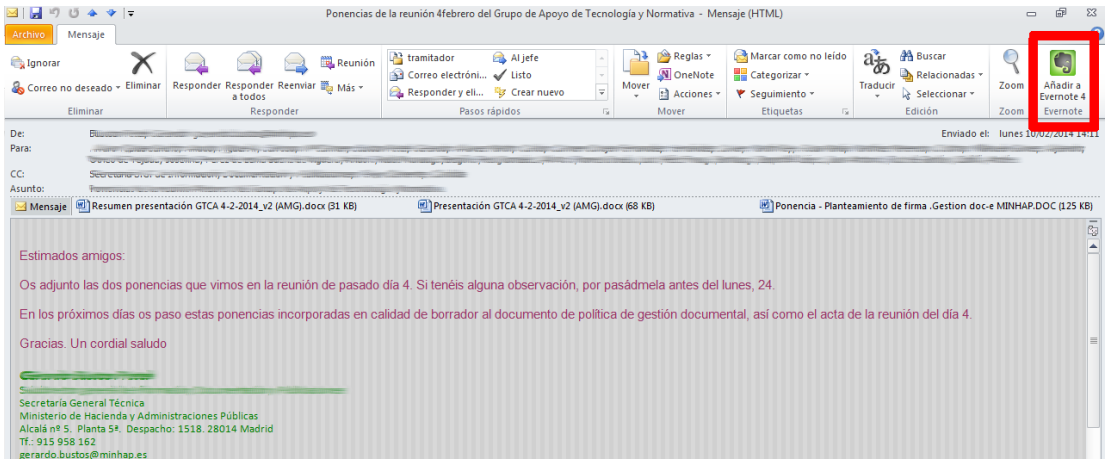
Aplicaciones integradas con el cliente de correo electrónico: Evernote

Evernote es una aplicación muy utilizada para almacenar notas y contenidos procedentes de diversas fuentes, organizando las “notas” en “libretas temáticas”:

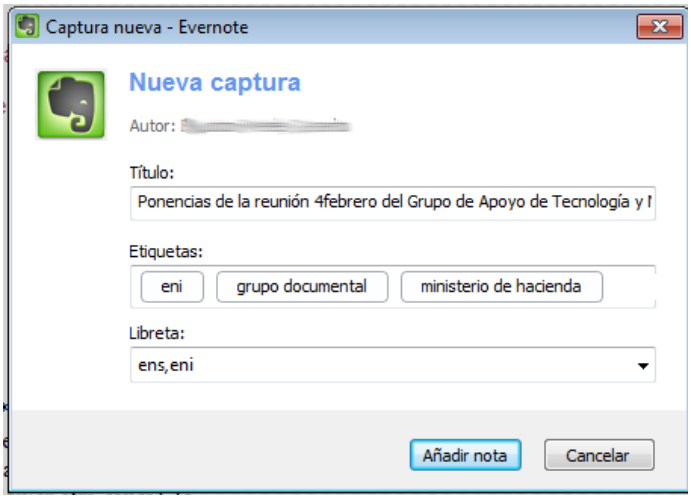


Incluye varias extensiones que facilitan la captura de notas. Entre ellas se encuentra el cliente para Microsoft Outlook. De este modo, una vez abierto un correo se puede capturar con facilidad, incorporándose a la libreta seleccionada, con los metadatos introducidos.

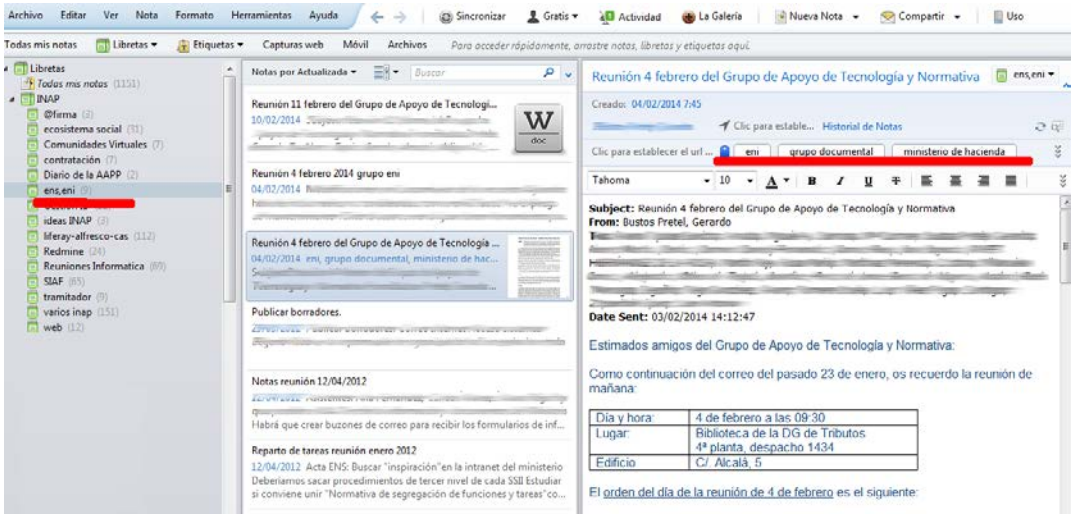
Tras pinchar en el botón se categoriza la nota:



[5] Sentencia del Tribunal Constitucional de 7 de octubre de 2013 (recurso de amparo nº2907/2011)



Finalmente, el correo electrónico queda almacenado:



Ventajas:

- Facilidad de uso, derivada de su integración con el cliente de correo corporativo.
- Posibilidad de desarrollar una pantalla de captura de metadatos sofisticada, incluso alimentándose de información del Tramitador ENI.

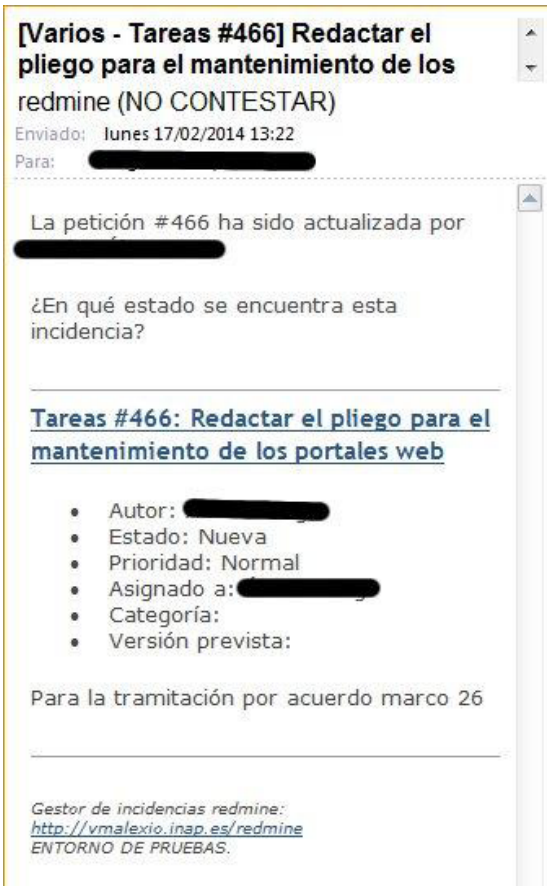
Inconvenientes:

- Dificultad de desarrollar aplicaciones para una pluralidad de clientes de correo electrónico / sistemas operativos.
- Incertidumbre sobre el software de uso obligatorio que se pueda imponer.

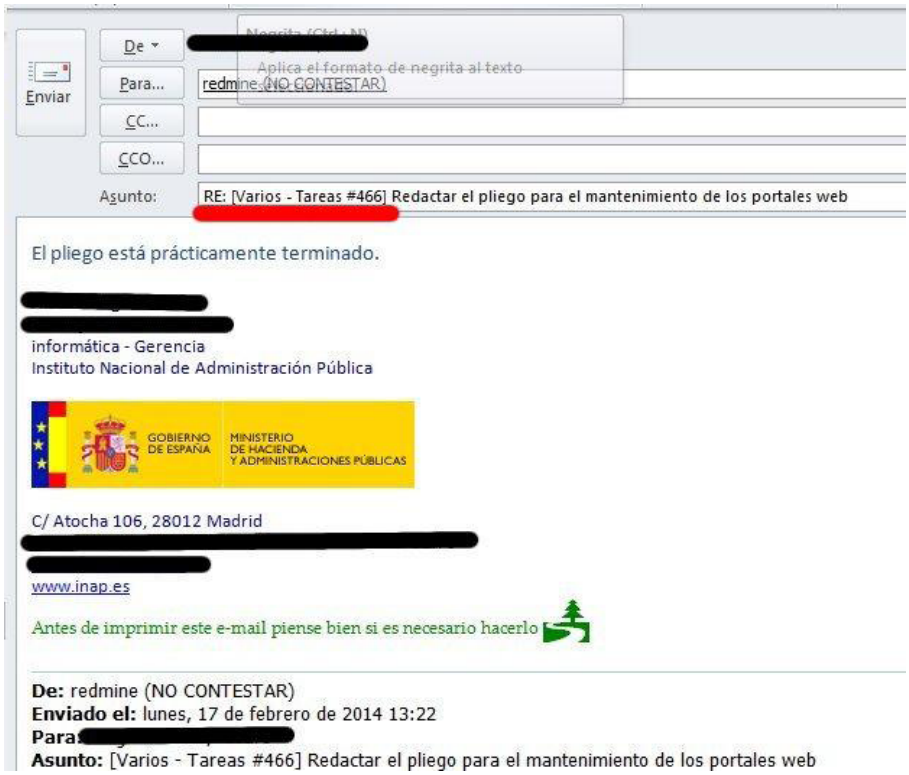
Aplicaciones con acceso a un buzón de correo electrónico dedicado: Redmine

Redmine es una aplicación web de gestión de peticiones, que facilita la gestión de proyectos o la tramitación de incidencias. Cada petición almacena todas las interacciones alrededor de un problema concreto:

Una de las funcionalidades de Redmine es el envío de correos electrónicos para notificar sobre cualquier cambio en una petición:



Así pues, es posible contestar al correo electrónico y el texto introducido será incorporado a la propia incidencia:



Ventajas:

- Más sencillo y barato de desarrollar. Basta con un algoritmo que escanee un buzón compartido y añada los documentos electrónicos.
- Menores posibilidades de generar incidencias y molestias a los usuarios.

Inconvenientes:

- No se dispone de la posibilidad de rellenar metadatos con antelación.
- Menos amigable para el usuario final, ya que si quiere introducir valores para los metadatos deberá teclearlos en el asunto o cuerpo del correo.

Conclusión

El enfoque más realista parece el desarrollo de una aplicación con acceso a un buzón de correo electrónico. De este modo, cuando un usuario deseara guardar como documento ENI un correo electrónico debería reenviarlo a una dirección del estilo documentos_eni@minhap.es. Posteriormente, un proceso escanearía y procesaría dichos correos.

VI Anexo 1. Normas legales

4. Ley 16/1985, de 25 de junio, de Patrimonio Histórico Español
5. Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común
6. Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
7. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
8. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
9. RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
10. Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información
11. RD 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007.
12. RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
13. Resolución de 9 de junio de 2011, de la Secretaría de Estado para la Función Pública, por el que se aprueba la Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos.
14. Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por el que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico.

VII Anexo 2. Bibliografía

Constitución española. Sinopsis artículo 18. Ascensión Elvira Perales y Ángeles González Escudero. Congreso de los Diputados. 2011.

Curating E-Mails: A life-cycle approach to the management and preservation of e-mail messages. DCC, Digital Curation Manual. Maureen Pennock. 2006.

El correu electrònic: un problema a resoldre. Teresa Banús Giménez y Marta Cortés Longares. Revista Lligall nº 25. 2006.

Email management. Electronic Records Management Guidelines. Minessota State Archives. 2012.

La gestió i la conservació de la documentació electrònica de les empreses. Arxiu Nacional d'Andorra. Govern d'Andorra. 2012.

Manual de buen uso del correo electrónico. Guía de las personas trabajadoras para la protección de la privacidad en el uso del correo electrónico. Autoritat Catalana de Protecció de Dades. Generalitat de Catalunya. 2013.

Propuesta de recomendaciones para la gestión y conservación del correo electrónico en las universidades españolas. Grupo de Trabajo de Documentos Electrónicos de la Conferencia de Archiveros de Universidades Españolas. 2010.

RFC 5322 http://tools.ietf.org/html/rfc5322

RFC 2045 - 2049 http://tools.ietf.org/html/rfc2045

Ponencia nº 7

Proceso de transferencia de documentos electrónicos

Cristina Martínez Merencio
(División de Sistemas de Información y Comunicaciones.
Secretaría de Estado de Administraciones Públicas)

Ponencia nº 7

Proceso de transferencia de documentos electrónicos

Cristina Martínez Merencio
(División de Sistemas de Información y Comunicaciones. Secretaría de Estado de Administraciones Públicas)

I TRANSFERENCIA COMO PROCESO BÁSICO DE GESTIÓN DOCUMENTAL

La Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos identifica los procesos mínimos de gestión de documentos electrónicos que deben incluirse en cualquier organización, estando entre ellos la transferencia de documentos entre repositorios.

Concepto de transferencia

Un aspecto clave en el concepto de transferencia es el de la responsabilidad de la custodia. La guía de aplicación de la NTI de Política de Gestión de Documento Electrónico se refiere a movimientos de documentos entre repositorios, tanto internos dentro de la organización (sin cambios en la responsabilidad de custodia) como entre entidades administrativas, con o sin cambios en la responsabilidad. El concepto de transferencia va sin embargo muy ligado al cambio de responsabilidad de la custodia o la propiedad de los documentos (ej. ISO 15489). Y aún limita más el ámbito el diccionario de terminología archivística del Ministerio de Cultura al definir transferencia como "Procedimiento habitual de ingreso de fondos en un archivo mediante traslado de las fracciones de series documentales, una vez que éstas han cumplido el plazo de permanencia fijado por las normas establecidas en la valoración para cada una de las etapas del ciclo vital de los documentos."[1]

En esta ponencia se hablará de movimientos o traspasos de documentos entre repositorios en sentido general y de transferencia, como cambio de responsabilidad en la custodia en particular.

Consideraciones generales

Un requisito común a todo escenario en el que se produzca un traspaso de expedientes o documentos, es el de controlar y dejar constancia de dichos movimientos, preferiblemente mediante metadatos de trazabilidad. Los metadatos de trazabilidad han sido incluidos en la ponencia sobre metadatos y en la propuesta de Esquema Institucional de Metadatos por lo que no se incidirá más sobre ese punto en esta ponencia, aun cuando sea un punto de suma importancia a la hora de tratar las transferencias de documentos.

El paso entre repositorios, salvo migraciones puntuales de plataformas o sistemas de almacenaje, o intercambios de expedientes o documentos, no relacionadas con el ciclo de vida de expedientes o documentos, debe estar definido y controlado por reglas en el sistema de gestión de documentos electrónicos, a partir de lo dispuesto en los calendarios de conservación. Sin embargo, se debe disponer de mecanismos de bloqueo para aquellos expedientes objeto de recursos administrativos, económico administrativos o que por algún motivo deban exceptuarse de la aplicación de las reglas generales.

Se deberán auditar los mecanismos, procedimientos y controles de transferencia regularmente para garantizar la correcta conservación y la seguridad de los documentos.

II TRASPASO ENTRE REPOSITORIOS DE LA ORGANIZACIÓN

Una organización puede definir reglas aplicables en el ciclo de vida del documento para establecer cambios en sus **sistemas de almacenamiento**, de forma que se puedan optimizar

[1] http://www.mcu.es/archivos/MC/DTA/Diccionario.html#_t

los recursos, empleando tecnologías que proporcionan mejores prestaciones en cuanto a velocidad de acceso para documentos de acceso frecuente y tecnologías más lentas pero más baratas para documentos a los que se accede con una frecuencia muy inferior.

También podría producirse un traspaso cuando por motivos de obsolescencia tecnológica, económicos o estratégicos, una organización decide sustituir sus sistemas de almacenamiento, sus plataformas o su sistema de gestión de documentos electrónicos por otros. Este escenario podría definirse mejor con el término "**migración**". Se tendrá que gestionar el cambio de forma adecuada, con una correcta evaluación del riesgo, adoptando las medidas necesarias para minimizarlo, planificando las acciones a realizar y estableciendo puntos de control exhaustivos para prevenir que la información se pierda o que no se cumplan los requisitos de seguridad en el tránsito.

Una vez conformados los documentos en su forma definitiva y cerrados los expedientes sin posibilidad de cambios, se podría programar su traspaso a un **sistema de gestión de documentos de archivo "de oficina"** que, igual que el sistema de gestión de documentos vivos, estaría bajo control de la organización que lo produjo.

Otro escenario posible sería la gestión por parte de un proveedor externo de los documentos/expedientes: se deberá tener en cuenta todas las consideraciones de tipo legal respecto a servicios externos, establecidas por LOPD, ENS y otras normas aplicables. También es importante garantizar una transmisión segura, al utilizar redes externas para las comunicaciones, para lo cual, se deberá cumplir la normativa sobre trasmisión de información en el ámbito de la Política de Seguridad de la Información de la organización. Se anexa a modo informativo a esta ponencia la Norma de Seguridad de Transmisión de la Información de la SEAP.

III TRASPASO ENTRE REPOSITORIOS DE DISTINTAS ORGANIZACIONES, SIN CAMBIO EN LA RESPONSABILIDAD DE LA CUSTODIA.

En el caso de envío de documentos a otras entidades sin cambio de responsabilidad, se trataría de un **intercambio de expedientes o de documentos electrónicos**, regulado en el apartado V de la NTI de expediente electrónico y en el apartado VII de la NTI de documento electrónico.

Si se produce entre entidades de las Administraciones Públicas, la transferencia deberá realizarse por red SARA como medio seguro de comunicación. En el caso improbable de no poderse realizar por red SARA, remitimos a lo dicho respecto a transmisión segura para intercambio con proveedores externos.

IV TRANSFERENCIA, CON CAMBIO DE RESPONSABILIDAD EN LA CUSTODIA

En el caso de una transferencia, que conlleve un cambio de responsabilidad en la custodia, además de las consideraciones generales para cualquier tipo de movimiento o traspaso (control de la trazabilidad, reglas de paso entre repositorio, transmisión por medio seguro), las NTI de expediente electrónico y documento electrónico establecen la obligación por parte del órgano o entidad que transfiere de verificar (garantizar) la integridad y autenticidad de los documentos y expedientes.

Esto se consigue mediante firma electrónica del organismo remisor de los índices de los expedientes y de los documentos electrónicos.

Aunque podrían darse otros escenarios de transferencia debidos, por ejemplo,a una reestructuración organizativa con cambio de atribuciones a otro órgano administrativo, el caso más habitual es el paso a archivo central o a archivo histórico (a través del archivo central o directamente, en función de la jerarquía de sistemas de gestión documental de archivo que se establezca), para conservación permanente de los documentos.

