MINISTERIO
DE EDUCACIÓN, CULTURA
Y DEPORTE

Política de Gestión de Documentos Electrónicos

ÍNDICE

Histórico de versiones del documento		
Versión	Fecha	Descripción
1.0	09/07/2015	Primera versión de la Política
1.1	03/05/2016	Primera revisión de la Política

Equipo responsable de la elaboración del documento
Subdirección General de Archivos Estatales:
• Guillermo Alonso Fernández • Blanca Desantes Fernández • Jorge Fernández García • Beatriz Franco Espiño • José Luis Muñoz Romano • Ricard Pérez Alcázar
Subdirección General de Tecnologías de la Información y las Comunicaciones
• Gloria Bautista Vega • Ana Beltrán Poveda • Carlos C. Herrero García • Alberto Sánchez Alonso • Juan Pablo Sanz Martín
Consejo Superior de Deportes
• Oscar Martínez Rodríguez
Biblioteca Nacional
• Ana Carrillo Pozas • José Patricio Hernández Sánchez
Gerencia de Infraestructuras y Equipamiento:
• Ernesto Garrote Pérez
Maquetación (S.G. Tecnologías de la Información y las Comunicaciones)
• Ángela Barroso Pastor • Araceli de Bunes del Valle

PRESENTACIÓN

Los documentos son la base y el fundamento de un gobierno abierto y el soporte de los principios de transparencia, participación ciudadana y colaboración. Los documentos correctamente gestionados son también un valor añadido para las Administraciones Públicas ya que permiten a una organización evaluar el impacto de sus programas, mejorar los procesos de trabajo y compartir conocimientos entre diferentes instancias del gobierno. Además, los documentos protegen los derechos e intereses de los ciudadanos y hacen a los empleados públicos responsables de sus acciones, sin olvidar que los documentos de conservación permanente van a documentar la historia de nuestra nación.

La implementación de una política de gestión de documentos electrónicos es una obligación democrática de nuestra Administración que debe alinearse con otros objetivos estratégicos de alto nivel político como son la Transparencia, el Acceso a la Información Pública, el Buen Gobierno y la Rendición de Cuentas (mandatos establecidos en la Ley 19/2013, de Transparencia, Acceso a la Información Pública y Buen Gobierno, en adelante, LTAIBG).

El derecho de acceso de los ciudadanos a los documentos de las Administraciones públicas es un derecho esencial de la vida democrática. Las enormes posibilidades que ofrece el entorno digital para el acceso a la información convierten este derecho y deber en un elemento clave a considerar en el seno del Ministerio de Educación, Cultura y Deporte (en adelante, MECD). La administración electrónica debe, además, conjugar la transparencia administrativa y el derecho a la información con la protección de otros derechos fundamentales como la intimidad de las personas y otras restricciones recogidas en nuestro ordenamiento jurídico.

Por lo tanto, las condiciones y reglas que rigen el acceso a los documentos electrónicos deben estar claramente definidas y correctamente implementadas tecnológicamente en el seno de nuestra organización, estableciéndose los sujetos de acceso (ciudadanos, usuarios internos, otras administraciones), los objetos de acceso (expedientes y documentos electrónicos, redacciones parciales de documentos, etc.) y las condiciones propiamente dichas en relación con el acceso (público, restringido, secreto) así como los cambios en dichas condiciones que se pudieran producir (plazos, desclasificaciones, etc.), prestando especial atención a aquellos procedimientos con efectos frente a terceros y/o interesados.

La obligación de transparencia de la administración implica que los documentos y expedientes electrónicos puedan ser localizados e identificados y para ello deben contar con procedimientos obligatorios de asignación de los metadatos necesarios que hagan posible conocer su ubicación y uso. Implica, también, que los documentos sean legibles independientemente de la tecnología con la que se

hayan creado, sean procesables, reutilizables y que los medios (metodológicos y tecnológicos) que se utilicen para la búsqueda, recuperación y consulta de los documentos electrónicos estén diseñados de acuerdo con los estándares de usabilidad y accesibilidad.