Protocolo de transferencia a archivo

Al igual que en el caso de archivos físicos, debería definirse un protocolo de transferencia a archivos centrales o archivos históricos de documentos electrónicos. Entre otros puntos, debería incluir:

La adaptación en el origen de los documentos y expedientes:

- Adaptar cuando sea necesario los documentos que vayan a enviarse, preferiblemente, a un formato longevo, como PDF-A y, en todo caso, a formatos recogidos en la NTI de Catálogo de Estándares.
- Añadir las firmas que pudieran faltar así como la información necesaria para la verificación y validación y los sellos de tiempo que garanticen la conservación a largo plazo de las mismas, a no ser que la transferencia se produzca a un sistema que garantice la conservación de las firmas por otros medios.
- Conformar los documentos y expedientes según las estructuras establecidas en las NTIs de Documento Electrónico y Expediente Electrónico.
- Actualizar y completar metadatos complementarios necesarios para la gestión archivística.

Las siguientes tareas a nivel de expedientes:

- Eliminar aquellos documentos que no sean parte del Patrimonio Documental de la AGE, sino documentos de apoyo informativo[2]. Si en el dictamen de la Comisión Calificadora competente se solicita que se transfieran solamente algunos documentos que formen parte del expediente, se deberá realizar la selección de los mismos.
- Realizar el muestreo de expedientes y/o documentos si así se indica en el Dictamen de la Comisión Calificadora.

Deberá generarse un paquete con los expedientes o documentos a transferir, con un formato acordado, partiendo de normas internacionales como OAIS (ISO 14721). Tendría que incluirse en ese paquete o indicarse de alguna manera información general sobre la transferencia, al menos, las series documentales, las fechas extremas de cada serie, el dictamen de la autoridad calificadora y el número de expedientes o agrupaciones documentales que se van a enviar.

El receptor deberá verificar el contenido del paquete transferido, confirmando que contiene los expedientes y los documentos acordados, en el formato correcto y con los metadatos complementarios necesarios.

El receptor deberá enviar constancia de la recepción correcta al organismo que realizó la transferencia.

Destrucción de documentos

En el momento en que haya recibido la conformidad por parte del nuevo responsable de la custodia, el organismo que haya transferido los expedientes/documentos podría proceder a la eliminación de los mismos.

En el caso de los documentos o expedientes de la serie documental que hayan sido descartados por no requerirse la conservación a largo plazo de los mismos, deberá seguirse el procedimiento regulado por el Real Decreto 1164/2002. Hasta su destrucción deberán almacenarse en sistemas ajenos a los gestores de documentos de la organización. Deberán tenerse en cuenta también las medidas establecidas en el Esquema Nacional de Seguridad (Real Decreto 3/2010) en su apartado 5.5.5 de “Borrado y destrucción” de soportes de información (mp.si.5).

---

[2] http://www.mcu.es/archivos/docs/MetodologiaComSup.pdf *Son documentos de archivo de la Administración General de Estado y forman parte de su Patrimonio Documental los documentos de cualquier época, generados, conservados o reunidos en el ejercicio de su función por cualquiera de los departamentos y órganos que la componen, por sus organismos públicos, por las personas jurídicas en cuyo capital participe mayoritariamente el Estado y por las personas privadas, físicas o jurídicas, gestoras de servicios públicos de carácter estatal en lo relacionado con la gestión de dichos servicios.*

Constituye documentación de apoyo informativo, y no forma parte del Patrimonio Documental, aquella que no se produce como resultado de la gestión administrativa, aunque sea necesario disponer de ella para el correcto desarrollo de la actividad administrativa (textos legales, boletines oficiales, publicaciones, circulares).

LA DOCUMENTACIÓN DE APOYO INFORMATIVO NO TIENE QUE SER OBJETO DE VALORACIÓN a los efectos del R.D. 1164/2002, de 8 noviembre. Puede ser destruida una vez que ha cumplido los fines para los que fue reunida.

Otras consideraciones

La NTI de Expediente Electrónico dice que cuando la naturaleza o la extensión de las pruebas o documentos que forman parte del expediente electrónico no permitan o dificulten notablemente su inclusión en una de las estructuras establecidas, se incorporará al expediente electrónico un documento en el que se especifique cuáles son estas pruebas o documentos que no puedan incluirse en las estructuras establecidas. La transferencia en estos casos podrá realizarse usando otros soportes. Además de la referencia al apartado 5.5 de medidas de seguridad para la protección de los soportes de información del Esquema Nacional de Seguridad se anexa a efectos informativos la "**Norma de seguridad de soportes de la Secretaría de Estado de Administraciones Públicas**" en el ámbito de la Política de Seguridad de la Información de la SEAP.

En el caso de tramitación compartida de expedientes entre Administraciones Públicas o entidades administrativa, se deberá determinar en función del procedimiento concreto si cada intercambio de expedientes supone una transferencia de la responsabilidad de la custodia o no, siendo de aplicación en cada caso lo definido en los puntos anteriores de este documento.

Ponencia nº 8

Destrucción o eliminación segura de documentación electrónica y soportes informáticos

Alejandro Millaruelo Gómez y Andoni Pérez de Lema Sáenz de Viguera
(Intervención General de la Administración del Estado)

Resumen de la ponencia:

Destrucción o eliminación segura de documentación electrónica y soportes informáticos

Alejandro Millaruelo Gómez y Andoni Pérez de Lema Sáenz de Viguera
(Intervención General de la Administración del Estado)
Ponencia nº 8

INTRODUCCIÓN

Los sistemas de información capturan, procesan y guardan la información (y los documentos electrónicos) usando soportes de almacenamiento, sujetos a una evolución y cambio constantes. Además esta información no sólo se encuentra en estos soportes, sino también en dispositivos utilizados para crear, procesar o transmitir información. Obviamente la documentación puede eliminarse, lo que requerirá un proceso de borrado o, incluso, de destrucción del soporte de almacenamiento, para mitigar el riesgo de revelación no autorizada de la información contenida en los documentos, así como asegurar su confidencialidad. Los métodos de borrado dependerán del nivel de sensibilidad de la documentación y del soporte elegido para su almacenamiento.

Los procesos de destrucción o eliminación segura de documentación electrónica y soportes informáticos deben integrarse en la política de gestión de documentos electrónicos y la política de seguridad de la organización, y se atendrán al marco legal de referencia que establece las condiciones necesarias de confianza en el uso de los medios electrónicos por parte de las administraciones españolas. Estas condiciones de confianza incluyen las medidas y procedimientos que se han dispuesto legalmente para la eliminación de documentos que no requieren conservación permanente.

ACLARANDO CONCEPTOS

El diccionario de Terminología Archivística del Ministerio de Cultura define eliminación como el “procedimiento archivístico que consiste en la identificación de los documentos que se van a destruir conforme a los plazos establecidos en la fase de valoración” y la destrucción como la “destrucción física de unidades o series documentales que hayan perdido su valor administrativo, probatorio o constitutivo o extintivo de derechos y que no hayan desarrollado ni se prevea que vayan a desarrollar valores históricos. Esta destrucción se debe realizar por cualquier método que garantice la imposibilidad de reconstrucción de los documentos”.

Mediante el proceso de selección se localizan las fracciones de serie que han de ser eliminadas o conservadas en virtud de los plazos establecidos en el proceso de valoración.

Estas términos no pueden aplicarse a la documentación electrónica como se hace con la documentación en papel, puesto que aquella posee unas características específicas que deben tenerse en cuenta: se almacena en soportes de almacenamiento con un formato específico; el contenido informativo es independiente del soporte y el formato; los soportes son generalmente reutilizables; su vida útil es corta comparada con la de un soporte en papel; los procedimientos de destrucción deberán tener en cuenta las características de los soportes más adecuados para la conservación de los documentos electrónicos; pueden existir múltiples copias, no siempre controladas, de los documentos.

Atendiendo a estas características de la documentación electrónica se propone emplear los términos borrado, entendido como el procedimiento de eliminación de los datos o ficheros de un soporte o conjunto de soportes, permitiendo su reutilización, y destrucción, entendido como el proceso de destrucción física de un soporte de almacenamiento que contenga documentos electrónicos.

REQUERIMIENTOS LEGALES

La legislación en materia de destrucción o eliminación de documentos comprende:

- Esquema Nacional de Interoperabilidad.
- Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos.
- Esquema Nacional de Seguridad.
- Real Decreto 1164/2002
- Real Decreto 1720/2007

De acuerdo con el RD 1664/2002, se entiende por eliminación de documentos la destrucción física de unidades o series documentales por el órgano responsable del archivo u oficina pública en que se encuentren, empleando cualquier método que garantice la imposibilidad de reconstrucción de los mismos y su posterior utilización. La eliminación de documentos sólo podrá llevarse a cabo, tras el correspondiente proceso de valoración documental.

A iniciativa propia o de los órganos responsables de los documentos o series documentales concernidos, la Comisión Calificadora de Documentos Administrativos de cada Departamento u Organismo público podrá acordar la iniciación de un procedimiento de eliminación de documentos y, en su caso, de conservación del contenido de los mismos en soporte distinto del original en que fueron producidos.

El órgano responsable de la custodia de la documentación, una vez sea ejecutiva la autorización obtenida, abrirá un expediente de eliminación de los documentos o series documentales de que se trate.

Según el Esquema Nacional de Seguridad, cuando la naturaleza del soporte no permita un borrado seguro, o cuando así lo requiera el procedimiento asociado al tipo de información contenida, deberá procederse a la destrucción segura del soporte.

De conformidad con el RD 1720/2007, siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

Según el Esquema Nacional de Interoperabilidad, el borrado de la información o la destrucción de los soportes deberá hacerse de acuerdo con la legislación que resulte de aplicación, dejando registro de la eliminación.

SOPORTES Y SISTEMAS DE ALMACENAMIENTO

Aunque existe una relativa variedad de soportes de almacenamiento, no todos son capaces de asegurar la conservación y garantizar la accesibilidad y disponibilidad de la documentación electrónica durante todo el ciclo de vida de la misma. Como la conservación de los datos a lo largo del tiempo es una de las funciones primordiales de cualquier soporte de almacenamiento, los métodos de borrado estarán estrechamente ligados a las características de los soportes más adecuados para garantizar esta conservación.

Las tecnologías actuales proporcionan tres tipos de soportes:

- Soportes magnéticos (discos duros y cartuchos de cinta).
- Soportes ópticos (relegados hoy a entornos domésticos).
- Soportes basados en memorias de estado sólido.

Un aspecto importante a tener en consideración, en cuanto a soportes de almacenamiento, es la distinción entre almacenamiento local (puestos de usuario, dispositivos móviles, dispositivos removibles como discos duros externos, memorias USB, tarjetas de memorias, etc.) y almacenamiento en red (ya sea accesible mediante protocolos para compartir ficheros, como CIFS o NFS; redes SAN; almacenamiento en la nube; etc.).

El almacenamiento local (basado en discos duros magnéticos o memoria FLASH) no es el entorno adecuado para la conservación de documentos de archivo, por no reunir las características necesarias para asegurar su permanencia, integridad, confidencialidad y disponibilidad. Sin embargo, en el almacenamiento local se generan y editan documentos, y se pueden encontrar copias de documentos de archivo (sin que incluyan necesariamente los metadatos y firmas preceptivos). La eliminación de los documentos de archivo deberá contemplar también este tipo de almacenamiento, con objeto de conseguir un borrado exhaustivo.

LA NECESIDAD DE ESTABLECER PROCEDIMIENTOS DE BORRADO SEGURO DE LA DOCUMENTACIÓN ELECTRÓNICA

Las utilidades comunes de los sistemas operativos son generalmente insuficientes para garantizar que no pueda recuperarse, empleando técnicas específicas, la información una vez borrada. Este riesgo pone en peligro la necesaria confidencialidad de la información, más aún si ésta es reciente, o bien contradice el mismo proceso de eliminación de la documentación al no garantizar su irreversibilidad.

En consecuencia, se deben establecer controles en las organizaciones para salvaguardar los soportes que contienen la información de la que son responsables, tales como: identificar las técnicas de borrado apropiadas para cada soporte y tipo de información, dejar constancia de los procedimientos de borrado realizados, seguir todos los requisitos legales y trámites establecidos.

Las principales dificultades que pueden surgir en las operaciones de borrado, que requieren el uso de aplicaciones o técnicas de borrado especializadas son:

- Algunos paquetes software son incapaces de sobrescribir datos en sectores protegidos o defectuosos, o no conocen la capacidad real del disco.
- El fenómeno del “borde de la pista”.
- Los comandos de borrado del sistema operativo sólo modifican los registros del sistema de archivos, pero pueden dejar intacto el contenido propiamente dicho del documento, marcando únicamente el espacio en el cual se encuentra el archivo como disponible.
- El problema del “slack cluster” o cluster incompleto.

TERMINOLOGÍA Y TIPOS DE BORRADO Y DESTRUCCIÓN DE SOPORTES

Se propone la siguiente terminología aplicable al borrado de documentos electrónicos:

- Borrado de nivel 0: remoción de los documentos empleando comandos estándar del sistema operativo. Este procedimiento no proporciona ninguna garantía frente a la revelación no autorizada de la información.
- Borrado de nivel 1: es la remoción de los datos o documentos sensibles de un soporte de almacenamiento de tal manera que hay seguridad de que los datos no podrán ser reconstruidos utilizando las funciones normales del sistema o programas de recuperación de archivos. Los datos aún podrían ser recuperables, pero ello requeriría técnicas especiales de laboratorio o utilidades avanzadas. Una de las formas más conocidas para realizar un borrado de nivel 1 es la sobreescritura de datos.
- Borrado de nivel 2: es la remoción de datos o documentos sensibles de un dispositivo de almacenamiento con el objeto de que los datos no puedan ser reconstruidos utilizando alguna de las técnicas conocidas. Ejemplos de borrado de nivel 2 serían: desmagnetizar un disco, ejecutar el comando de borrado seguro del firmware de algunos dispositivos, o cifrar un soporte de almacenamiento con criptografía fuerte.
- Destrucción: El soporte de almacenamiento es físicamente destruido, lo que impide su reutilización.

Se analizan una serie de técnicas específicas de borrado seguro, identificando sus características, nivel de seguridad, y los escenarios en los que son aplicables:

A.- Sobreescritura. Existen diversos algoritmos (NAVSO P-539-2, Bruce Schneier, Peter Gutmann, Gutmann parcial, OTAN), que difieren en el número de sobreescrituras y en los patrones utilizados. Los más seguros son: Gutmann, Bruce Schneier, OTAN y Gutmann parcial.

B.- Comando "Secure Erase" en Firmware. Se considera como un medio válido de borrado de nivel 2, únicamente para los discos ATA.

C.- Desmagnetización. Cada dispositivo, según su tamaño, forma y el tipo de soporte magnético de que se trate, necesita de una potencia específica para asegurar la completa polarización de todas las partículas.

D.- Destrucción física. Existen diversas técnicas: desintegración, pulverización, fusión, incineración y triturado. Implican la utilización de métodos industriales de destrucción distintos para cada soporte, obligan a un transporte de los dispositivos a un centro de reciclaje adecuado, y los residuos generados deben ser tratados adecuadamente.

E.- Criptografía y Borrado Criptográfico: los SED ("self encrypting devices") disponen de cifrado permanente que reduce sustancialmente la probabilidad de que datos sin cifrar se retengan inadvertidamente en el dispositivo. El usuario no puede desactivar las capacidades de cifrado, asegurando así que todos los datos están cifrados. El fundamento del borrado criptográfico es que aprovecha el cifrado para implementar el borrado de los datos mediante la eliminación de la clave de cifrado del dispositivo. Una ventaja del borrado criptográfico es que permite realizar una limpieza de alta seguridad de manera mucho más rápida que con otras técnicas. Además, este método puede ser utilizado como un suplemento a otras aproximaciones de borrado seguro.

F.- Técnicas aplicables al caso particular de las memorias flash: aunque no existen estándares específicos para el borrado de memorias flash, se pueden emplear todas las técnicas descritas anteriormente, a excepción de la desmagnetización. No obstante, como las actualizaciones sobre la propia ubicación de los datos no son posibles en las memorias flash, es posible que las técnicas de borrado basadas en sobreescrituras que funcionan bien en los discos duros magnéticos no funcionen adecuadamente en las memorias flash. Ninguna de las técnicas actualmente existentes para el borrado de ficheros individuales en discos duros magnéticos son eficientes en memorias Flash, lo que conlleva la necesidad de llevar a cabo una limpieza completa del dispositivo.

PROCESO DE ELIMINACIÓN DE DOCUMENTOS ELECTRÓNICOS

El proceso de eliminación de documentos electrónicos forma parte de la política de gestión documental de la organización. En este sentido será necesario definir los métodos de borrado específicos y los de destrucción de soportes de almacenamiento a emplear en los distintos escenarios, en función de los siguientes factores condicionantes:

- Nivel de confidencialidad de la información recogida en el documento (dimensión ENS).
- Nivel LOPD.
- Soporte de almacenamiento:
  - Naturaleza del soporte: Magnético / Óptico.
  - Tipo de acceso: Aleatorio / Secuencial.
  - Portabilidad: Dispositivos extraíbles / Dispositivos fijos.
    - Se debe tener en cuenta si se pretende reutilizar el soporte o bien cambiar de soporte.
- Tipo de gestión de los sistemas de información: Interna / Externa.

- Alcance de la eliminación:
  - Parcial (si afecta a una parte del soporte de almacenamiento, por ejemplo a un fichero o conjunto de ficheros).
  - Total.

A partir de estas variables se determinará el tipo de eliminación mínimo recomendado:

- Borrado de nivel 0.
- Borrado de nivel 1 (equivalente al concepto de *clearing*).
- Borrado de nivel 2 (equivalente al concepto de *purging* o *sanitization*).
- Destrucción del soporte.

Se distinguen una serie de contextos en los que podrá tener lugar la eliminación de documentos electrónicos:

- Por un Acuerdo de Eliminación.
- Por cambio de formato.
- Si se han realizado varias copias auténticas a distintos formatos, podría eliminarse alguna de ellas.
- Por fallo en el soporte de almacenamiento y su sustitución.
- Por transferencia entre archivos.
- Por cambio de soporte de almacenamiento (por obsolescencia o migración entre sistemas de almacenamiento).

Se establece una Tabla de Decisión del Proceso de Borrado, en la que se indica el proceso de borrado mínimo recomendado para cada escenario, en función de los factores condicionantes señalados.

Ponencia nº 8

Destrucción o eliminación segura de documentación electrónica y soportes informáticos

Alejandro Millaruelo Gómez y Andoni Pérez de Lema Sáenz de Viguera
(Intervención General de la Administración del Estado)

Índice de la Ponencia

I INTRODUCCIÓN

Los sistemas de información operan como motor del cambio en los métodos de trabajo de empresas y organismos públicos, permitiendo ganancias en eficiencia económica, una mejor utilización de los recursos humanos y materiales y el desarrollo de servicios avanzados que refuercen el bienestar de los ciudadanos. Por esta razón la información se ha convertido en uno de los activos más valiosos y sensibles en el contexto de la Administración Electrónica.

Es preciso tener en cuenta que los sistemas de información capturan, procesan y guardan la información (y los documentos electrónicos) usando soportes de almacenamiento, sujetos a una evolución y cambio constantes. Además esta información no sólo se encuentra en estos soportes, sino también en dispositivos utilizados para crear, procesar o transmitir información.

Obviamente la documentación puede eliminarse, lo que requerirá un proceso de borrado o, incluso, de destrucción del soporte de almacenamiento, para mitigar el riesgo de revelación no autorizada de la información contenida en los documentos, así como asegurar su confidencialidad. Los métodos de borrado dependerán del nivel de sensibilidad de la documentación, del soporte elegido para su almacenamiento, del modelo de gestión (interna o externa) de los sistemas de almacenamiento, y de la posible necesidad de reutilización de estos soportes.

Cuando se trata la seguridad informática, se suelen destacar cuestiones como la protección frente a código malicioso, la implantación de firewalls, la separación de redes o la realización de copias de seguridad periódicas. Sin embargo hay que atender también una cuestión clave para proteger la confidencialidad de los datos y mantener la cadena de custodia: la necesidad de realizar mediante procedimientos seguros un borrado de los documentos que se encuentran almacenados en cualquier tipo de soporte, antes de reutilizarlo o deshacerse del mismo.

Los procesos de *Destrucción o eliminación segura de documentación electrónica y soportes informáticos* deben integrarse en la política de gestión de documentos electrónicos y la política de seguridad de la organización, y se atendrán al marco legal de referencia que establece las condiciones necesarias de confianza en el uso de los medios electrónicos por parte de las administraciones españolas. Estas condiciones de confianza incluyen las medidas y procedimientos que se han dispuesto legalmente para la eliminación de documentos que no requieren conservación permanente.

El uso de algoritmos de cifrado de sofisticación creciente, ha conducido a que los atacantes que desean ganar acceso a la información sensible de una organización se vean forzados a escudriñar fuera del sistema propiamente dicho para obtener la información. Un cauce de ataque es la recuperación de datos supuestamente borrados de los soportes, y las técnicas de destrucción o eliminación segura pueden ser utilizadas para asegurar que los datos borrados no puedan ser recuperados.

II ACLARANDO CONCEPTOS

Antes de todo es necesario definir una serie de conceptos archivísticos que son esenciales y que, como se verá, habría que adaptar o redefinir para la documentación electrónica.

El diccionario de Terminología Archivística del Ministerio de Cultura recoge tres términos estrechamente relacionados: destrucción, eliminación y selección, que define de la siguiente manera:

Destrucción

Destrucción física de unidades o series documentales que hayan perdido su valor administrativo, probatorio o constitutivo o extintivo de derechos y que no hayan desarrollado

ni se prevea que vayan a desarrollar valores históricos. Esta destrucción se debe realizar por cualquier método que garantice la imposibilidad de reconstrucción de los documentos.

Eliminación

Procedimiento archivístico que consiste en la identificación de los documentos que se van a destruir conforme a los plazos establecidos en la fase de valoración.

Selección

Operación intelectual y material de localización de las fracciones de serie que han de ser eliminadas o conservadas en virtud de los plazos establecidos en el proceso de valoración.

Basándonos en estas definiciones, la acción de destruir un conjunto de documentos debe ser consecuencia de un proceso previo de selección y de un procedimiento subsiguiente de eliminación. La destrucción tiene obviamente una connotación física, puesto que lo que se destruye es el soporte y con él la información que contiene. Si se trata de documentos de archivo en papel, soporte e información forman un todo, y destruyendo el primero destruimos también el segundo, pero si nos referimos a documentos electrónicos el resultado no es tan sencillo.

La documentación electrónica posee unas particularidades que no podemos pasar por alto:

- Los documentos electrónicos se almacenan en un soporte de almacenamiento, con un formato específico.
- El contenido informativo de un documento es independiente de su soporte y de su formato. Éstos puede cambiar sin que se altere su contenido.
- El soporte de un documento electrónico es generalmente reutilizable.
- Todo soporte tiene una vida útil, más o menos extensa, pero más corta que la de un soporte en papel. Así pues, será necesario afrontar cambios de soporte durante el ciclo de vida de un documento electrónico, incluso aunque carezca de valores secundarios que justifiquen su conservación permanente.
- Todo soporte o formato se hará obsoleto en un plazo más o menos largo de tiempo, lo que implicará necesariamente un cambio de soporte o formato (excepto algunos formatos longevos como PDF/A).
- Los procedimientos de destrucción de la documentación deberán tener en cuenta las características tecnológicas de los distintos soportes. En este sentido hay que señalar que no todos los soportes de almacenamiento reúnen las condiciones necesarias para asegurar la conservación de los documentos.
- Los soportes de almacenamiento idóneos para asegurar la conservación, disponibilidad y accesibilidad de los documentos electrónicos deben contemplarse en el contexto de sistemas de almacenamiento, que cumplirán necesariamente unos requisitos de alta disponibilidad, rendimiento, escalabilidad no disruptiva y replicación, para ser considerados aptos para la conservación de los documentos.
- Pueden existir múltiples réplicas o copias de un documento, sin que se pierda su condición de original. Los backups, las réplicas locales o remotas, las descargas, etc., harán que un documento electrónico se encuentre en múltiples soportes o ubicaciones, muchas de ellas desconocidas o no controlables.
- La información que contiene un documento electrónico puede recogerse, total o parcialmente, en bases de datos. La destrucción de un documento, ¿implicaría necesariamente la destrucción de los registros correspondientes de una base de datos?
- Una transferencia de documentos electrónicos, con cambio de soporte, por ejemplo, entre un archivo de gestión y uno intermedio, supone de facto la duplicación temporal de este conjunto de documentos.

Atendiendo a estas particularidades, se propone emplear los siguientes términos, que se adaptan mejor a las características de la documentación electrónica:

Destrucción

Referido a un soporte de almacenamiento que contenga documentos electrónicos, proceso de destrucción física del mismo, ya sea por obsolescencia del soporte, por sustitución completa del sistema de almacenamiento o porque las características de la información de los documentos aconsejen esta destrucción (por ejemplo, por su elevado grado de confidencialidad).

Borrado

Referido a documentos electrónicos, procedimiento de eliminación de los datos o ficheros de un soporte o conjunto de soportes, permitiendo su reutilización. Se definirán más adelante los distintos procedimientos de borrado seguro de los documentos electrónicos, atendiendo a las características de los soportes y al tipo de información.

Eliminación

Referido a los documentos electrónicos, procedimiento de identificación de los documentos electrónicos a borrar, sus metadatos, sus copias, réplicas, etc., y de selección de los métodos de borrado adecuados en función del tipo de soporte y clasificación de la información.

III REQUERIMIENTOS LEGALES

A continuación se hace un repaso de la legislación en materia de destrucción o eliminación de documentos, al objeto de determinar las obligaciones legales que corresponden a las Administraciones Públicas.

III.1 ESQUEMA NACIONAL DE INTEROPERABILIDAD

En el apartado “k” de su artículo 21 (Condiciones para la recuperación y conservación de documentos) se establece la siguiente medida:

k) Si el resultado del procedimiento de evaluación documental así lo establece, borrado de la información, o en su caso, **destrucción física de los soportes, de acuerdo con la legislación que resulte de aplicación, dejando registro de su eliminación.**

En su glosario de términos define “Ciclo de vida de un documento electrónico” como sigue: *Conjunto de las etapas o períodos por los que atraviesa la vida del documento, desde su identificación en un sistema de gestión de documentos, hasta su selección para conservación permanente, de acuerdo con la legislación sobre Archivos de aplicación en cada caso,* ***o para su destrucción reglamentaria.***

III.2 NORMA TÉCNICA DE INTEROPERABILIDAD DE POLÍTICA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS

Apartado VI.1.9:

Destrucción o eliminación de los documentos, que atenderá a la **normativa aplicable en materia de eliminación de Patrimonio Documental** y contemplará la aplicación de las medidas de seguridad relacionadas definidas en el Real Decreto 3/2010, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad** en el ámbito de la Administración Electrónica: **Borrado y destrucción del capítulo de «Protección de los soportes de información [mp.si]» y Limpieza de documentos del capítulo de «Protección de la información [mp.info]**».

Borrado y destrucción [mp.si.5]

dimensiones	C		
nivel	bajo	medio	alto
	no aplica	aplica	=

La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

a) Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su anterior contenido.

b) Se destruirán de forma segura los soportes, en los siguientes casos:

1. Cuando la naturaleza del soporte no permita un borrado seguro.
2. Cuando así lo requiera el procedimiento asociado al tipo de la información contenida.

c) Se emplearán, preferentemente, productos certificados [op.pl.5].

Limpieza de documentos [mp.info.6]

dimensiones	C		
nivel	bajo	medio	alto
	aplica	=	=

En el proceso de limpieza de documentos, se retirará de estos toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.

Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.

Se tendrá presente que el incumplimiento de esta medida puede perjudicar:

a) Al mantenimiento de la confidencialidad de información que no debería haberse revelado al receptor del documento.
b) Al mantenimiento de la confidencialidad de las fuentes u orígenes de la información, que no debe conocer el receptor del documento.
c) A la buena imagen de la organización que difunde el documento por cuanto demuestra un descuido en su buen hacer.

III.4 REAL DECRETO 1164/2002

Esta norma, que 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 documentos administrativos en soporte distinto al original”, trata profusamente en diversos artículos la cuestión que nos ocupa:

Artículo 2. Régimen de la eliminación de documentos y, en su caso, de la conservación de los mismos en soporte distinto al original.

1. A los efectos de este Real Decreto se entiende por eliminación de documentos la destrucción física de unidades o series documentales por el órgano responsable del archivo u ofi-

cina pública en que se encuentren, **empleando cualquier método que garantice la imposibilidad de reconstrucción de los mismos y su posterior utilización**. La eliminación de documentos **sólo podrá llevarse a cabo, tras el correspondiente proceso de valoración documental**, según se establece en los artículos siguientes.

Artículo 4. Iniciación del procedimiento.

1. A iniciativa propia o de los órganos responsables de los documentos o series documentales concernidos, la Comisión Calificadora de Documentos Administrativos de cada Departamento u Organismo público podrá acordar la **iniciación de un procedimiento de eliminación de documentos y, en su caso, de conservación del contenido de los mismos en soporte distinto del original** en que fueron producidos.

Artículo 7. Eliminación de documentos.

1. El órgano responsable de la custodia de la documentación, una vez sea ejecutiva la autorización obtenida, **abrirá un expediente de eliminación** de los documentos o series documentales de que se trate, el cual comprenderá:

   a) La **memoria realizada sobre la documentación** y cualquier otra información o documentos presentados con la **propuesta de eliminación**, así como el texto de esta última.

   b) El **dictamen de la Comisión Superior Calificadora de Documentos Administrativos** y el de cualquier otra Comisión que se haya pronunciado previamente.

   c) La **memoria del muestreo** de la documentación a expurgar.

   d) La **resolución que haya autorizado la eliminación**, así como cualquier otro documento administrativo o judicial relacionado con la misma.

   e) El **acta de eliminación**, en la que el órgano responsable de los documentos acreditará que, habiendo transcurrido el plazo de tres meses establecido en el apartado 2, párrafo b), del artículo 6 de este Real Decreto, no tiene constancia de la interposición de recursos de ninguna naturaleza contra la resolución adoptada, o que ésta ha adquirido firmeza, con los demás extremos relativos a la destrucción que se lleva a cabo, fecha de la misma e identificación de los funcionarios y cualquier otro personal que intervenga en ella. En dicha acta **se hará constar lugar, fecha y duración de las operaciones de eliminación con o sin sustitución, procedimiento utilizado, personas intervinientes y funcionario fedatario de la operación y del acta.**

2. **Si se hubiese dispuesto la conservación del contenido de los documentos o series documentales en soporte distinto al original**, antes de proceder a la eliminación de dicho original **deberán obtenerse copias auténticas** en soporte diferente, con los requisitos establecidos en el artículo 46 de la Ley 30/1992, de 26 de diciembre y, en su caso, en el artículo 45 de dicha Ley y en el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas en la Administración General del Estado.

En este mismo supuesto deberá finalmente levantarse un acta complementaria de la reseñada en el párrafo e) del apartado 1 de este mismo artículo, comprensiva de las actuaciones que se sigan para hacer efectiva la **conservación del contenido de los documentos en soporte distinto al original**. En el acta se hará constar las características técnicas del nuevo soporte de acuerdo con el citado Real Decreto 263/1996, de 16 de febrero.

3. Un **duplicado del acta y, en su caso, del acta complementaria se remitirá a la Comisión Superior Calificadora de Documentos Administrativos** en el plazo de los diez días siguientes a la fecha de las actuaciones correspondientes.

III.5 REAL DECRETO 1720/2007 (REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL)

Artículo 92. Gestión de soportes y documentos

Siempre que vaya a **desecharse cualquier documento o soporte que contenga datos de carácter personal** deberá procederse a su **destrucción o borrado**, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

Las medidas y procedimiento a través de las cuales se cumplirá con las obligaciones reguladas en este apartado se incluirán dentro del documento de seguridad, en virtud del artº. 88.3 del mismo Real Decreto

Artículo 88. El documento de seguridad

3. El documento deberá contener, como mínimo, los siguientes aspectos:

   g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

IV SOPORTES Y SISTEMAS DE ALMACENAMIENTO

Aunque existe una relativa variedad de soportes de almacenamiento, no todos son capaces de asegurar la conservación y garantizar la accesibilidad y disponibilidad de la documentación electrónica durante todo el ciclo de vida de la misma. Como la conservación de los datos a lo largo del tiempo es una de las funciones primordiales de cualquier soporte de almacenamiento, los métodos de borrado estarán estrechamente ligados a las características de los soportes más adecuados para garantizar esta conservación.

Actualmente existen tres tecnologías distintas que dan lugar, a su vez, a tres tipos genéricos de soportes de almacenamiento:

Soportes magnéticos

Entre los soportes de esta naturaleza encontramos:

Disco duro

Es el dispositivo de almacenamiento más extendido. Su precio y su tamaño físico se han ido reduciendo a medida que aumentaba su capacidad y la velocidad de transferencia. Es un soporte de los denominados de acceso aleatorio, lo que reduce el tiempo de acceso a los datos, aunque existen diferencias notables en función de las distintas tecnologías que se emplean a día de hoy.

Las principales tecnologías son:

- Discos SAS (Serial SCSI), a 15.000 y 10.000 rpm (revoluciones por minuto), hasta 1 TB de capacidad.
- Discos NL-SAS (Near Line SAS), de 7.200 rpm, hasta 4 TB de capacidad.
- Discos SATA (Serial ATA), de 7.200 rpm, hasta 4 TB de capacidad.

Al tratarse de dispositivos mecánicos que están constantemente girando, su vida útil es de unos pocos años (entre 3 y 5, según los propios fabricantes). Sin embargo es relativamente fácil replicar el contenido de un disco (o parte de él) en otro disco, por lo que este tipo de soportes son probablemente los más adecuados para garantizar la accesibilidad y disponibilidad de los documentos electrónicos.

Cartucho de cinta

Este tipo de soporte se emplea básicamente para almacenar datos de backup o datos de poco acceso y que deban ser conservados durante un período largo de tiempo.

Es un soporte relativamente económico y de gran capacidad. Así, por ejemplo, un cartucho de tipo Ultrium LTO 5 almacena hasta 3,2 TB (con compresión). Al ser un dispositivo de acceso secuencial el acceso es bastante más lento que el de un disco duro.

Para escribir o leer de estos dispositivos es necesario disponer de una librería robótica. Si se respetan las condiciones de conservación (temperatura, humedad, radiaciones electromagnéticas), los principales fabricantes señalan una vida útil de unos 30 años (cartuchos de cinta de Barium-Ferrita).

Soportes ópticos

Aunque tuvieron una época dorada como soporte similar a las cintas magnéticas, actualmente han quedado prácticamente relegados al mercado doméstico, aunque en este ámbito también están en retroceso. Este tipo de soporte no puede competir con la capacidad que proporcionan los soportes de tipo magnético.

Por orden de aparición comercial, mencionaremos los CD (Compact Disc) y los DVD (Digital Versatile Disc). Necesitan dispositivos lectores y de escritura (Juke-Box), y su vida útil se sitúa entre la de un disco duro magnético y la de una cinta magnética.

Soportes basados en memorias de estado sólido (FLASH)

Este tipo de soporte se está extendiendo, desde el ámbito doméstico donde comenzó a popularizarse, a entornos profesionales. A medida que su precio ha ido disminuyendo y su capacidad ha aumentado, los discos duros magnéticos de muchos portátiles están siendo sustituidos por discos de estado sólido, lo que redunda en un menor consumo eléctrico, reduce la posibilidad de fallos mecánicos (al no necesitar estos soportes de dispositivos mecánicos) y disminuye el tiempo de acceso a los datos.

En entornos profesionales los SSD (*solid state drive*) sustituyen a los discos duros magnéticos de mayor rendimiento, garantizando a las aplicaciones el menor tiempo de acceso a la información. Se emplean además para las memorias caché de sistemas de almacenamiento.

Existen tres tecnologías de memorias de estado sólido:

- SLC: Single Level Cell (un bit por celda).
- MLC: Multi Level Cell (dos bits por celda).
- TLC: Triple Level Cell (tres bits por celda)

Su vida útil depende del número de ciclos (u operaciones de escritura) por celda, que se contabiliza en millares. Cuanto más grande sea el número de ciclos (o sea, su vida útil), mayor será el precio de este tipo de soportes; cuanto mayor sea el número de bits por celda, más lento (aunque más económico).

A día de hoy resulta un soporte más adecuado para el almacenamiento de datos "vivos" y no para la conservación a largo de plazo de documentos electrónicos, dado su mayor precio en relación a otros soportes, aunque esta situación puede cambiar si la tecnología sigue evolucionando y el precio disminuye.

Un aspecto importante a tener en consideración, en cuanto a soportes de almacenamiento, es la distinción entre almacenamiento local (puestos de usuario, dispositivos móviles, dispositivos removibles como discos duros externos, memorias USB, tarjetas de memorias, etc.) y almacenamiento en red (ya sea accesible mediante protocolos para compartir ficheros, como CIFS o NFS; redes SAN; almacenamiento en la nube; etc.).