El Esquema Nacional de Interoperabilidad establece en su artículo 21 que las Administraciones públicas deberán poner en marcha las medidas necesarias que garanticen el "acceso completo e inmediato a los documentos a través de métodos de consulta en línea que permitan la visualización con todo detalle del contenido de los documentos, la recuperación exhaustiva y pertinente de los documentos, la copia o descarga en línea en los formatos originales y la impresión en papel de aquellos documentos que sean necesarios". Por lo tanto, el MECD tiene que contar con una política de gestión de documentos electrónicos consistente dentro de la planificación de la administración electrónica.

Los beneficios de implantar una correcta política de gestión de documentos electrónicos en el seno del MECD son indudables: permitirá mostrar correctamente la evidencia de las actividades de los departamentos y sus unidades dependientes; documentar la toma de decisiones; facilitar la rendición de cuentas y la transparencia administrativa; cumplir con los requisitos legislativos y normativos de nuestra organización; ofrecer protección y soporte en caso de conflicto o litigio; interrelacionarse con los administrados y otras administraciones; y mantener la memoria colectiva.

La obligación de transparencia y rendición de cuentas supone también realizar un análisis de los riesgos a nivel estratégico que identifique las consecuencias, tanto para el MECD como para los ciudadanos, de la pérdida, destrucción o gestión inadecuada de la documentación electrónica de nuestra organización. Una adecuada gestión de riesgos deberá poner los medios para controlar, eliminar y mitigar los riesgos identificados en relación con la gestión de los documentos electrónicos de la organización. Las estrategias de gestión de riesgos en materia de política de gestión de documentos electrónicos deberán alinearse con las estrategias generales de gestión de riesgos del MECD.

El Gobierno abierto -entendido como modelo de gobierno que fundamenta su funcionamiento en los principios de transparencia, participación y colaboración, aprovechando las oportunidades que ofrecen las Tecnologías de la Información y la Comunicación, con el objetivo general de mejorar la calidad democrática y el funcionamiento de los gobiernos y las instituciones públicas- cuenta con la gestión de documentos y archivos electrónicos como un elemento esencial para implementar políticas de transparencia activa y datos abiertos, ya que permiten generar y mantener información y datos de calidad y proporcionar herramientas para su descubrimiento, comprensión y reutilización, tal y como dicta la Ley 37/2007, sobre Reutilización de la Información del Sector Público modificada por la Ley 18/2015, de 9 de julio.

Por lo tanto, resulta obvio que los procesos de gestión de documentos electrónicos contenidos en este documento pueden respaldar decididamente las estrategias de transparencia activa y datos abiertos que nos permitan crear datos y documentos auténticos y fidedignos; documentar la relación de los datos con sus fuentes y su contexto de producción; mejorar el descubrimiento y comprensión de la información y los datos; proporcionar antecedentes y continuidad a los conjuntos de datos contenidos en los documentos. El *NARA´s Open government plan* 2012-2014 es un ejemplo reciente de planificación estratégica de los Archivos Nacionales de la Administración de Estados Unidos para el cumplimiento de la directiva de gobierno abierto.

El MECD, a través de la Secretaria de Estado de Cultura, Dirección General de Bellas Artes y Bienes Culturales y de Archivos y Bibliotecas, tiene competencias, según lo dispuesto en la Ley 16/1985, del Patrimonio Histórico Español, en materia de protección del patrimonio documental sea cual sea el soporte en el que éste se ha generado, incluyendo, por lo tanto los documentos electrónicos. Además, tiene atribuciones específicas sobre la custodia de los documentos y expedientes electrónicos que, habiendo finalizado su fase activa según los calendarios de conservación establecidos, pasan a su fase de archivo y debe transferirse la responsabilidad de la custodia al archivo intermedio (Archivo General de la Administración de Alcalá de Henares) o al archivo histórico (Archivo Histórico Nacional) de la Administración General del Estado, según lo dispuesto en el Real Decreto 1708/2011 que regula, entre otros aspectos, el Sistema de Archivos de la Administración General del Estado. Tanto el Archivo General de la Administración General del Estado como el Archivo Histórico Nacional son Archivos dependientes de este Departamento ministerial.