El almacenamiento local (basado en discos duros magnéticos o memoria FLASH) no es el entorno adecuado para la conservación de documentos de archivo, por no reunir las características necesarias para asegurar su permanencia, integridad, confidencialidad y disponibilidad. Sin embargo, en el almacenamiento local se generan y editan documentos, y se pueden encontrar copias de documentos de archivo (sin que incluyan necesariamente los metadatos y firmas preceptivos). La eliminación de los documentos de archivo deberá contemplar también este tipo de almacenamiento, con objeto de conseguir un borrado exhaustivo.

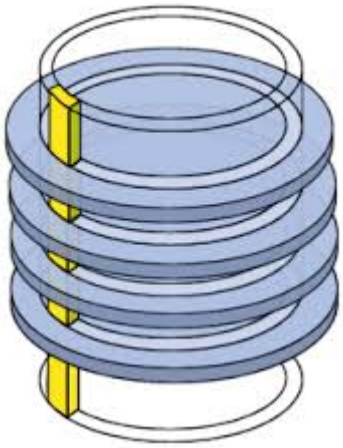
VI LA NECESIDAD DE ESTABLECER PROCEDIMIENTOS DE BORRADO SEGURO DE LA DOCUMENTACIÓN ELECTRÓNICA

Existen diversos problemas que dan lugar a la necesidad de implementar un proceso de borrado seguro de la documentación electrónica contenida en los soportes de almacenamiento, cuando así se haya establecido. Las utilidades comunes de los sistemas operativos son generalmente insuficientes para garantizar que no pueda recuperarse, empleando técnicas específicas, la información una vez borrada. Este riesgo pone en peligro la necesaria confidencialidad de la información, más aún si ésta es reciente, o bien contradice el mismo proceso de eliminación de la documentación al no garantizar su irreversibilidad.

En consecuencia, se deben establecer controles en las organizaciones para salvaguardar los soportes que contienen la información de la que son responsables, tales como: identificar las técnicas de borrado apropiadas para cada soporte y tipo de información, dejar constancia de los procedimientos de borrado realizados, seguir todos los requisitos legales y trámites establecidos en los procedimientos de eliminación, etc.

Seguidamente pasamos a describir las principales dificultades que pueden surgir en las operaciones de borrado, las cuales implican que éstas no puedan considerarse como seguras sin emplear técnicas específicas.

1. Hay una gran diversidad de fabricantes de discos y de interfaces con los sistemas operativos. Algunos paquetes software son incapaces de sobrescribir datos en sectores protegidos o defectuosos. En ocasiones, la aplicación toma el tamaño del disco de la BIOS (Basic Input/Output System), y el valor no coincide con la capacidad real del disco, lo que deriva en una sobreescritura incompleta.
2. El fenómeno del “borde de la pista”. Cuando se escribe en un disco magnético, o cuando se efectúan sobreescrituras, las cabezas de lectura/escritura no pasan concéntricamente sobre el centro exacto de la pista del bit de datos, debido a las tolerancias en las variables eléctricas y magnéticas. Ello implica que pueden quedar bits parciales en los bordes de las pistas tras una o varias sobreescrituras, dado que el grado de precisión que presentan las cabezas lectoras de los discos comerciales comunes no proporciona una seguridad absoluta de que los bordes de las pista hayan sido completamente reescritos.



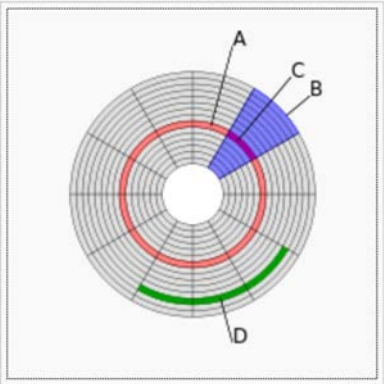
Estos restos parciales de los bits originales que permanecen en los bordes de la pista pueden recuperarse mediante técnicas microscópicas. Dependiendo del número de pistas y la remanencia magnética del material, se puede efectuar un procesado específico de la señal para reconstruir los patrones de bits de la información original.

3. Desde el punto de vista de un usuario, una unidad de almacenamiento se le presenta como una secuencia de celdas en las que se puede leer y/o escribir, así como ejecutar otras funcionalidades complementarias (tales como conocer el espacio libre o reorganizar la información). En todo soporte, existe una cantidad mínima de datos que pueden transferirse en una operación de entrada/salida entre la memoria principal de un ordenador y los dispositivos periféricos o viceversa. Así, generalmente el bloque mínimo de lectura/escritura de un disco duro es el sector, formado por un

número determinado de bytes que se puede configurar al formatear una unidad de almacenamiento. Con el fin de ocultar las peculiaridades de los dispositivos y adecuar la operativa a las necesidades de los usuarios finales y los programadores, los usuarios no trabajan con bytes o sectores de un disco sino con archivos. Un archivo o fichero informático es un conjunto ordenado de bytes que son almacenados en un dispositivo según un formato establecido (por ejemplo, concebido para almacenar textos, imágenes, o presentaciones), y que es tratado por el sistema operativo como una unidad lógica. Para poder almacenar este tipo de archivos en el dispositivo, es necesario organizar la superficie del disco mediante la creación de una estructura lógica sobre el espacio de almacenamiento físico. Esta estructura lógica, que agrupa los archivos en directorios y establece una jerarquía, se denomina Sistema de archivos. Se puede asemejar este concepto a una base de datos que contiene fundamentalmente un sector de arranque y dos tipos de entidades:

a. Los registros (descriptores que forman una tabla de contenidos del espacio de almacenamiento, la cual permite conocer el conjunto de bloques –no necesariamente contiguos- correspondientes a cada fichero, la estructura de los directorios y los derechos de acceso);

b. Los datos de usuario (el contenido útil almacenado en el sistema).



Si se elimina el registro de un archivo, como consecuencia de la ejecución de un comando de borrado del sistema operativo, no se podrán conocer los datos que identifican al archivo (como el nombre), ni se sabrá dónde está ubicado su contenido. No obstante, este contenido permanece inalterado hasta que se sobrescriban nuevos datos sobre ese espacio, y podría ser recuperado utilizando técnicas forenses o aplicaciones especializadas.

Además, como la unidad mínima de información con la que trabaja el Sistema de Archivos no es el “sector” sino el “clúster” (conjunto contiguo de sectores, en cuantía dependiente del tamaño de la unidad), se presenta otro problema, conocido como “slack cluster” o *cluster incompleto*. Este fenómeno consiste en que si el tamaño de un archivo no es múltiplo del tamaño de un clúster, se crea un área al final del último clúster que no forma parte ni del archivo ni del espacio libre del disco. Normalmente esos espacios contienen la información del archivo anterior que hubiera sido almacenado en esa ubicación, y serían vulnerables a técnicas de recuperación de datos.

VI TERMINOLOGÍA Y TIPOS DE BORRADO Y DESTRUCCIÓN DE SOPORTES

VI.1 TERMINOLOGÍA APLICABLE AL BORRADO DE DOCUMENTOS

Ante la proliferación de términos en la literatura técnica, y la diversidad de traducciones de los términos anglosajones -que sí están más consolidados-, se impondría normalizar una

terminología que permita sistematizar el análisis del proceso de eliminación de la documentación. Se refleja a continuación una propuesta de terminología aplicable a este ámbito.

Borrado de nivel 0

Remoción de los documentos empleando comandos estándar del sistema operativo para el borrado de archivos o el formateo de dispositivos o particiones. Este procedimiento no proporciona ninguna garantía frente a la revelación no autorizada de la información, ya que el sistema operativo funciona de tal manera que cuando se borra un archivo, éste no desaparece físicamente, sino que en muchas ocasiones se marca el espacio en el cual se encuentra el archivo como disponible, pero a menos de que algo nuevo se escriba en ese espacio, podría recuperarse.

Borrado de nivel 1

Equivalente al término inglés "**clearing**" o "limpieza": es la remoción de los datos o documentos sensibles de un soporte de almacenamiento de tal manera que hay seguridad de que los datos no podrán ser reconstruidos utilizando las funciones normales del sistema o programas de recuperación de archivos. Una de las formas más conocidas para realizar un borrado de nivel 1 es la **sobreescritura de datos** o *wiping,* que sustituye los datos escritos en el soporte por información aleatoria. Este proceso escribe encima de donde se "encontraba" la información, de tal forma que lo que existía anteriormente no pueda ser recuperado con las herramientas que están disponibles habitualmente en un sistema de información. Los datos aún podrían ser recuperables, pero ello requeriría técnicas especiales de laboratorio o utilidades avanzadas.

Borrado de nivel 2

Equivalente al término inglés "**sanitizing**" o "**purging**", también conocido en la literatura especializada como *purgado*, *higienización*, *sanitización* o *saneamiento*: es la remoción de datos o documentos sensibles de un dispositivo de almacenamiento con el objeto de que los datos no puedan ser reconstruidos utilizando alguna de las técnicas conocidas. Es decir, el riesgo de compromiso de la confidencialidad tras la ejecución de un borrado de nivel 2 es muy bajo o inexistente. Además de la remoción de los datos, el proceso de borrado de nivel 2 incluye la supresión manual de las indicaciones externas de que el soporte o dispositivo contuvo alguna vez datos sensibles. El borrado de nivel 2, proporcional a la sensibilidad de los datos, generalmente se efectúa antes de dejar libres de control a los dispositivos de almacenamiento. Ejemplos de borrado de nivel 2: desmagnetizar un disco, ejecutar el comando de borrado seguro del *firmware* de algunos dispositivos, o cifrar un soporte de almacenamiento con criptografía fuerte.

La difusión de soportes de almacenamiento alternativos, como las memorias de estado sólido o los discos duros basados en memorias flash, han conducido a que en algunos tipos de dispositivos no se pueda emplear la desmagnetización para borrar los datos.

Destrucción

El soporte de almacenamiento es físicamente destruido, lo que impide su reutilización. Su efectividad puede variar dependiendo de la densidad de grabación del soporte y/o de la técnica de destrucción, pero cuando se utilizan los métodos apropiados, la destrucción física es considerada como el método más seguro.

Se incluyen entre los métodos de destrucción la pulverización, la fusión y la incineración. Se realizan normalmente en una instalación externa de destrucción de metales o con incineración con licencia para las capacidades concretas de realizar estas actividades con eficacia, seguridad y protección.

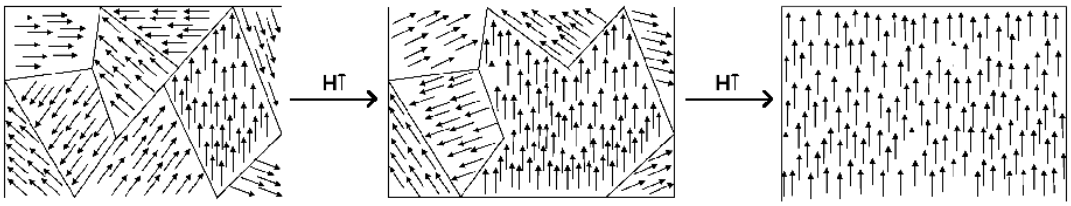
VI.2 CONSIDERACIONES EN RELACIÓN A LOS SOPORTES MAGNÉTICOS

Para facilitar la interpretación del siguiente apartado, vamos a efectuar previamente una sucinta aproximación a la física subyacente a la grabación en soportes magnéticos, dada su difusión como dispositivos de almacenamiento.

Los soportes magnéticos son muy sensibles a su historia magnética previa; una propiedad denominada "histéresis". El ferromagnetismo es un fenómeno físico de determinados mate-

riales (como hierro, cobalto o níquel) en el que se produce espontáneamente un ordenamiento microscópico de los espines de los electrones, el cual conduce a la formación de regiones de alineamiento magnético llamadas dominios. Estos están separados por superficies conocidas como paredes de *Bloch*.

Como se ve en la gráfica anterior, de manera global los dominios se cancelan mutuamente en condiciones normales, debido a que están orientados de forma aleatoria entre ellos, con lo cual el material queda sin magnetización neta. La aplicación de un campo magnético externo, por ejemplo con un solenoide, origina un mayor grado de alineamiento de los momentos magnéticos de los dominios. Si se va incrementando gradualmente la intensidad del campo externo, aquellos dominios en los que los dipolos tienen la misma orientación que el campo magnético inductor aumentan su tamaño, hasta llegar a la eventual desaparición de las paredes de Bloch, dando lugar a un "monodominio" (fenómeno conocido también como saturación magnética).



En definitiva, en los materiales ferromagnéticos existe de manera espontánea un alto grado de magnetización dentro de los dominios individuales, pero en ausencia de campos magnéticos externos, esos dominios están orientados de forma aleatoria y se cancela la magnetización neta. No obstante, todos los materiales ferromagnéticos presentan un temperatura máxima, donde desaparecen las propiedades ferromagnéticas como resultado de la agitación térmica. Esta temperatura se denomina temperatura de Curie, en honor al físico francés Pierre Curie que la descubrió. Por encima de dicha temperatura, los ferromagnetos se comportan como sustancias paramagnéticas (aquellas en las que los momentos magnéticos están orientados de manera completamente aleatoria, sin que existan dominios de alineamiento magnético a nivel microscópico). Los materiales ferromagnéticos son aquellos que tienen una temperatura de Curie muy alta (por ejemplo, 1388ºK para el Cobalto y 1043ºK para el Hierro).

La principal implicación práctica del ferromagnetismo en el ámbito del almacenamiento de información es que los materiales ferromagnéticos se caracterizan por su tendencia a permanecer magnetizados en cierta medida tras su exposición a un campo magnético externo. Esta propensión de los materiales ferromagnéticos a ser condicionados por su "historial magnético" previo se denomina histéresis, y es la propiedad física que sirve de base a las técnicas de grabación en soportes magnéticos, como los discos duros. En física se define la histéresis como "la tendencia de un material a conservar una de sus propiedades en ausencia del estímulo que la ha generado", y es un fenómeno que aparece en áreas diferentes al electromagnetismo, como el comportamiento de cuerpos elásticos.

La fracción de la magnetización que es retenida cuando se elimina el campo de generación externa, se llama **remanencia** del material. Otro concepto ligado al anterior es la coercitividad, que es la intensidad del campo magnético que se debe aplicar a ese material para reducir su magnetización a cero después de que la muestra ha sido magnetizada hasta saturación. Por lo tanto, la **coercitividad mide la resistencia de un material ferromagnético a ser desmagnetizado**.

Las características descritas de memoria magnética que presentan compuestos como los óxidos de hierro y cromo, entre otros, los hacen apropiados para el almacenamiento de datos en sistemas informáticos.

VI.3 TÉCNICAS ESPECÍFICAS DE BORRADO SEGURO DE DOCUMENTOS Y DESTRUCCIÓN DE SOPORTES

A continuación se describen una serie de técnicas específicas de borrado seguro, orientadas preferentemente a soportes de almacenamiento de tipo magnético y de estado sólido, dado que son los tipos de soportes actuales más adecuados para la conservación de documentos electrónicos. Aun así, se hace también mención a sistemas de destrucción de soportes de tipo óptico.

A. Sobreescritura

Consiste en reemplazar los datos almacenados en todas las áreas de un dispositivo de almacenamiento (incluyendo las áreas ocultas - como HPA y DCO - y los bloques marcados como defectuosos) por un patrón binario de información sin sentido. El método puede indicar que es necesario efectuar al final una pasada de comprobación. Eso permite, además de comprobar que los datos que deberían haberse grabado se han almacenado correctamente, asegurar el correcto funcionamiento de todos los sectores sobre los que se realiza la comprobación.

Como mínimo, este método evitará que los datos originales sean recuperados utilizando simplemente las funciones habituales del sistema operativo.

La eficacia de este método depende el número de ciclos de sobreescritura, y de las funcionalidades de verificación del software para asegurar que la sobreescritura se efectúa sobre todo el área accesible de almacenamiento del soporte.

A pesar de lo que cabría pensar a priori, cualquier sobreescritura de los datos grabados en un soporte, sustituyéndolos por otros valores, no garantiza la imposibilidad de recuperar la información original. Existen procedimientos avanzados que mediante sofisticadas técnicas forenses (las cuales consisten en analizar el valor magnético de la posición de memoria del disco) permiten saber, con una precisión bastante grande, la información que existía originalmente en dicha posición del soporte. En consecuencia, la información espuria que se debe sobrescribir no puede ser cualquiera, sino que tiene que ser capaz de generar tal desorden en el soporte magnético que la recuperación de los datos originales sea prácticamente imposible.

Los modernos sistemas de borrado seguro de archivos consisten precisamente en eso: en algoritmos de escritura que buscan que el magnetismo residual que queda en el disco no guarde ninguna relación con la información original.

La sobreescritura es generalmente un método aceptable de borrado de nivel 1, pero dado que la sobreescritura se realiza accediendo al contenido de los dispositivos y modificando los valores almacenados, no se puede utilizar este método en aquellos soportes que están dañados ni en los que no son regrabables, como los CD y DVD de solo escritura.

Para aquellos soportes que estén dañados, o bien no sean susceptibles de sobreescritura, los dispositivos de almacenamiento deberán ser desmagnetizados o destruidos.

Por otro lado, los métodos de borrado por sobreescritura presentan el inconveniente de su elevado tiempo de ejecución, dependiente del número de ciclos de sobreescritura del algoritmo.

Dentro de las técnicas de borrado lógico, nos encontramos varios mecanismos y estándares, de los que destacaremos:

U.S. Navy Staff Office Publication, NAVSO P-5239-2

Este procedimiento efectúa tres sobreescrituras: la primera compuesta por un patrón de un único byte, la segunda por el byte complementario, y la tercera por un patrón generado de manera pseudoaleatoria. Finalmente se lee el área de datos para verificar la correcta ejecución de la sobreescritura.

El algoritmo de Bruce Schneier

Se basa en un generador de números aleatorios criptográficamente seguro, que es empleado por el algoritmo para sobrescribir 7 veces la información. En primer lugar se escribe un patrón compuesto íntegramente de “1”s, luego se aplica un patrón de “0”s, y por último realiza cinco sobreescrituras con patrones pseudoaleatorios. Es **muy seguro**, pero es un método relativamente lento debido a la generación de números aleatorios seguros. A cambio exige menos escrituras que el método de Peter Gutmann.

El algoritmo de Peter Gutmann

El método fue creado por Peter Gutmann en 1996. Es considerado **el método de borrado de datos más seguro que existe** y puede ser utilizado para todos los soportes que contienen información sensible.

Este procedimiento efectúa, combinando sobreescrituras de las descritas anteriormente (patrón predeterminado de secuencia de bytes, todo "1"s, todo "0"s, patrones pseudoaleatorios) hasta 35 pasadas por el disco. Se compone de 35 patrones especialmente seleccionados para maximizar la entropía del dispositivo, incluyendo patrones específicos para distintos tipos de discos, de tal manera que sea extremadamente difícil recuperar el contenido original.

Entrando más en detalle en el algoritmo:

- En la primera etapa, la sobreescritura del soporte se realiza grabando valores aleatorios cuatro veces sobre cada sector.
- Seguidamente se sobrescribirá todo el soporte aplicando valores pseudoaleatorios sobre cada sector, y se repitirá este proceso un total de veintisiete pasadas.
- Para terminar, se aplicarán cuatro pasadas de valores aleatorios sobre cada sector.

En la actualidad los discos duros ya no utilizan los métodos de codificación para los cuales fue diseñado el Método de Gutmann, y por otro lado los discos cuentan con una mayor densidad de datos sobre la superficie. Todo ello implica que el número de sobreescrituras necesarias para garantizar un borrado seguro ha disminuido considerablemente con respecto al año en que se ideó este método (1996).

Gutmann parcial (5 pasadas)

Este método es un subconjunto del método Gutmann completo (35 rondas). Toma los 5 patrones más eficaces del método anterior y los aplica secuencialmente. **Es seguro** y se puede utilizar para los documentos cuya naturaleza no sea reservada o confidencial.

Estándar OTAN

En este método se sobrescribe un archivo 7 veces. Las primeras seis pasadas se basan en la sobreescritura con valores fijos alternativos entre cada pasada: (0x00) y (0xff). La última pasada aplica un patrón de sobreescritura pseudoaleatorio.

Es seguro y se puede utilizar para los documentos cuya naturaleza no sea reservada o confidencial.

B. Comando "Secure Erase" en firmware

Los discos ATA tienen incorporado, como parte del estándar, un comando firmware de borrado seguro mediante sobreescritura. Este comando se ejecuta notablemente más rápido que los intentos de reescritura mediante el interfaz nativo de lectura y escritura. Hay dos opciones: "borrado normal" (que reemplaza el contenido por "todo 0's" o "todo 1's") y "borrado mejorado" (cuya implementación es dependiente del fabricante). El comando de borrado seguro no está definido en el estándar SCSI (sólo existe un comando opcional y no se contempla en la certificación de dispositivos), por lo que el borrado mediante comando de firmware no aplica a medios con un interfaz SCSI.

La guía NIST 800-88 del gobierno de los EE.UU. considera el uso del comando "secure erasure" como un medio válido de borrado de nivel 2, únicamente para los discos ATA.

C. Desmagnetización

Este procedimiento consiste en la exposición de los soportes de almacenamiento a un campo magnético suficientemente potente para modificar la polaridad de las partículas magnéticas, proceso que elimina los datos almacenados en el dispositivo e impide la recuperación de los mismos. La eficacia de este método depende de la fuerza relativa del campo magnético generado por el dispositivo desmagnetizador en relación a las propiedades de resistencia al campo magnético (o la "coercitividad") del soporte magnético.

Este método es válido para la destrucción de datos de los dispositivos magnéticos, como por ejemplo los discos duros o cartuchos de cinta . Cada dispositivo, según su tamaño, forma y

el tipo de soporte magnético de que se trate, necesita de una potencia específica para asegurar la completa polarización de todas las partículas. Por consiguiente, es necesario asegurarse de que el equipo desmagnetizador es adecuado para el tipo de soporte y que el campo magnético va a incidir sobre la capa magnética del medio sin que ningún elemento como la carcasa impida el acceso del campo polarizador a toda la superficie magnética del soporte.

La cinta magnética y los discos duros de generaciones anteriores pueden ser borrados con desmagnetizadores de relativa baja potencia, mientras que los discos duros modernos requieren desmagnetizadores extremadamente potentes. El motivo es que los discos duros modernos están diseñados con aleaciones especiales que tienen una resistencia muy elevada al cambio magnético, lo que ha permitido que los fabricantes disminuyan las regiones magnéticas del disco para obtener mayores densidades.

Los inconvenientes que presenta este método son:

- Los dispositivos deben trasladarse al lugar donde se encuentre el desmagnetizador, lo que implica unos costes de transporte y el aseguramiento de la cadena de custodia.
- Tras el proceso, estos dejan de funcionar correctamente y por tanto requieren de un reciclado que sea respetuoso con el medio ambiente.
- Para comprobar que todos los datos han sido borrados completamente es necesario acceder a los dispositivos. Al no funcionar correctamente, este acceso no es posible, lo que dificulta la certificación del proceso.
- Es recomendable analizar el campo aplicado para desmagnetizar cada dispositivo. En ocasiones se opta por aplicar la máxima potencia, desperdiciando energía de forma innecesaria.
- Se han introducido en el mercado unidades de almacenamiento “híbridas” que incluyen una caché de memoria Flash en discos duros magnéticos, para aumentar su rendimiento. La desmagnetización no afectaría a los datos residentes en esos chips de memoria en semiconductor. Los datos en esos semiconductores no volátiles deberían eliminarse empleando otras técnicas.
- Según indica el documento “Tutorial on Disk Drive Sanitization” (ver bibliografía) del año 2008: “Las futuras generaciones de medios de grabación magnética usarán discos de alta coercitividad magnética para conseguir densidades de grabación superiores a 3.500 Gigabits por centímetro cuadrado. Estos dispositivos utilizarán un haz de luz láser en la cabeza de escritura magnética del disco duro, para elevar la temperatura de un punto del medio magnético, a fin de disminuir la coercitividad magnética hasta que sea posible que el elemento de escritura pueda grabar un bit en el medio de alta coercitividad magnética. Para las unidades de disco que usen esta tecnología de grabación magnética asistida por calor, el campo desmagnetizador requerido para borrar el disco a temperaturas ambiente puede ser inviable. En este caso, el soporte debería ser destruido físicamente.”

  En el año 2012 se rompió la barrera de densidad de grabación señalada, ya que se alcanzaron en algunos discos comerciales magnéticos densidades superiores a 6.000 Gigabits por centímetro cuadrado. La evolución tecnológica experimentada en los últimos años conlleva la necesidad de aplicar un procedimiento de Destrucción en los discos magnéticos, dado que la desmagnetización resulta inviable, salvo en los disco de menor densidad.

D. Destrucción física

El objetivo de la destrucción física es la inutilización del soporte que almacena la información en el dispositivo para evitar la posibilidad de recuperación posterior de los datos. Existen diferentes tipos de técnicas y procedimientos para la destrucción de soportes de almacenamiento, que de acuerdo con la “Guía sobre almacenamiento y borrado seguro de información” de INTECO, se pueden clasificar en dos grupos:

Desintegración, pulverización, fusión e incineración

Son métodos diseñados para destruir por completo los soportes de almacenamiento. Estos métodos suelen llevarse a cabo en una destructora de metal o en una planta de inci-

neración autorizada, con las capacidades específicas para realizar estas actividades de manera eficaz, segura y sin peligro.

- La desintegración se consigue mediante el uso de un mecanismo de corte o triturado no uniforme (como unas cuchillas rotatorias en un contenedor cerrado), que reduce el dispositivo a pedazos de tamaño y forma aleatorios.
- La incineración puede destruir completamente todos los dispositivos, y a todos los niveles de seguridad. Debe llevarse a cabo en incineradoras que hayan sido aprobadas en cuanto a impacto medioambiental, para plásticos y otros materiales.
- La fusión es un proceso diferente mediante el cual el material se calienta a una temperatura que es menor que el punto de encendido pero suficientemente alta para derretirlo, pudiendo ser un medio efectivo de destrucción para los discos duros.
- La pulverización es un proceso que consiste en machacar el material. Puede ser efectivo para discos duros, siempre que la pulverización se haga de tal manera que las superficies del disco no puedan ser separadas del resto del material destruido para su análisis en laboratorio.

Triturado

Es un sistema de destrucción que se efectúa reduciendo el soporte a pedazos minúsculos de tamaño y forma uniformes. El uso de trituradoras está típicamente limitado a soportes de grosor fino, como CDs o DVDs.

Las trituradoras de papel se pueden utilizar para destruir los soportes de almacenamiento flexibles. El tamaño del fragmento de la basura debe ser suficientemente pequeño para que haya una seguridad razonable, en proporción a la confidencialidad de los datos, de que no pueden ser reconstruidos. Los soportes ópticos de almacenamiento (CD, DVD, magneto-ópticos), deben ser destruidos por pulverización, triturado de corte transversal o incineración. Cuando el material se desintegra o desmenuza, todos los residuos se reducen a cuadrados de cinco milímetros (5mm) de lado.

Como todo proceso de borrado seguro de datos, su correcta realización implica la imposibilidad de recuperación posterior por ningún medio conocido en la actualidad. Así, en el caso de los discos duros se deberá asegurar que los platos internos del disco han sido destruidos eficazmente. Los métodos de destrucción física pueden llegar a ser completamente seguros en cuanto a la destrucción real de los datos, pero presentan algunos inconvenientes, como son:

- Conllevan la utilización de métodos industriales de destrucción distintos para cada soporte.
- Obligan a un transporte de los dispositivos a un centro de reciclaje adecuado, obligando a extremar las medidas de custodia para asegurar el control de los dispositivos.
- Los residuos generados deben ser tratados adecuadamente.
- La certificación de la operación de destrucción es compleja, ya que no es posible acceder a los dispositivos para confirmar que la información ha sido eliminada y se deben hacer comprobaciones manuales, como fotografías que certifiquen que el dispositivo ha sido eliminado.

E. Criptografía y Borrado Criptográfico

Muchos fabricantes de dispositivos han sacado al mercado en los últimos años dispositivos con cifrado integrado y capacidades de control de acceso, también conocidos como Dispositivos con AutoCifrado (SED). Los SED (“self encrypting devices”) disponen de cifrado permanente que reduce sustancialmente la probabilidad de que datos sin cifrar se retengan inadvertidamente en el dispositivo. El usuario no puede desactivar las capacidades de cifrado, asegurando así que todos los datos están cifrados.

Un beneficio adicional de los SEDs es que permiten acoplar fuertemente el controlador y las áreas de almacenamiento, de manera que el dispositivo puede acceder directamente a la localización en la que se almacenan las claves criptográficas, mientras que las soluciones que dependen sólo del interfaz de acceso mediante software no pueden acceder directamente a dichas áreas.

Los SEDs cifran generalmente todas las áreas accesibles por el usuario, con la excepción potencial de algunas áreas claramente identificadas que están dedicadas al almacenamiento de aplicaciones de pre-arranque y sus datos asociados.

El fundamento del borrado criptográfico es que aprovecha el cifrado para implementar el borrado de los datos mediante la eliminación de la clave de cifrado del dispositivo. Esto implica que sólo quedarán en el soporte de almacenamiento los datos cifrados, impidiendo su recuperación sin la clave, y por tanto efectuando un borrado seguro (siempre que se use criptografía fuerte, por ejemplo AES de 256 bits).

Una ventaja del borrado criptográfico es que permite realizar una limpieza de alta seguridad de manera mucho más rápida que con otras técnicas. Además, este método puede ser utilizado como un suplemento a otras aproximaciones de borrado seguro.

Para asegurar la eficacia de este método, todas las localizaciones del soporte en las que se almacene la clave deben ser directamente accesibles para su borrado, usando una de las técnicas de borrado seguro descritas. Además, deberá asegurarse que todas las copias de las claves de cifrado serán eliminadas.

El principal inconveniente de esta técnica, cuya seguridad radica en la implementación del proceso de borrado de la clave criptográfica por parte del fabricante, reside en su falta de verificabilidad. Ello es debido a que los proveedores no suelen proporcionar información detallada sobre el firmware del dispositivo y la tecnología utilizada para fabricar el controlador (la cual es necesaria para comprender las cuestiones de permanencia en memoria de residuos de datos). Los fabricantes de dispositivos son reacios a proporcionar este tipo de información y, aunque lo hicieran, cada modelo de dispositivo requeriría una verificación independiente, lo que supone un proceso intensivo en tiempo y recursos.

Sin embargo, existe una aproximación híbrida denominada “SAFE” (*Scramble and Finally Erase*), alternativa a las puramente criptográficas, y que proporciona tanto velocidad como verificabilidad, ya que no requiere confiar en las soluciones de borrado criptográfico que incorpora el firmware de cada fabricante. SAFE sigue un proceso en dos pasos: en primer lugar, elimina el almacén de la clave, y a continuación ejecuta un borrado sobre cada página física de un dispositivo. Una vez el borrado ha concluido, el dispositivo entra en un estado “verificable” (en el que se puede comprobar que no permanece ningún resto de la información original).

F. Caso particular de las memorias Flash

Las memorias Flash no son soportes magnéticos, sino dispositivos de estado sólido, y se basan en el uso de puertas lógicas. Aunque no existen estándares específicos para el borrado de memorias flash, se pueden emplear todas las técnicas descritas anteriormente, a excepción de la desmagnetización. También se debe realizar la advertencia de que las memorias flash representan un desafío para algunos modelos de trituradores o pulverizadoras, debido a la dureza de los componentes.

Las memorias flash difieren respecto a los discos duros tanto en la tecnología que usan para almacenar datos (dispositivos de estado sólido frente a discos magnéticos) como en los algoritmos que usan para gestionar y acceder a los datos. Las memorias flash usan una capa de indirección entre las direcciones de bloques lógicos (LBA) que los ordenadores utilizan para acceder a los datos y las direcciones flash en bruto que identifican al almacenamiento físico. La capa de indirección mejora el rendimiento de la memoria flash y su fiabilidad, al ocultar el peculiar interfaz de la memoria flash y gestionar su limitado tiempo de vida, pero también puede producir copias de los datos que son invisibles al usuario pero un atacante sofisticado puede recuperar.

Las memorias flash están divididas en bloques y páginas. Las operaciones programáticas aplican a páginas y sólo pueden cambiar 1s a 0s (o a la inversa). Las operaciones de borrado aplican a bloques y pueden poner a 1 (o 0) todos los bits de un bloque. Una capa denominada “Flash Translation Layer” (FTL) gestiona el mapeo entre las direcciones de bloques lógicos que son visibles a través de los interfaces externos de la memoria y las páginas físicas de la memoria flash. Debido al desajuste de granularidad entre las operaciones de borrado y las operaciones programáticas en flash, no se puede realizar una actualización in situ de un

sector. En su lugar, para modificar un sector, el FTL escribirá los nuevos contenidos del sector en otra localización y actualizará el mapeo, de manera que los nuevos datos aparecen en la dirección de bloque lógico objetivo. En consecuencia, la versión antigua de los datos permanece en forma digital en la memoria flash, constituyendo "residuos digitales".

Como las actualizaciones in situ no son posibles en las memorias flash, es posible que las técnicas de borrado basadas en sobreescrituras que funcionan bien en los discos duros magnéticos no funcionen adecuadamente en las memorias flash. Estas técnicas asumen que sobrescribir una porción del espacio de direcciones redunda en una sobreescritura del mismo soporte físico que almacenaba los datos originales. Sin embargo, sobrescribir datos en una memoria flash provoca un borrado lógico (es decir, los datos no son recuperables a través de interfaz del dispositivo) pero no un borrado digital de la información.

El principal estudio de referencia en relación al borrado seguro de memorias flash ("Reliably Erasing Data From Flash-Based Solid State Drives", de Wei, Grupp y Spada), llega a cuatro conclusiones:

1. Los comandos que incorporan las memorias flash son efectivos, pero algunos fabricantes los implementan de manera incorrecta (se han detectado "bugs"). De acuerdo con la guía NIST 800-88 del gobierno de los EE.UU., mientras que el uso de un comando "borrado seguro" en firmware se considera un método de borrado de nivel 2 en los discos ATA, sólo se puede considerar como un método de borrado de nivel 1 en los discos basados en Flash.

2. Sobrescribir el espacio completo de direcciones de un soporte Flash es generalmente (aunque no siempre) suficiente para efectuar un borrado seguro del dispositivo. A pesar de que la sobreescritura es efectiva en un amplio conjunto de dispositivos, no se puede considerar un sistema universal para las memorias flash, ya que en algunos dispositivos comerciales se detectó que permanecía el 1% de los datos tras 20 sobreescrituras.

3. Ninguna de las técnicas actualmente existentes para el borrado de ficheros individuales en discos duros magnéticos son eficientes en memorias Flash, lo que conlleva la necesidad de llevar a cabo una limpieza completa del dispositivo.

4. Las memorias flash más recientes incorporan cifrado de datos por defecto, porque proporciona seguridad mejorada. Además, el cifrado también provee un medio rápido para borrar el dispositivo, ya que eliminar la clave de cifrado será en teoría suficiente para convertir los datos del dispositivo en irrecuperables. La desventaja de esta aproximación es que confía en el controlador para borrar adecuadamente la localización de almacenamiento interna que alberga la clave de cifrado y otros valores criptográficos relacionados con la misma. Debido a la existencia de "bugs" o fallos de implementación, es indebidamente optimista asumir que los fabricantes de memorias flash borrarán adecuadamente el almacén de la clave.

VII PROCESO DE ELIMINACIÓN DE DOCUMENTOS ELECTRÓNICOS

El proceso de eliminación de documentos electrónicos forma parte de la política de gestión documental de la organización. En este sentido será necesario definir los métodos específicos de borrado y los de destrucción de soportes de almacenamiento a emplear, en función de una serie de escenarios, que contemplen:

- El nivel de confidencialidad de la información (dimensión del ENS), el nivel de seguridad del fichero de datos según la Ley Orgánica de Protección de Datos, el tipo de soporte, el propósito de reutilizarlo o no, el tipo de control de la gestión (interno o externo) de los soportes de almacenamiento, y el alcance de la eliminación (parcial o total).

Así pues, se incluirán en este apartado, con una pretensión de exhaustividad, todas las situaciones o escenarios de eliminación de documentación electrónica que pueden aparecer en la gestión documental, y se indicará para cada caso el método de borrado mínimo recomendado. En la prescripción del método de borrado se ha aplicado el principio de proporcionalidad, modulando el adecuado equilibrio entre la importancia del documento y las medidas de seguridad.

VII.1 FACTORES CONDICIONANTES

Los aspectos que se han tenido en cuenta a la hora de determinar los procedimientos de borrado recomendados para los documentos electrónicos, son los siguientes:

Nivel de confidencialidad de la información recogida en el documento

- De acuerdo con el Esquema Nacional de Seguridad, "*La determinación de la categoría de un sistema se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas*".
- Asimismo, con arreglo al ENS, "*A fin de poder determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, y de poder establecer la categoría del sistema, se tendrán en cuenta las siguientes dimensiones de la seguridad:*
  - *Disponibilidad.*
  - *Autenticidad.*
  - *Integridad.*
  - *Confidencialidad.*
  - *Trazabilidad*."
- Las posibles categorías de los sistemas de información son:
  - Bajo.
  - Medio.
  - Alto.
- El concepto de categoría del Esquema Nacional de Seguridad aplica a los sistemas de información, pero una de las dimensiones de la seguridad (la confidencialidad) es inherente a los documentos y puede deducirse de su contenido, si bien puede ser también modulada posteriormente por el servicio al que pertenezca.
- Hay que tener en cuenta también que podemos encontrar sistemas no afectados por el ENS ("sistemas no relacionados con el ejercicio de derechos ni con el cumplimiento de deberes por medios electrónicos ni con el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, de acuerdo con lo previsto en la Ley 11/2007, de 22 de junio.").