De la Secretaría de Estado de Cultura depende también la Comisión Superior Calificadora de Documentos Administrativos, que dictamina, previa valoración documental, qué documentos de la Administración General del Estado pueden ser eliminados reglamentariamente y qué documentos deben ser de conservación permanente mediante la aplicación de procedimientos de valoración reglados, transparentes y participativos.

Una correcta política de gestión de documentos electrónicos del MECD debe garantizar la interoperabilidad de los documentos y expedientes electrónicos generados y recibidos por nuestra organización con otros departamentos, administraciones y ciudadanos (la denominada interoperabilidad sincrónica) en el contexto de una e-administración.

Pero, dadas sus competencias, el MECD tiene especial responsabilidad en articular estrategias para garantizar la integridad, autenticidad, disponibilidad, trazabilidad y contexto de producción de los documentos y expedientes electrónicos, así como de sus metadatos asociados, a lo largo de todo el ciclo

de vida de los mismos con el fin de garantizar para generaciones futuras la conservación de los documentos con valor histórico y patrimonial (interoperabilidad diacrónica). La Política de Gestión de Documentos Electrónicos del MECD debe abarcar todo el ciclo de vida de los documentos hasta su conservación permanente. El *continuum* documental puede procurar la máxima eficacia en la gestión de los documentos electrónicos custodiados.

El MECD debe elaborar los requisitos necesarios con el fin de crear, mantener, tratar y conservar documentos electrónicos que sean auténticos, fiables, disponibles y proteger la integridad de los mismos durante todo su ciclo de vida (incluida la fase histórica). Los documentos electrónicos deben estar protegidos frente a cualquier adición, supresión, eliminación no reglada, modificación u ocultación no autorizada.

El MECD, al tener responsabilidades y competencias sobre todo el ciclo de vida de los documentos y expedientes electrónicos, incluida su conservación permanente, debe diseñar una política de gestión de documentos y establecer los requisitos necesarios para que cuando se produzca el cambio físico de los documentos y/o el cambio de responsabilidad de custodia de los mismos, dicho cambio se haga sin merma de la autenticidad, fiabilidad, integridad y disponibilidad de los documentos, expedientes o series de documentos, ni del contexto de producción de los documentos y de los metadatos necesarios asociados a los mismos.

0. INTRODUCCIÓN

1. El Esquema Nacional de Interoperabilidad (en adelante, ENI, regulado por el Real Decreto 4/2010) se define en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos como "*…el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deben ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad".* El citado Esquema establece en su Disposición transitoria Primera la obligatoriedad de su implementación en las organizaciones administrativas.

2. La Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos, publicada por Resolución de 28 de junio de 2012 de la Secretaría de Estado de Administraciones Públicas, establece los conceptos relacionados con el desarrollo de políticas de gestión de documentos electrónicos por parte de las Administraciones públicas en el marco de la Administración electrónica, incluyendo los aspectos relacionados con su implantación práctica, e identificación de los requisitos de la gestión de los documentos electrónicos necesarios para la recuperación y conservación de los mismos, así como los procesos y acciones presentes a lo largo de todo su ciclo de vida.

3. Para la elaboración de la Política de Gestión de Documentos Electrónicos del MECD se ha seguido lo especificado en el Modelo de Política de Gestión de Documentos Electrónicos. Asimismo, se ha contado con el documento de Política de Gestión de Documentos Electrónicos del MINHAP en el que ha participado el MECD mediante las aportaciones realizadas por expertos de nuestro Departamento ministerial.

4. Hay que destacar, además, los beneficios de la implantación de la Política, entre los que destacan una mayor transparencia en la actividad Administrativa, un mejor gobierno y una rendición de cuentas más ágil hacia los ciudadanos. Una eficaz gestión de los documentos y expedientes electrónicos generados por la Administración es un elemento clave para llevar a efecto el mandato establecido en la Ley 37/2007 y en la Ley 19/2013.