Nivel LOPD

- La LOPD distingue, en función de la naturaleza de los datos personales, tres niveles de protección para los ficheros de datos (bajo, medio y alto), que requieren diferentes medidas de seguridad.

Nivel de clasificación de la información

- Información clasificada: es aquella información a la que se le ha asignado una clasificación de seguridad (Centro Nacional de Inteligencia).
- Documentación clasificada: cualquier soporte que contenga información clasificada registrada en cualquier formato físico (CNI).
- Grados de clasificación de seguridad (de mayor a menor):
  - Secreto
  - Reservado
  - Confidencial
  - Difusión limitada
- Materias clasificadas: aquellas calificadas con la categoría de secreta o reservada.

– Materias objeto de reserva interna: aquellas calificadas con las categorías de confidencial y difusión limitada.
– Materias no restringidas: aquellas que no poseen ninguna de las clasificaciones presentadas anteriormente.
– Normativa aplicable:
    - Ley 9/1968, de 5 de abril, sobre secretos oficiales.
    - Norma “NS/04-Seguridad de la Información” del Centro Nacional de Inteligencia.

Los soportes de almacenamiento

– Se deben contemplar las siguientes cuestiones:
    - La naturaleza del soporte de almacenamiento, que puede ser:
        - Magnético
            - Disco duro
            - Cinta
        - Óptico
        - SSD (Flash)
    - El tipo de acceso al soporte:
        - Acceso aleatorio
        - Acceso secuencial
    - El uso de técnicas de *deduplicación*. La deduplicación de datos es una técnica, transparente a los usuarios, que persigue la eliminación de datos redundantes. En esta técnica, se analiza el flujo de información entrante y se compara con el historial previo, a fin de buscar secuencias que coincidan con otra anterior ya almacenada. En ese caso, en vez de guardarla nuevamente, se reemplazará (en línea o mediante un procesamiento posterior) la secuencia entrante por una referencia a la primera versión almacenada.
    - La portabilidad:
        - Dispositivos extraíbles (almacenamiento local)
        - Dispositivos fijos (sistemas de almacenamiento o almacenamiento en red)
    - La existencia de copias o réplicas de los documentos en distintos soportes.
    - Asimismo, es importante tener en cuenta si se pretende reutilizar o no el soporte de almacenamiento tras la aplicación del procedimiento de borrado.

Tipo de gestión de los sistemas de información

    - Interna
    - Externa (encomendada a un contratista o a otra organización)

Alcance de la eliminación

    - Parcial (si afecta a una parte del soporte de almacenamiento, por ejemplo a un fichero o conjunto de ficheros).
    - Total (si afecta a todo el soporte de almacenamiento o sistema de almacenamiento).

A partir de estas variables, se determinará el **tipo de eliminación** mínimo recomendado:

– Tipos de borrado (en relación al soporte de almacenamiento):
    - Borrado de nivel 0.

- Borrado seguro:
  - Borrado de nivel 1 (equivalente al concepto de *clearing*).
  - Borrado de nivel 2 (equivalente al concepto de *purging* o *sanitization*).
  - Destrucción del soporte.

– Técnicas y métodos de borrado:

- Borrado de nivel 0:
  - Marcado en un soporte de almacenamiento de los sectores ocupados por un fichero como espacio libre.
  - Eliminación de la referencia al fichero en la tabla de particiones.
- Borrado seguro:
  - Sobreescritura con un número reducido de pasadas (borrado de nivel 1).
  - Sobreescritura con un número alto de pasadas (borrado de nivel 2).
  - Desmagnetización (borrado de nivel 2).
  - Borrado por firmware (borrado de nivel 2).
  - Borrado de tipo criptográfico (borrado de nivel 2).
  - Destrucción física del soporte:
    - Desintegración
    - Pulverización
    - Fusión
    - Incineración
    - Triturado

– Merece mención aparte la eliminación lógica (generalmente a nivel de aplicación de gestión documental), que implica necesariamente y como mínimo un borrado de nivel 0.

VII.2 MOTIVACIÓN DEL BORRADO O ELIMINACIÓN

Se distinguen, a modo de ejemplo, una serie de contextos o escenarios en los que podrá tener lugar la eliminación de un conjunto de documentos electrónicos. Las motivaciones pueden ser, además, concurrentes:

– Por un acuerdo de eliminación.

- Si se ha dictado un acuerdo de eliminación.

– Por cambio de formato.

- Se produce un cambio de formato de la documentación por haber realizado una copia electrónica auténtica. Si se han realizado varias copias a distintos formatos (por ejemplo, una a PDF y otra a PDF/A), podría eliminarse alguna de las copias auténticas.

– Por fallo en el soporte de almacenamiento y su sustitución.

- Un soporte falla y debe ser retirado para su sustitución.

– Por transferencia entre archivos.

- La documentación electrónica se elimina una vez se ha transferido al archivo de destino.

– Por cambio de soporte de almacenamiento.

- Por obsolescencia del soporte, o por migración entre sistemas de almacenamiento.

VII.3 TABLA DE DECISIÓN DEL PROCESO DE BORRADO

A continuación se detallan las tablas de decisión del proceso de borrado en función de los factores condicionantes descritos anteriormente.

Es preciso efectuar las siguientes consideraciones para la correcta aplicación de este instrumento:

- La variable correspondiente a la columna "Confidencialidad / LOPD" corresponde al mayor de los dos siguientes valores:
  - Nivel de confidencialidad de la información (considerada como dimensión de seguridad regulada en el ENS).
  - Nivel LOPD.
- No se ha incluido ninguna columna correspondiente al alcance del borrado (parcial o total), por cuanto éste no afecta al método de borrado recomendado sino a su extensión.
- No se ha contemplado si el soporte de almacenamiento emplea tecnologías de deduplicación porque consideramos que no afecta al método de borrado recomendado, sino a la eventual necesidad de complementar estos métodos con algoritmos específicos (ver artículo "Memory Efficient Sanitization of a Deduplicated Storage System", citado en la bibliografía).
- Estas tablas se deben aplicar para todas y cada una de las copias de los documentos a borrar.
- En el nivel de borrado 2 (equivalente a *purging* o *sanitization*) se ha indicado la técnica más común, si bien también es posible aplicar el borrado por firmware o criptográfico, cuando fuera posible.
- Todos los métodos indicados en las tablas deberán ir acompañados de un proceso posterior de validación de la correcta ejecución de la técnica de borrado.
- Sería recomendable, en la medida de lo posible, separar físicamente los entornos de almacenamiento en función del nivel de confidencialidad o nivel LOPD de la información. Esta medida facilitaría la aplicación de los distintos métodos de borrado propuestos.
- Cuando la técnica de borrado propuesta es “SOBREESCRITURA”, se indica un número entre paréntesis, el cual se corresponde con el número mínimo de pasadas de sobreescritura del algoritmo.

Tabla 1. Gestión interna con reutilización del soporte de almacenamiento.

EN CUANTO A LAS CONDICIONES			EN CUANTO AL SOPORTE				MÉTODO DE BORRADO MÍNIMO RECOMENDADO		
Gestión de los sistemas de información	Confidencialidad / LOPD	Condiciones de uso	Naturaleza	Tipo	Tipo de acceso	Dispositivo	Nivel de borrado	Técnicas de borrado	Observaciones
INTERNA	NIVEL BÁSICO	REUTILIZACIÓN	MAGNÉTICO	DISCO	ALEATORIO	EXTRAÍBLE	NIVEL 0		
			MAGNÉTICO	DISCO	ALEATORIO	SISTEMA	NIVEL 0		
			MAGNÉTICO	CINTA	SECUENCIAL	EXTRAÍBLE	NIVEL 0		
			ÓPTICO	DISCO	ALEATORIO	EXTRAÍBLE	DESTRUCCIÓN		1
			SSD	DISCO	ALEATORIO	SISTEMA	NIVEL 0		
			SSD	MEMORIA	ALEATORIO	EXTRAÍBLE	NIVEL 0		
Gestión de los sistemas de información	Confidencialidad / LOPD	Condiciones de uso	Naturaleza	Tipo	Tipo de acceso	Dispositivo	Nivel de borrado	Técnicas de borrado	Observaciones
INTERNA	NIVEL MEDIO	REUTILIZACIÓN	MAGNÉTICO	DISCO	ALEATORIO	EXTRAÍBLE	NIVEL 1	SOBREESCRITURA (3)	
			MAGNÉTICO	DISCO	ALEATORIO	SISTEMA	NIVEL 1	SOBREESCRITURA (3)	
			MAGNÉTICO	CINTA	SECUENCIAL	EXTRAÍBLE	NIVEL 2	DESMAGNETIZACIÓN	2
			ÓPTICO	DISCO	ALEATORIO	EXTRAÍBLE	DESTRUCCIÓN		1
			SSD	DISCO	ALEATORIO	SISTEMA	NIVEL 1	SOBREESCRITURA (3)	
			SSD	MEMORIA	ALEATORIO	EXTRAÍBLE	NIVEL 1	SOBREESCRITURA (3)	
Gestión de los sistemas de información	Confidencialidad / LOPD	Condiciones de uso	Naturaleza	Tipo	Tipo de acceso	Dispositivo	Nivel de borrado	Técnicas de borrado	Observaciones
INTERNA	NIVEL ALTO	REUTILIZACIÓN	MAGNÉTICO	DISCO	ALEATORIO	EXTRAÍBLE	NIVEL 2	SOBREESCRITURA (7)	
			MAGNÉTICO	DISCO	ALEATORIO	SISTEMA	NIVEL 2	SOBREESCRITURA (7)	
			MAGNÉTICO	CINTA	SECUENCIAL	EXTRAÍBLE	NIVEL 2	DESMAGNETIZACIÓN	2
			ÓPTICO	DISCO	ALEATORIO	EXTRAÍBLE	DESTRUCCIÓN		1
			SSD	DISCO	ALEATORIO	SISTEMA	NIVEL 2	SOBREESCRITURA (7)	
			SSD	MEMORIA	ALEATORIO	EXTRAÍBLE	NIVEL 2	SOBREESCRITURA (7)	

1 Se recomienda la destrucción de los soportes ópticos basándonos en las guías NIST 880-88 y ITSG-06, porque en la actualidad la sobreescritura no está indicada para el borrado de medios de esta naturaleza. Además a este tipo de soporte no es posible aplicarles la desmagnetización. Esto además podría requerir una copia de otros datos o documentos que se almacenen en el soporte y que, al no borrarse, deban conservarse.

2 Se recomienda la desmagnetización de los soportes de cinta por la rapidez y eficiencia de este método frente a una sobreescritura. En este caso habrá que contemplar el copiado a otro soporte de otros datos o documentos que se encuentren en el mismo soporte y que deban conservarse.

Tabla 2. Gestión interna con cambio del soporte de almacenamiento.

EN CUANTO A LAS CONDICIONES			EN CUANTO AL SOPORTE				MÉTODO DE BORRADO MÍNIMO RECOMENDADO		
Gestión de los sistemas de información	Confidencialidad / LOPD	Condiciones de uso	Naturaleza	Tipo	Tipo de acceso	Dispositivo	Nivel de borrado	Técnicas de borrado	Observaciones
INTERNA	NIVEL BÁSICO	CAMBIO DE SOPORTE	MAGNÉTICO	DISCO	ALEATORIO	EXTRAÍBLE	NIVEL 1	SOBREESCRITURA (3)	
			MAGNÉTICO	DISCO	ALEATORIO	SISTEMA	NIVEL 1	SOBREESCRITURA (3)	
			MAGNÉTICO	CINTA	SECUENCIAL	EXTRAÍBLE	NIVEL 2	DESMAGNETIZACIÓN	2
			ÓPTICO	DISCO	ALEATORIO	EXTRAÍBLE	DESTRUCCIÓN		1
			SSD	DISCO	ALEATORIO	SISTEMA	NIVEL 1	SOBREESCRITURA (3)	
			SSD	MEMORIA	ALEATORIO	EXTRAÍBLE	NIVEL 1	SOBREESCRITURA (3)	
Gestión de los sistemas de información	Confidencialidad / LOPD	Condiciones de uso	Naturaleza	Tipo	Tipo de acceso	Dispositivo	Nivel de borrado	Técnicas de borrado	Observaciones
INTERNA	NIVEL MEDIO	CAMBIO DE SOPORTE	MAGNÉTICO	DISCO	ALEATORIO	EXTRAÍBLE	NIVEL 2	SOBREESCRITURA (7)	
			MAGNÉTICO	DISCO	ALEATORIO	SISTEMA	NIVEL 2	SOBREESCRITURA (7)	
			MAGNÉTICO	CINTA	SECUENCIAL	EXTRAÍBLE	NIVEL 2	DESMAGNETIZACIÓN	2
			ÓPTICO	DISCO	ALEATORIO	EXTRAÍBLE	DESTRUCCIÓN		1
			SSD	DISCO	ALEATORIO	SISTEMA	NIVEL 2	SOBREESCRITURA (7)	
			SSD	MEMORIA	ALEATORIO	EXTRAÍBLE	NIVEL 2	SOBREESCRITURA (7)	
Gestión de los sistemas de información	Confidencialidad / LOPD	Condiciones de uso	Naturaleza	Tipo	Tipo de acceso	Dispositivo	Nivel de borrado	Técnicas de borrado	Observaciones
INTERNA	NIVEL ALTO	CAMBIO DE SOPORTE	MAGNÉTICO	DISCO	ALEATORIO	EXTRAÍBLE	DESTRUCCIÓN		
			MAGNÉTICO	DISCO	ALEATORIO	SISTEMA	DESTRUCCIÓN		
			MAGNÉTICO	CINTA	SECUENCIAL	EXTRAÍBLE	DESTRUCCIÓN		
			ÓPTICO	DISCO	ALEATORIO	EXTRAÍBLE	DESTRUCCIÓN		
			SSD	DISCO	ALEATORIO	SISTEMA	DESTRUCCIÓN		
			SSD	MEMORIA	ALEATORIO	EXTRAÍBLE	DESTRUCCIÓN		

1 Se recomienda la destrucción de los soportes ópticos basándonos en las guías NIST 880-88 y ITSG-06, porque en la actualidad la sobreescritura no está indicada para el borrado de medios de esta naturaleza. Además a este tipo de soporte no es posible aplicarles la desmagnetización. Esto además podría requerir una copia de otros datos o documentos que se almacenen en el soporte y que, al no borrarse, deban conservarse.

2 Se recomienda la desmagnetización de los soportes de cinta por la rapidez y eficiencia de este método frente a una sobreescritura. En este caso habrá que contemplar el copiado a otro soporte de otros datos o documentos que se encuentren en el mismo soporte y que deban conservarse.

Tabla 3. Gestión externa con reutilización del soporte de almacenamiento.

EN CUANTO A LAS CONDICIONES			EN CUANTO AL SOPORTE				MÉTODO DE BORRADO MÍNIMO RECOMENDADO		
Gestión de los sistemas de información	Confidencialidad / LOPD	Condiciones de uso	Naturaleza	Tipo	Tipo de acceso	Dispositivo	Nivel de borrado	Técnicas de borrado	Observaciones
EXTERNA	NIVEL BÁSICO	REUTILIZACIÓN	MAGNÉTICO	DISCO	ALEATORIO	SISTEMA	NIVEL 0		
			MAGNÉTICO	CINTA	SECUENCIAL	EXTRAÍBLE	NIVEL 0		
			ÓPTICO	DISCO	ALEATORIO	EXTRAÍBLE	DESTRUCCIÓN		1
			SSD	DISCO	ALEATORIO	SISTEMA	NIVEL 0		
Gestión de los sistemas de información	Confidencialidad / LOPD	Condiciones de uso	Naturaleza	Tipo	Tipo de acceso	Dispositivo	Nivel de borrado	Técnicas de borrado	Observaciones
EXTERNA	NIVEL MEDIO	REUTILIZACIÓN	MAGNÉTICO	DISCO	ALEATORIO	SISTEMA	NIVEL 2	SOBREESCRITURA (7)	
			MAGNÉTICO	CINTA	SECUENCIAL	EXTRAÍBLE	NIVEL 2	DESMAGNETIZACIÓN	2
			ÓPTICO	DISCO	ALEATORIO	EXTRAÍBLE	DESTRUCCIÓN		1
			SSD	DISCO	ALEATORIO	SISTEMA	NIVEL 2	SOBREESCRITURA (7)	
Gestión de los sistemas de información	Confidencialidad / LOPD	Condiciones de uso	Naturaleza	Tipo	Tipo de acceso	Dispositivo	Nivel de borrado	Técnicas de borrado	Observaciones
EXTERNA	NIVEL ALTO	REUTILIZACIÓN	MAGNÉTICO	DISCO	ALEATORIO	SISTEMA	DESTRUCCIÓN		
			MAGNÉTICO	CINTA	SECUENCIAL	EXTRAÍBLE	DESTRUCCIÓN		2
			ÓPTICO	DISCO	ALEATORIO	EXTRAÍBLE	DESTRUCCIÓN		1
			SSD	DISCO	ALEATORIO	SISTEMA	DESTRUCCIÓN		

1 Se recomienda la destrucción de los soportes ópticos basándonos en las guías NIST 880-88 y ITSG-06, porque en la actualidad la sobreescritura no está indicada para el borrado de medios de esta naturaleza. Además a este tipo de soporte no es posible aplicarles la desmagnetización. Esto además podría requerir una copia de otros datos o documentos que se almacenen en el soporte y que, al no borrarse, deban conservarse.

2 Se recomienda la desmagnetización de los soportes de cinta por la rapidez y eficiencia de este método frente a una sobreescritura. En este caso habrá que contemplar el copiado a otro soporte de otros datos o documentos que se encuentren en el mismo soporte y que deban conservarse.

Tabla 4. Gestión externa con cambio del soporte de almacenamiento.

EN CUANTO A LAS CONDICIONES			EN CUANTO AL SOPORTE				MÉTODO DE BORRADO MÍNIMO RECOMENDADO		
Gestión de los sistemas de información	Confidencialidad / LOPD	Condiciones de uso	Naturaleza	Tipo	Tipo de acceso	Dispositivo	Nivel de borrado	Técnicas de borrado	Observaciones
EXTERNA	NIVEL BÁSICO	CAMBIO DE SOPORTE	MAGNÉTICO	DISCO	ALEATORIO	SISTEMA	NIVEL 2	SOBREESCRITURA (7)	
			MAGNÉTICO	CINTA	SECUENCIAL	EXTRAÍBLE	NIVEL 2	DESMAGNETIZACIÓN	2
			ÓPTICO	DISCO	ALEATORIO	EXTRAÍBLE	DESTRUCCIÓN		1
			SSD	DISCO	ALEATORIO	SISTEMA	NIVEL 2	SOBREESCRITURA (7)	
Gestión de los sistemas de información	Confidencialidad / LOPD	Condiciones de uso	Naturaleza	Tipo	Tipo de acceso	Dispositivo	Nivel de borrado	Técnicas de borrado	Observaciones
EXTERNA	NIVEL MEDIO	CAMBIO DE SOPORTE	MAGNÉTICO	DISCO	ALEATORIO	SISTEMA	DESTRUCCIÓN		
			MAGNÉTICO	CINTA	SECUENCIAL	EXTRAÍBLE	DESTRUCCIÓN		
			ÓPTICO	DISCO	ALEATORIO	EXTRAÍBLE	DESTRUCCIÓN		
			SSD	DISCO	ALEATORIO	SISTEMA	DESTRUCCIÓN		
Gestión de los sistemas de información	Confidencialidad / LOPD	Condiciones de uso	Naturaleza	Tipo	Tipo de acceso	Dispositivo	Nivel de borrado	Técnicas de borrado	Observaciones
EXTERNA	NIVEL ALTO	CAMBIO DE SOPORTE	MAGNÉTICO	DISCO	ALEATORIO	SISTEMA	DESTRUCCIÓN		
			MAGNÉTICO	CINTA	SECUENCIAL	EXTRAÍBLE	DESTRUCCIÓN		
			ÓPTICO	DISCO	ALEATORIO	EXTRAÍBLE	DESTRUCCIÓN		
			SSD	DISCO	ALEATORIO	SISTEMA	DESTRUCCIÓN		

1 Se recomienda la destrucción de los soportes ópticos basándonos en las guías NIST 880-88 y ITSG-06, porque en la actualidad la sobreescritura no está indicada para el borrado de medios de esta naturaleza. Además a este tipo de soporte no es posible aplicarles la desmagnetización. Esto además podría requerir una copia de otros datos o documentos que se almacenen en el soporte y que, al no borrarse, deban conservarse.

2 Se recomienda la desmagnetización de los soportes de cinta por la rapidez y eficiencia de este método frente a una sobreescritura. En este caso habrá que contemplar el copiado a otro soporte de otros datos o documentos que se encuentren en el mismo soporte y que deban conservarse.

VII.4 RECOMENDACIONES PARA LA DESTRUCCIÓN DE SOPORTES

Se recogen a continuación los requisitos mínimos para los procesos de destrucción de distintos tipos de soportes, basados en la guía "*Clearing and Declassifying Electronic Data Storage Systems*" del Gobierno de Canadá:

VII.4.1 Medios magnéticos

DESTRUCCIÓN (cualquier medio excepto incineración)	
Nivel de confidencialidad BAJO o MEDIO	**Disco**: al menos 3 pedazos, cada uno con un área máxima de 580 mm^2. **Cinta magnética**: pedazos con una longitud máxima de 50 mm.
Nivel de confidencialidad ALTO	**Disco**: al menos 3 pedazos, cada uno con un área máxima de 40 mm^2. **Cinta magnética**: pedazos con una longitud máxima de 6 mm.
Materias reservadas (información clasificada como SECRETA o RESERVADA)	**Disco**: al menos 3 pedazos, cada uno con un área máxima de 10 mm^2. **Cinta magnética**: pedazos con una longitud máxima de 3 mm.
INCINERACIÓN	
Todos los niveles de confidencialidad y grados de clasificación	Destrucción total. Se debe realizar en instalaciones con licencia para destrucción de metales o plásticos con habilitación para realizar estas actividades. Se utilizarán: herramientas de alto impacto, mazos, tornillos de banco, etc.

VII.4.2 Medios ópticos

DESTRUCCIÓN (cualquier medio excepto incineración)	
Nivel de confidencialidad BAJO o MEDIO	**CD exclusivamente**: moler la superficie del disco para suprimir la capa de datos coloreada; o **CD o DVD**: triturar en pequeños pedazos de área <160 mm^2
Nivel de confidencialidad ALTO	**CD exclusivamente**: moler la superficie del disco para suprimir la capa de datos coloreada; o **CD o DVD**: triturar en pequeños pedazos de área < 36 mm^2
Materias reservadas (información clasificada como SECRETA o RESERVADA)	**CD exclusivamente**: moler la superficie del disco para suprimir la capa de datos coloreada; o **CD o DVD**: triturar en pequeños pedazos de área < 10 mm^2
INCINERACIÓN	
Todos los niveles de confidencialidad y grados de clasificación	Destrucción total. Se debe realizar en instalaciones con licencia para destrucción de metales o plásticos con habilitación para realizar estas actividades. Se utilizarán: herramientas de alto impacto, mazos, tornillos de banco, etc.

VII.4.3 Medios basados en memorias de estado sólido

DESTRUCCIÓN (cualquier medio excepto incineración)	
Nivel de confidencialidad BAJO o MEDIO	Reducir a pedazos el dispositivo, cada uno con un área <160 mm^2
Nivel de confidencialidad ALTO	Triturar o pulverizar el chip de almacenamiento o el dispositivo de almacenamiento completo, en pedazos de tamaño < 2 mm
INCINERACIÓN	
Todos los niveles de confidencialidad y grados de clasificación	Destrucción total. Se debe realizar en instalaciones con licencia para destrucción de metales o plásticos con habilitación para realizar estas actividades. Se utilizarán: herramientas de alto impacto, mazos, tornillos de banco, etc.

VIII. BIBLIOGRAFÍA

Clearing and declassifying electronic data storage devices. Communications Security Establishment. 2006.

Corporate Governance - The Importance of a Compliant Record Retention Program. Christopher N. Weiss. 2007.

Guía/Norma de seguridad de las TIC (CCN-STIC-305). Destrucción y sanitización de soportes informáticos. Centro Criptológico Nacional. 2013.

Guía sobre almacenamiento y borrado seguro de información. INTECO, Ministerio de Industria, Comercio y Turismo. Abril de 2011.

Guidelines for Media Sanitization. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-88. Richard Kessel, Matthew Scholl, Steven Skolochenko, Xing Li. 2006.

Guidelines for Media Sanitization. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-88. Revisión 1. Richard Kessel, Matthew Scholl, Steven Skolochenko, Xing Li. 2012.

Memory Efficient Sanitization of a Deduplicated Storage System. Fabiano C. Botelho, Philip Shilane, Nitin Garg, Windsor Hsu. EMC Corporation. 2013

MoReq2010. DLM Forum Foundation. 2010.

Reliably erasing data from flash-based solid state drives. Michael Wei, Laura M. Grupp, Frederick E. Spada, Steven Swanson. 2011.

SAFE: Fast, Verifiable Sanitization for SSDs. Steven Swanson, Michael Wei 2010.

“Tutorial on Disk Drive Data Sanitization”. Gorgon Hughes, Tom Coughlin. 2008.

Ponencia nº 9

Valoración documental

José Luis García Martínez (Secretaría General Técnica)

Resumen de la ponencia:

La Valoración documental

José Luis García Martínez (Secretaría General Técnica)
Ponencia nº 9

El *Diccionario de terminología archivística* del Consejo Internacional de Archivos (ICA) define la valoración documental como "la fase del tratamiento archivístico que consiste en analizar y determinar los valores primarios y secundarios de las series documentales, fijando los plazos de transferencia, acceso y conservación o eliminación total o parcial".

La serie documental se constituye como la unidad de trabajo de la valoración, pues los valores primarios y secundarios, así como los plazos de conservación o vigencia y los términos de disposición que se asignan durante el proceso de valoración, no podrían ser fijados para documentos o expedientes individualmente considerados.

Para llevar a cabo la valoración se deben tener en cuenta los siguientes criterios de carácter general: **criterio de procedencia y evidencia:** se primarán los documentos y series documentales procedentes de los órganos que ocupan una posición más elevada dentro de la jerarquía administrativa; **criterio de contenido:** la misma información es mejor conservarla comprimida que extendida; **criterio diplomático:** los documentos originales, terminados y validados, son más valiosos que las copias; **criterio cronológico:** los documentos de archivo anteriores a 1940 no se considerarán objeto de valoración con vistas a su eliminación; **criterio funcional:** se primarán las series documentales producidas por los órganos administrativos en el ejercicio de funciones que les son propias y específicas, sobre aquellas series de carácter común; **criterio de producción:** se primarán las series documentales producidas por los órganos que realizan el seguimiento completo del procedimiento; y **criterio de utilización:** se primarán los documentos y series documentales que durante la etapa activa y semiactiva de su ciclo vital han sido objeto de demanda frecuente.

Estudiados los valores de cada serie documental, teniendo en cuenta los criterios anteriores, se pueden establecer las propuestas de valoración siguientes:

– **Conservación total** de documentos textuales que permitan conocer los orígenes del organismo, su organización y su evolución; los procesos de elaboración de leyes y reglamentos que afectan al organismo; que permitan valorar la eficacia de las actividades del organismo; que supervisan el funcionamiento interno del organismo; que tienen datos significativos sobre un acontecimiento, un individuo, una institución o un lugar, o sobre las ciencias y técnicas; que conservan datos significativos sobre acontecimientos o movimientos importantes de la historia política, económica y social; que contienen datos necesarios para la protección de los derechos civiles, financieros, jurídicos u otros derechos de los individuos, instituciones y de la misma institución; que contemplan de manera significativa la información contenida en otros fondos o series documentales; o que responden a las necesidades del análisis estadístico y de la historia cuantitativa.

– **Eliminación parcial:** cuando se trata de series documentales homogéneas y voluminosas, que aun siendo ejemplares primarios son susceptibles de eliminación conservando una muestra.

– **Eliminación total:** en el caso de series compuestas de ejemplares secundarios sin valor histórico, y cuya información está recogida en otros organismos.

Determinando los valores de la serie documental se determinan los criterios relativos a los tres ámbitos siguientes: los **plazos de transferencia**: en la documentación electrónica, la transferencia al Archivo Central supone ante todo un cambio en la responsabilidad de custodia sobre determinados documentos, bien situados en un mismo repositorio, o entre diferentes repositorios; los **plazos de selección y eliminación:** desaparecidos los valores primarios de los documentos, y comprobada la existencia de series paralelas, llega el momento de proceder a la selección, decidiendo la conservación o eliminación total o parcial de la serie, o el cambio de soporte. En esta fase se decide lo que se va a conservar y lo que se va a eliminar; y los **plazos de acceso**, analizados en el apartado 1.5.5. del documento de Política de Gestión de Documentos Electrónicos.

El Calendario de conservación es “el listado de series o asuntos a los cuales se asigna tanto el tiempo de permanencia en el Archivo Central como su disposición final”. Se trata de un inventario, organizado de acuerdo al cuadro de clasificación de fondos, en donde figuran las diferentes series documentales producidas por cada una de las unidades administrativas, proporcionando información sobre los plazos de permanencia de dichas series en cada una de las fases de archivo, así como la selección y eliminación de los documentos de manera adecuada.

La norma ISO 15489 define **Disposición** como la serie de procesos asociados con la aplicación de decisiones de transferencia, destrucción o conservación de documentos, que se documentan en los calendarios de conservación u otros instrumentos. Debe identificarse en el momento de captura, registro y clasificación. Asimismo, debería ser posible que las decisiones sobre la disposición se activen mediante alertas en el sistema.

Las propuestas de dictamen de conservación y eliminación corresponden al **Grupo de Trabajo de Coordinación de Archivos del Ministerio**, y deben ser elevadas a la **Comisión Superior Calificadora de Documentos Administrativos**.

Según la norma ISO 23081-2, los metadatos para la gestión de documentos deben ser ellos mismos objeto de valoración. La valoración determina no sólo qué metadatos deben capturarse acerca del documento, sino durante cuánto tiempo deben conservarse.

Ponencia nº 9

Valoración documental

José Luis García Martínez (Secretaría General Técnica)

I. LA VALORACIÓN, CONCEPTO Y OBJETIVOS

El *Diccionario de terminología archivística* del Consejo Internacional de Archivos (ICA) define la valoración documental como "la fase del tratamiento archivístico que consiste en analizar y determinar los valores primarios y secundarios de las series documentales, fijando los plazos de transferencia, acceso y conservación o eliminación total o parcial".

La valoración surge como una respuesta a los problemas de acumulación y explosión de documentos. Sus propósitos centrales son establecer los criterios, métodos e instrumentos que ayuden a la mejor administración de los documentos resultantes de los procesos de gestión de las organizaciones, así como a la conservación del patrimonio documental.

En la fase de Valoración se decide cuando los documentos deben transferirse a otro archivo del sistema, o si éstos deben eliminarse total o parcialmente, en cuyo caso debemos aplicar técnicas de selección. Si la valoración es un proceso intelectual, la selección es un proceso práctico en el que se diferencian las series a conservar de aquellas que deben eliminarse.

En la Valoración encontramos tres tipos de acciones diferenciadas, que tienen lugar de manera escalonada:

1) acciones destinadas al análisis de los valores asociados a la documentación (fase intelectual);

2) acciones destinadas a la generación de políticas, reglas e instrucciones para normar el proceso de valoración (fase normativa);

3) acciones destinadas al uso y aplicación de las políticas y regulaciones asociadas a la valoración en los archivos, que se materializan en la conservación, transferencia, acceso o eliminación de los documentos (fase práctica).

II. LA SERIE DOCUMENTAL COMO UNIDAD DE TRABAJO DE LA VALORACIÓN

La serie documental se constituye como la unidad de trabajo de la valoración, pues los valores primarios y secundarios, así como los plazos de conservación o vigencia y los términos de disposición que se asignan durante el proceso de valoración, no podrían ser fijados para documentos o expedientes individualmente considerados, en virtud de que la gestión de archivos centra su atención en conjuntos orgánicos y organizados de información; es decir, sobre conjuntos de documentos que guardan relaciones entre sí, pues son resultado de un mismo proceso de gestión o acumulación y producidos por una misma entidad productora.

La Administración contemporánea no desarrolla su actividad de forma aislada y puntual, sino en un contexto determinado por normas de procedimiento. Por tanto, los documentos de archivo tienen carácter seriado. Se producen en el ejercicio de diferentes actividades que se prolongan en el tiempo, dando lugar a las distintas series documentales.

Una serie es un conjunto organizado y homogéneo de documentos producidos o recibidos a lo largo del tiempo por una oficina en el desarrollo de una función concreta.

Ello supone que todas las unidades que componen la serie, normalmente expedientes, se rigen por la misma normativa, tienen una estructura interna similar y contienen el mismo tipo de información, lo que permite establecer normas de conservación para el conjunto de los mismos.

Según los criterios generales para la valoración de los documentos de la Administración General del Estado[1], los documentos de archivo insuficientemente identificados no pueden valorarse adecuadamente. Se establecerán plazos de transferencia, acceso y conservación o, en su caso, eliminación total o parcial para las series documentales.

Análisis de los valores de los documentos

El Diccionario de Terminología Archivística, basándose en la clasificación de Schellemberg establece dos tipos de valores, los primarios (administrativo, legal, jurídico, fiscal y contable) y los secundarios (histórico e informativo). El análisis de los valores se centrará en la identificación de los valores primarios, para determinar su caducidad administrativa, y en el estudio del desarrollo de los secundarios[2].

VALORES PRIMARIOS	
Administrativo	Sirve como testimonio de los procedimientos y actividades de la administración que los ha producido.
Jurídico	Aquel del que se derivan derechos u obligaciones legales regulados por el derecho común.
Legal	Es el que sirve de testimonio ante la Ley.
Fiscal	Es el que sirve de testimonio de obligaciones tributarias.
Contable	El que puede servir de explicación o justificación de operaciones destinadas al control presupuestario

VALORES SECUNDARIOS	
Informativo	Sirve de referencia para la elaboración o reconstrucción de cualquier actividad de la Administración y que también puede ser testimonio de la memoria colectiva.
Histórico	El que posee un documento como fuente primaria para la Historia.

Criterios a tener en cuenta antes de la valoración

Determinar los valores de los documentos es una tarea complicada, por tanto, necesitamos una serie de criterios que, unidos al análisis de los valores, nos proporcionen las pautas para decidir los plazos de transferencia entre los diferentes archivos del sistema, y los plazos de selección o eliminación.

Según los criterios generales para la valoración de los documentos de la Administración General del Estado aprobados en 2003[3], **son documentos de archivo de la Administración General de Estado y forman parte de su Patrimonio Documental** los documentos de cualquier época, generados, conservados o reunidos en el ejercicio de su función por cualquiera de los departamentos y órganos que la componen, por sus organismos públicos, por las personas jurídicas en cuyo capital participe mayoritariamente el Estado y por las personas privadas, físicas o jurídicas, gestoras de servicios públicos de carácter estatal en lo relacionado con la gestión de dichos servicios.

Constituye **documentación de apoyo informativo**, y no forma parte del Patrimonio Documental, aquella que no se produce como resultado de la gestión administrativa, aunque sea necesario disponer de ella para el correcto desarrollo de la actividad administrativa (textos lega-

[1] Documento aprobado por la Comisión Superior Calificadora de Documentos Administrativos, en sesión de 27 de noviembre de 2003.

[2] Sobre el análisis de los valores de los documentos véase: LA TORRE MERINO, J.L., y MARTÍN-PALOMINO Y BENITO, M., *Metodología para la identificación de fondos documentales*, Madrid, Ministerio de Educación, Cultura y Deportes, S.G. Información y Publicaciones, 2000, p. 36.

[3] Documento aprobado por la Comisión Superior Calificadora de Documentos Administrativos, en sesión de 27 de noviembre de 2003.

les, boletines oficiales, publicaciones, circulares). **La documentación de apoyo informativo no tiene que ser objeto de valoración a los efectos del R.D. 1164/2002, de 8 noviembre.** Puede ser destruida una vez que ha cumplido los fines para los que fue reunida.

Para llevar a cabo la valoración se deben tener en cuenta los siguientes criterios de carácter general:

– **Criterio de procedencia y evidencia:** se primarán los documentos y series documentales procedentes de los órganos que ocupan una posición más elevada dentro de la jerarquía administrativa. Los documentos de unidades administrativas de rango inferior son importantes cuando reflejan su propia actividad irrepetible.