5. En el caso del MECD, se debe tener muy presente su condición de custodio de los archivos históricos. En efecto, este Departamento, a través de la Dirección General de Bellas Artes y Bienes Culturales y de Archivos y Bibliotecas, tiene específicamente encomendada la responsabilidad de la gestión y la custodia de los documentos y expedientes electrónicos

que, habiendo finalizado su fase activa según sus calendarios de conservación, deben transferirse al archivo intermedio o al archivo histórico, como dispone el Real Decreto 1708/2011.

6. El presente documento de Política de Gestión de Documentos Electrónicos está abierto a futuras reflexiones y actuaciones, como la implementación de un Esquema de Metadatos multientidad; el impulso, en colaboración con el MINHAP, de una Norma Técnica de Interoperabilidad que aborde de manera clara la transferencia de responsabilidad de la gestión y custodia de documentos y expedientes electrónicos a lo largo del ciclo de vida de los mismos; los procedimientos de archivo a largo plazo de la información almacenada en bases de datos de la Administración; la elaboración de un Cuadro de Clasificación funcional consistente para toda la organización, el desarrollo de Tablas de Acceso y Seguridad; la preparación de un Informe o Tabla de Evaluación de Riesgos, etc.

7. Se ha dividido el documento en dos grandes bloques: el **cuerpo principal** (que comprende la Presentación, la Introducción y los Capítulos 1, 2 y 3) y los **anexos** al final del documento.

   En el cuerpo principal se encuentran las disposiciones de esta Política que, previsiblemente, van a ser más duraderas en el tiempo, por derivar de leyes, reglamentos, estándares internacionales y normas técnicas que han sido formalmente aprobadas con el propósito de que estén vigentes durante un período prolongado. Por otra parte, los anexos recogen aquella información complementaria al cuerpo principal que es más susceptible de modificaciones (sean periódicas o puntuales) y cuya actualización no exige de un proceso formal tan riguroso como para las previsiones del cuerpo principal. En los anexos también se recogen especificaciones técnicas que será necesario ir actualizando debido a la rápida evolución de la tecnología y del mercado para dar respuesta a demandas de información o prestaciones de seguridad en continua transformación y crecimiento.

8. Algunos anexos de este documento contienen información que debe clasificarse como de "difusión limitada", debido a que detallan especificaciones técnicas sobre los sistemas informáticos de la organización cuya revelación pública podría aumentar la exposición a incidentes de seguridad deliberados. Tales anexos se mantienen intencionadamente en blanco en la versión pública de esta Política. Aquellas personas u organizaciones que necesiten conocer su contenido íntegro deberán solicitarlo a los Gestores de la Política indicados en el apartado 1.3.2.

Del mismo modo, las referencias a algunos de los documentos o normas en que se basa esta Política no se encuentran disponibles para su consulta pública, bien porque la misma se encuentra sujeta a las condiciones de una licencia de uso, o bien porque están clasificadas con un nivel de seguridad que impide su difusión pública. En tales casos, las personas u organizaciones interesadas deberán contactar con la Organización que produjo el documento original a fin de que les indiquen los procedimientos y condiciones para acceder a su contenido.

9. En la confección de este documento se han tenido en cuenta las recomendaciones en cuanto a estilo y formato recogidas en la "Guía de Comunicación Digital para la Administración del Estado" aprobada por Resolución de 21 de marzo de 2013 de la Secretaría de Estado de Administraciones Públicas. Por otro lado, las disposiciones normativas, estándares, guías y otras fuentes que se citan en este documento se detallan en el Capítulo 3 ("Referencias"), de modo que se inserta un enlace a su detalle explícito en las partes del documento donde sean citadas.

1. POLÍTICA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS

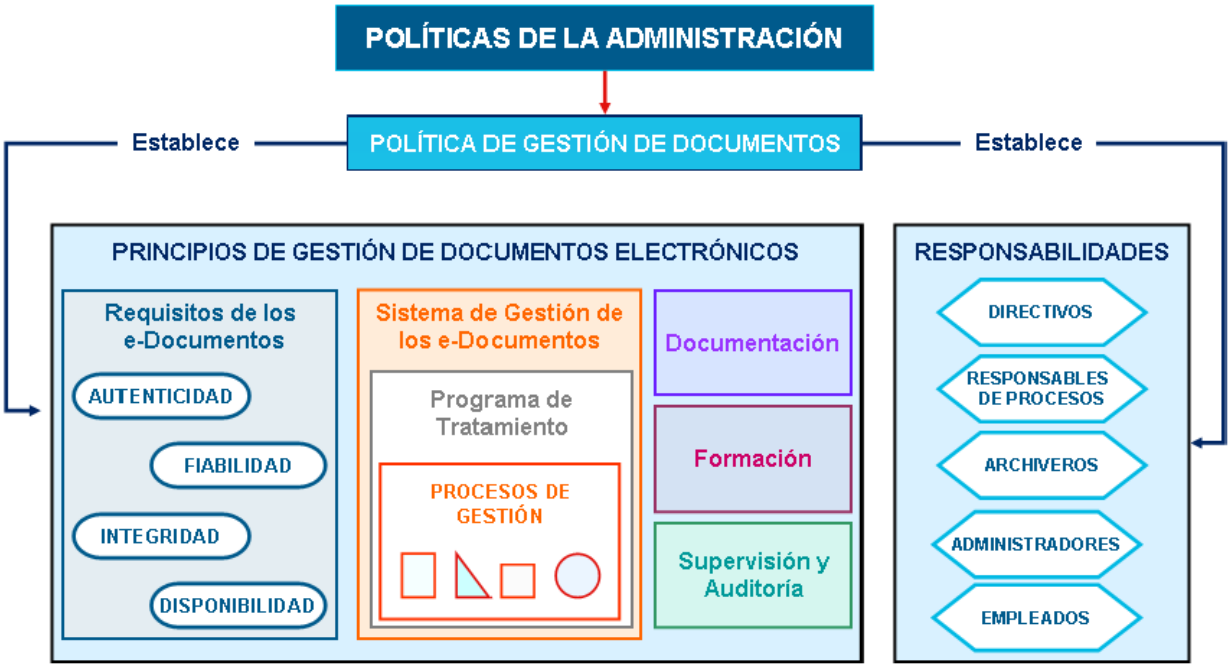
1.1. Referencias

10. Para el desarrollo del contenido de esta Política, se han tenido en cuenta las normas, buenas prácticas y referencias normativas que se enumeran en el apartado 3 de este documento.

1.2. Objeto y Alcance de la Política

11. La presente Política de Gestión de Documentos Electrónicos está integrada en el contexto de la organización junto al resto de las políticas implantadas para el desempeño de sus actividades. En particular, esta política está integrada en el marco general de gestión de documentos del MECD, con independencia del soporte en el que puedan estar materializados dichos documentos.

12. A continuación, se incluye un esquema tomado de la Guía de aplicación de la NTI de Política de Gestión de Documentos Electrónicos, en la cual se incluye el programa de tratamiento de los documentos electrónicos en el contexto de la Política de Gestión de Documentos de la organización, como el elemento que contempla los procesos de gestión documental:



13. La Política de Gestión de Documentos Electrónicos de este Departamento ministerial tiene por objeto establecer el conjunto de criterios comunes asumidos por el MECD así como documentar los mismos, en relación con la gestión de los documentos y expedientes

electrónicos producidos o custodiados por dicho Departamento Ministerial y sus organismos dependientes.

14. Esta Política de Gestión de Documentos Electrónicos persigue elaborar los requisitos necesarios con el fin de crear, mantener, tratar y conservar documentos electrónicos auténticos y fiables, así como proteger la integridad de los mismos durante todo su ciclo de vida (incluida la fase histórica).