– **Criterio de contenido:** la misma información es mejor conservarla comprimida que extendida. Se primarán los documentos y series que recogen información sustancial para reconstruir la historia del órgano productor, de un acontecimiento, de un periodo cronológico concreto, de un territorio o de las personas. Los documentos y series documentales que contienen información que se encuentra duplicada o recapitulada en otros documentos o series documentales de cuya existencia se tenga constancia son susceptibles de eliminación.

– **Criterio diplomático:** los documentos originales, terminados y validados, son más valiosos que las copias. Las copias, siempre que se tenga constancia de la conservación de los originales, son susceptibles de eliminación.

– **Criterio cronológico:** según los criterios generales para la valoración de los documentos de la Administración General del Estado aprobados en 2003, los documentos de archivo anteriores a 1940 no se considerarán objeto de valoración con vistas a su eliminación. Se conservarán de forma permanente en los archivos históricos correspondientes, al servicio de su utilización para la investigación y la cultura y la información.

– **Criterio funcional:** se primarán las series documentales producidas por los órganos administrativos en el ejercicio de funciones que les son propias y específicas, sobre aquellas series de carácter común. El contenido informativo de las series con funciones generales puede estar recogido en otro organismo, por ello son más susceptibles de eliminación que las de funciones específicas.

– **Criterio de producción:** se primarán las series documentales producidas por los órganos que realizan el seguimiento completo del procedimiento. Las series documentales que, en virtud de las competencias y funciones desarrolladas por el órgano que las produce, reflejen sólo una parte del procedimiento son susceptibles de ser eliminadas, siempre que se conserve la serie reflejo de la tramitación completa. Los ejemplares principales son los que conserva la unidad de origen del expediente, mientras que el ejemplar secundario es acumulado por una oficina diferente a la productora como consecuencia de las relaciones que entre ellas se establecen.

– **Criterio de utilización:** se primarán los documentos y series documentales que durante la etapa activa y semiactiva de su ciclo vital han sido objeto de demanda frecuente por parte del órgano productor, de los investigadores o de los ciudadanos en general.

Según la norma UNE-ISO 15489, la decisión sobre qué documentos deben incorporarse al Sistema de Gestión de Documentos y durante cuánto tiempo deberían conservarse requiere un análisis del entorno interno y externo de la organización, su relación o relaciones con dicho entorno y la identificación de las funciones y actividades de la organización. Según esta norma, para la conservación de los documentos electrónicos se deberían:

1.- Satisfacer las necesidades de gestión, presentes y futuras, mediante:

- La conservación de información relativa a decisiones y actividades presentes y pasadas como parte de la memoria corporativa para apoyar decisiones y actividades en el presente y en futuro.
- La conservación de elementos de prueba de las actividades presentes y pasadas para cumplir las obligaciones de rendición de cuentas.

- La eliminación, lo antes posible y de manera sistemática y autorizada, de los documentos que ya no se necesiten.

- La conservación del contexto del documento, lo que permitirá a futuros usuarios juzgar su autenticidad y fiabilidad, incluso en sistemas de gestión de documentos cerrados o que hayan sufrido importantes cambios.

2.- Cumplir los requisitos legales, garantizando que se documenta, entiende e implementa la reglamentación aplicable a la gestión de documentos producidos en el ejercicio de las actividades específicas, y

3.- Satisfacer las necesidades presentes y futuras de las partes interesadas, tanto externas como internas, mediante:

- La identificación de los intereses legítimos y exigibles que las partes interesadas puedan tener en relación con la conservación de los documentos durante un periodo de tiempo superior al requerido por la propia organización.

- La identificación y la evaluación de los beneficios legales, financieros, políticos, sociales y de cualquier otro tipo que se deriven de la conservación de los documentos al servicio de la investigación y de la sociedad en su conjunto.

- El cumplimiento, en su caso, de las disposiciones reglamentarias de la autoridad archivística competente.

III. TIPOS DE DICTAMEN

Estudiados los valores de cada serie documental, teniendo en cuenta los criterios anteriores, se pueden establecer las propuestas de valoración siguientes:

Conservación total: Se trata de documentación con valor evidencial, testimonial e informativo representada por ejemplares primarios, aquellos que conserva la unidad de origen del expediente. **Según la Norma UNE-ISO 15489, los documentos de conservación permanente son aquellos que**:

- Proporcionan información y pruebas sobre las políticas y las acciones de la organización.

- Proporcionan información y pruebas sobre la interacción de la organización con aquellos a quienes presta sus servicios.

- Documentan derechos y las obligaciones de individuos y organizaciones.

- Contribuyen a la elaboración de la memoria de la organización con fines científicos, culturales o históricos.

- Contienen información y pruebas relativas a actividades de interés para partes interesadas externas e internas.

Según los **Criterios aprobados por la Generalitat de Catalunya** por orden de 15 de octubre de 1992 se deben conservar:

1.- Los documentos textuales que permitan conocer los orígenes del organismo, su organización y su evolución.

2.- Los documentos que permitan conocer los procesos de elaboración de leyes y reglamentos que afectan al organismo.

3.- Los documentos textuales que permitan valorar la eficacia de las actividades del organismo.

4.- Los documentos que supervisan el funcionamiento interno del organismo.

5.- Los documentos que tienen datos significativos sobre un acontecimiento, un individuo, una institución o un lugar, o sobre las ciencias y técnicas.

6.- Los documentos que conservan datos significativos sobre acontecimientos o movimientos importantes de la historia política, económica y social.

7.- Los documentos que contiene datos necesarios para la protección de los derechos civiles, financieros, jurídicos u otros derechos de los individuos, instituciones y de la misma institución.

8.- Los documentos que contemplan de manera significativa la información contenida en otros fondos o series documentales.

9.- Los documentos que responden a las necesidades del análisis estadístico y de la historia cuantitativa.

Eliminación parcial: Se trata de series documentales homogéneas y voluminosas, que aún siendo ejemplares primarios son susceptibles de eliminación conservando una muestra.

Eliminación total: Cuando se trata de series compuestas de ejemplares secundarios sin valor histórico, y cuya información está recogida en otros organismos. En los **Criterios aprobados por la Generalidad de Catalunya** se establece que son susceptibles de eliminación:

- Los documentos cuyos datos se recogen en publicaciones.
- Los documentos en fase de deterioro avanzado.
- Las series que presentan vacíos informativos que imposibilitan su comprensión.

Para determinar los documentos que se van a conservar en la eliminación parcial o los testigos que quedarán en la eliminación total se utilizará la técnica del muestreo. Se entiende por muestreo la técnica de selección según criterios sistemáticos (numéricos, alfabéticos, topográficos) o cualitativos, de cierta proporción de documentos en representación de un conjunto.

EJEMPLAR O TESTIGO	Se selecciona uno o varios expedientes, dentro de una serie documental para ilustrar la práctica administrativa del momento. No pone de manifiesto las características del conjunto
CUALITATIVO O SELECTIVO	Método subjetivo que se basa en una serie de criterios preconcebidos de antemano, mediante los cuales se conservan los documentos que se consideran más importantes
SISTEMÁTICO	Se establece un criterio previo de selección numérico, cronológico, geográfico o alfabético, dependiendo de la organización de la serie documental. Es el que ofrece una mayor garantía.
ALEATORIO	Es un criterio por el que se seleccionan varios expedientes al azar teniendo en cuenta que cualquiera de ellos tiene las mismas cualidades para representar al conjunto de la serie documental.

IV. METODOLOGÍA DE TRABAJO

La primera valoración debe realizarse por los Archivos Centrales del Departamento, que debe proceder al análisis de los valores primarios y secundarios, sobre todo los primeros. Para llevar a cabo esta labor es necesario el apoyo de los gestores de la documentación, quienes conocen con precisión los plazos de vigencia administrativa, su valor legal o probatorio, y el interés informativo que poseen[4].

El conocimiento del periodo de vigencia administrativa se puede conocer a través de la frecuencia de consulta y por los plazos que estén establecidos por norma oficial.

A la hora de llevar a cabo la valoración de la documentación las tareas que deben realizarse son las siguientes[5]:

[4] Sobre la metodología de trabajo véase: MOLINA NORTES, J., y LEYVA PALMA, V., *Técnicas de Archivo y tratamiento de la documentación administrativa*, Guadalajara, ANABAD Castilla-La Mancha, 1996, p. 164-171.
[5] LA TORRE MERINO, J.L., y MARTÍN-PALOMINO Y BENITO, M., *op.cit.* p. 39.

1.- Acotación del objeto de estudio, desde un punto de vista orgánico y cronológico: el objeto de estudio debe ser la serie documental	Realizados en la fase de Identificación
2.- Identificación del organismo productor	
3.- Identificación de las series documentales	
4.- Elaboración de los cuadros de clasificación	
5.- Confección del repertorio general de series	
6.- Análisis de los valores de cada serie, procedimiento y documentos que componen el expediente	
7.- Estudio comparativo de las **series complementarias** (aquellas que respondiendo a trámites administrativos diferentes, contribuyen a la realización de un mismo objetivo) y **paralelas** (las que materializan actividades dentro de las funciones administrativas comunes que en consecuencia son producidas por las distintas oficinas que en cada organismo tienen ese cometido)	
8.- Valoración de cada serie documental, determinando sus plazos de transferencia, conservación y/o eliminación, y plazos de acceso	

Sería necesario cumplimentar una ficha de identificación y valoración para cada serie documental, que debemos incluir en un repertorio de series documentales, como hemos indicado en el apartado 1.5.3. de Clasificación en el documento de Política de Gestión de Documentos Electrónicos.

V. RESULTADOS DE LA FASE DE VALORACIÓN

Analizando los valores de la serie documental se determinan los criterios relativos a los tres ámbitos siguientes:

Los plazos de transferencia. En la documentación electrónica, la transferencia al Archivo Central supone ante todo un cambio en la responsabilidad de custodia sobre determinados documentos, bien situados en un mismo repositorio, o entre diferentes repositorios.

El artículo 21.1j) del Real Decreto 4/2010, prevé “la transferencia de los expedientes entre los diferentes repositorios electrónicos a efectos de conservación, de acuerdo con lo establecido en la legislación en materia de Archivos, de manera que se pueda asegurar su conservación, y recuperación a medio y largo plazo”.

Por su parte, el artículo 21.2 indica que: “las Administraciones públicas crearán repositorios electrónicos, complementarios y equivalentes en cuanto a su función a los archivos convencionales, destinados a cubrir el conjunto del ciclo de vida de los documentos electrónicos”.

El flujo documental en la Administración General del Estado quedó estructurado en el Decreto 914/1969, de 8 de mayo de creación del Archivo General de la Administración. El artículo segundo establece: “Anualmente, en las fechas y forma que se determine por el subsecretario de cada Departamento, las dependencias de la Administración Pública, Central e Institucional, remitirán al Archivo Central del Ministerio a que pertenezcan la totalidad de los expedientes en que se hayan dictado actos administrativos de resolución que afecten de algún modo a derechos e intereses del Estado o de los administrados, cuando dichos actos hayan devenido firmes y se hayan practicado por la Administración las actuaciones conducentes a la total ejecución de sus pronunciamientos. Cuando se trate de expedientes o documentos en que no proceda dictar actos administrativos de resolución de carácter expresado, así como informes, estudios, etc., pasarán al Archivo General cuando hayan producido en la dependencia que los ha elaborado o tramitado la totalidad de sus efectos”.

Por otro lado, el artículo tercero establece que “la documentación de los Archivos Centrales de los Ministerios se trasladará al Archivo General de la Administración al cumplirse los quince años desde su ingreso en los mismos”.

Los plazos de selección y eliminación. Desaparecidos los valores primarios de los documentos, y comprobada la existencia de series paralelas, llega el momento de proceder a la selec-

ción, decidiendo la conservación o eliminación total o parcial de la serie, o el cambio de soporte. En esta fase se decide lo que se va a conservar y lo que se va a eliminar.

Los plazos de acceso. Los plazos de acceso analizados en la fase de valoración se analizan en el apartado 1.5.5. del presente documento de Política de Gestión de Documentos.

VI. ELABORACIÓN DEL CALENDARIO DE CONSERVACIÓN

El Calendario de conservación se estructura en las denominadas tablas de Valoración Documental, que se definen como "el listado de series o asuntos a los cuales se asigna tanto el tiempo de permanencia en el Archivo Central como su disposición final". Se trata de un inventario, organizado de acuerdo al cuadro de clasificación de fondos, en donde figuran las diferentes series documentales producidas por cada una de las unidades administrativas, proporcionando información sobre los plazos de permanencia de dichas series en cada una de las fases de archivo, así como la selección y eliminación de los documentos de manera adecuada.

Para su confección, consultando a los órganos gestores, se debe normalizar la terminología utilizada y elaborar un inventario de series documentales sobre las cuales se van a aplicar las reglas de conservación. Deben priorizarse las series comunes porque pueden ser aplicadas por un número mayor de organismos. Es necesario contar con los recursos humanos necesarios así como de un marco legal que parta de las autoridades superiores, mediante la formulación de normas internas.

ELEMENTOS DE INFORMACIÓN DEL INVENTARIO PARA UN CALENDARIO DE CONSERVACIÓN[6]
Código numérico que identifica el número de norma (las normas aparecen agrupadas de acuerdo a la confección del inventario bajo grandes categorías o grupos funcionales)
Título de la serie
Descripción o contenido de los documentos de la serie
Nombre del órgano productor
Tipo de ejemplar si se trata de ejemplares primarios o secundarios
Periodo de conservación, con indicación del número de años en el estado activo y semiactivo de la serie
Modo de conservación y disposición en el estado inactivo (conservación total, eliminación total o eliminación parcial) y tipo de soporte

En las Administraciones Públicas los calendarios de conservación deben ser enviados una vez elaborados a los órganos competentes en materia de archivos que deberá estudiarlos, aprobarlos o revisarlos y hacerlos públicos oficialmente.

Según la Norma UNE-ISO 15489-2 para determinar los plazos de conservación deben contemplarse cinco etapas:

1.- Determinar el **marco legal o administrativo** del mantenimiento de documentos dentro del sistema. Los requisitos legales o administrativos pueden interponer plazos mínimos de conservación.

2.- Determinar los diversos usos de los documentos dentro del sistema. Debería distinguirse entre los documentos principales, de uso recurrente, y los documentos de múltiples operaciones específicas, que hacer referencia a los anteriores. Puede ser posible eliminar del sistema estos segundos.

3.- Determinar los vínculos de unión con otros sistemas. Los documentos de un sistema pueden servir de respaldo o referencia para otros sistemas.

[6] MOLINA NORTES, J., y LEYVA PALMA, V., *Op. Cit.*, p. 170.

4.- Tener en cuenta la variedad de usos de los documentos, identificando a los usuarios externos con intereses en la conservación de los documentos, evaluando el riesgo asociado a la destrucción de los documentos, una vez que se haya completado su utilización habitual; determinando cuáles son los documentos esenciales para garantizar la continuidad de la organización en caso de pérdida o daño y qué acciones son necesarias para conservarlos; evaluar los beneficios financieros, políticos, sociales o de otro tipo derivados de la conservación de los documentos; y analizar el balance coste-beneficios no financieros de la conservación de los documentos para decidir cuánto tiempo deben conservarse una vez cubiertas las necesidades de la organización.

5.- Asignar los plazos de conservación y acciones de disposición de similares ca**racterísticas** para conjuntos de documentos que reflejan o registran actividades similares. Todos los documentos pertenecientes a un mismo sistema de gestión deberían estar contemplados en algún calendario de conservación. Los plazos de conservación deben fijarse con claridad y las acciones de disposición deben identificarse de forma inequívoca.

VII. DISPOSICIÓN DOCUMENTAL

La norma ISO 15489 define Disposición como la serie de procesos asociados con la aplicación de decisiones de transferencia, destrucción o conservación de documentos, que se documentan en los calendarios de conservación u otros instrumentos.

En un sistema de gestión de documentos, preferiblemente, debe determinarse el destino de los documentos y los plazos de conservación de los mismos en el momento de captura, registro y clasificación, cuando éstos hayan sido objeto de dictamen por parte de la Comisión Superior Calificadora de Documentos Administrativos. Asimismo, debería ser posible que las decisiones sobre la disposición se activen mediante alertas en el sistema, que permitan su ejecución bajo la supervisión del Archivo. Los sistemas deberían proporcionar pistas de auditoría u otros métodos de seguimiento con objeto de controlar las acciones de disposición que se hayan realizado.

Las propuestas de dictamen de conservación y eliminación corresponden al **Grupo de Trabajo de Coordinación de Archivos del Ministerio**, y debe ser elevadas a la **Comisión Superior Calificadora de Documentos Administrativos**. La ejecución de las acciones debe quedar en manos del administrador del sistema, siempre bajo la supervisión del Archivo Central. El administrador será el único usuario con la potestad de ejecutar todas las acciones derivadas de los dictámenes de la comisión de valoración y reflejados en los Calendarios de conservación, e incluso debe ser capaz de bloquear o paralizar de forma manual o automática la eliminación de documentos.

La aplicación del calendario de conservación se ejecutará desde el nivel de serie documental. No obstante, los sistemas de gestión de documentos electrónicos deben ser capaces de asignar un criterio de valoración para cualquier documento o agrupación. Incluso la aplicación de gestión deberá permitir que los documentos electrónicos que hayan sido reclasificados adopten el mismo criterio de valoración que la nueva serie.

Valoración y uso de los metadatos

Según la norma UNE-ISO 23081-2, los metadatos para la gestión de documentos deben ser ellos mismos objeto de valoración. La valoración determina no sólo qué metadatos deben capturarse acerca del documento, sino durante cuánto tiempo deben conservarse, y cuándo, en función del documento, algunos o todos ellos pueden destruirse o gestionarse de manera separada del objeto documento.

Los metadatos pueden diseñarse en el momento de incorporación, adaptados para su uso para conjuntos muy específicos de documentos. La adaptación y selección de los metadatos adecuados constituyen en sí mismas una decisión relacionada con la valoración

Algunos documentos tienen periodos de conservación largos, y pueden necesitar intervenciones activas un cierto número de veces a lo largo de ese periodo. Cada vez que se reali-

ce una intervención con vistas a la conservación, se requiere una valoración para decidir qué metadatos mantener.

En el momento de implementar una decisión de valoración que implique destruir documentos, deberían adoptarse un conjunto de decisiones independientes acerca de cuáles, en su caso, de los metadatos asociados a ese documento, también deberían destruirse.

MoReq2010 prevé que una parte de los metadatos se retiene después de que el documento mismo haya sido destruido, como evidencia del hecho de la existencia del documento en un periodo de tiempo. La valoración también se tendrá en cuenta para decidir el formato y métodos de almacenamiento de los metadatos para la gestión de documentos.

GOBIERNO
DE ESPAÑA

MINISTERIO
DE HACIENDA
Y ADMINISTRACIONES PÚBLICAS

CENTRO
DE PUBLICACIONES