    Igualmente, esta Política persigue garantizar la disponibilidad e integridad de los metadatos mínimos obligatorios y, en su caso, los complementarios o necesarios (metadatos de contenido, contexto y estructura) para asegurar la gestión, recuperación y conservación de los documentos y expedientes electrónicos del MECD manteniendo permanentemente su relación.

15. En particular, se integrará con la política de seguridad que establece el Esquema Nacional de Seguridad, puesto que los documentos electrónicos se van a manejar mediante sistemas a los que les es aplicable lo previsto en dicho Esquema.

16. A fin de extender la política a entornos híbridos en los que conviven documentos en soportes analógicos y electrónicos, según el Esquema Nacional de Seguridad, se tendrá en cuenta que *"toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el presente real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos"*.

1.3. Datos identificativos la Política

17. Los datos identificativos principales son:

Nombre del documento	Política de Gestión de Documentos Electrónicos MECD
Versión	1.1 (Versión 1, Revisión 1)
Identificador de la Política[1] y [2]	E04921401_1.1
URI de referencia de la Política	http://intranet.mecd.es/normativa/normativa-de-interes/politica-doc-electronico.html

[1] Código alfanumérico único para cada órgano/unidad/oficina extraído del Directorio Común de Unidades Orgánicas y Oficinas (DIR3).

[2] Los dos últimos dígitos de este identificador corresponderán con la versión de la Política de Gestión de Documentos Electrónicos.

Fecha de expedición	9 de julio de 2015[3]
Fecha de revisión	3 de mayo de 2016 [4]
Entrada en vigor de la revisión	Inmediata, sin necesidad del período de adaptación que señala el apartado 1.3.1
Ámbito de aplicación	Documentos y expedientes producidos y/o custodiados por el Ministerio de Educación, Cultura y Deporte.

1.3.1. Período de validez

18. La presente Política de Gestión de Documentos Electrónicos entrará en vigor en la *fecha de expedición* indicada en los Datos Identificativos y será válida hasta que no sea sustituida o derogada por una política o versión posterior. En este caso, se podrá facilitar un periodo de tiempo transitorio, en el cual convivan las dos versiones, que permita adecuar los diferentes sistemas de gestión de documentos electrónicos utilizados por el MECD a las especificaciones de la nueva versión.

19. Este periodo de tiempo transitorio deberá indicarse en la nueva versión pasado el cual sólo será válida la versión actualizada.

20. Una versión actualizada del texto de la Política (con exclusión de la información indicada en el punto 8 de la Introducción) se publicará en la Intranet corporativa del MECD. También podrá ser publicada en el Portal Web del MECD para facilitar su difusión.

21. Los anexos podrán ser actualizados sin necesidad de un proceso de revisión formal de la Política. Asimismo, las referencias al esquema de metadatos e-EMGDE que se encuentran en el cuerpo principal serán actualizadas automáticamente sin necesidad de un proceso de revisión formal cuando se publiquen las sucesivas versiones del esquema[5].

1.3.2. Identificador del gestor de la Política

Nombre del gestor[6]	Subdirección General de los Archivos Estatales Subdirección General de Tecnologías de la Información y Comunicaciones
Dirección de contacto	Secretaría Archivo (Plaza del Rey) <archivos.estatales@mecd.es> Secretaría SGTIC (Vitruvio) <secretaria.sgtic@mecd.es>

[3] Fecha en que fue aprobado por la CPCMAD (Comisión Permanente de la Comisión Ministerial de Administración Digital).
[4] Fecha en que la revisión fue propuesta por la Comisión Técnica Multidisciplinar prevista en el apartado 1.10
[5] El responsable del mantenimiento de dicho esquema es el Ministerio de Hacienda y Administraciones Públicas.
[6] El titular del órgano con competencia y función específicas en la gestión de documentos y archivos de la entidad.

Identificador del gestor[7]	E03013904 – Subdirección General de los Archivos Estatales E04857803 – Subdirección General de Tecnologías de la Información y Comunicaciones

1.4. Actores y responsabilidades

1.4.1. Actores

22. Los actores involucrados en los procesos de gestión documental contemplados en la presente política serán como mínimo los siguientes:

- La alta dirección, que aprobará e impulsará la Política, que corresponderá a los siguientes actores:
  - A la persona titular del MECD y, por su delegación, a la persona titular de la Subsecretaría.
  - Al Presidente en el caso de una Agencia Estatal.
  - Al Director General en el caso de otros Organismos Públicos.
- Los responsables de procesos de gestión, que aplicarán la Política en el marco de los procesos a su cargo.

  Corresponde esta responsabilidad a las personas titulares de los órganos directivos que tienen atribuida por norma la función a la que responden los diferentes procesos y, por delegación de los mismos, a los titulares de las Subdirecciones competentes.
- El personal responsable de la planificación, implantación y administración del programa de tratamiento de documentos y sus operaciones, cualificado, dedicado e instruido en gestión y conservación documental y que participará en el diseño, implementación y actualización de los sistemas de gestión y conservación documental. Esta categoría incluye tanto a archiveros y expertos en gestión documental como a administradores de sistemas y desarrolladores de aplicaciones.

  El personal implicado cotidianamente en tareas de gestión de documentos electrónicos en el ámbito de su actividad, que aplicará lo establecido en la Política a través del programa de tratamiento implantado.

1.4.2. Responsabilidades

23. La asignación de responsabilidades debe realizarse apropiadamente a todo el personal de la organización en los niveles y funciones pertinentes, como se especifica en las normas ISO 30300:2011 *Información y documentación. Sistemas de gestión para los documentos.*

[7] Código alfanumérico único para cada órgano/unidad/oficina extraído del Directorio Común de Unidades Orgánicas y Oficinas (DIR3).

Fundamentos y vocabulario e *ISO 30301:2011 Información y documentación. Sistemas de gestión para los documentos. Requisitos*.

El objetivo fundamental de la definición y asignación de responsabilidades y competencias es crear y mantener un sistema de gestión de documentos electrónicos que satisfaga las necesidades de todas las partes interesadas, tanto internas como externas a la organización.

Se detallan a continuación las responsabilidades y competencias que deben asumir los actores implicados en los procesos de gestión documental y las responsabilidades que deben asumir en relación a la presente Política.

1.4.2.1. Alta Dirección

24. La Alta Dirección de la entidad integrará la Política de gestión de documentos con el resto de políticas del Departamento o de su organización. Asimismo, deberá ser consciente de los riesgos que supone una gestión inadecuada de sus documentos.

25. A partir de principios tales como: la perspectiva del ciudadano y otras partes interesadas; el liderazgo y responsabilidad; la toma de decisiones basada en la evidencia; la implicación del personal; el enfoque sobre los procesos; y la orientación sistemática de la gestión para una y mejora continua, se trata de:
    - Conseguir coherencia en las operaciones para toda la organización.
    - Asegurar que los procesos de negocio sean transparentes y comprensibles.
    - Garantizar a los consejos de dirección, reguladores, ciudadanos y otras partes interesadas que los documentos se gestionan apropiadamente.

    Para la consecución de estos objetivos tiene las siguientes competencias:

    - Establecer, mantener y promover la Política y objetivos de gestión documental para incrementar la conciencia, motivación y cumplimiento de la organización.
    - Asegurar que las responsabilidades y competencias de la gestión de documentos están definidas, asignadas y comunicadas a toda la organización.
    - Asegurar que se establece, implementa y mantiene una política de gestión efectiva y eficiente para alcanzar los objetivos de la organización.
    - Asegurar la disponibilidad de los recursos y capacitación necesarios para apoyar y mantener dicha Política.
    - Promover su revisión periódica y decidir e impulsar las acciones de mejora precisas.

1.4.2.2. Responsables de procesos de gestión

26. Los responsables de procesos de gestión aplicarán la Política de gestión de documentos en el seno de la organización, y garantizarán el ejercicio de los derechos reconocidos a los ciudadanos. Asimismo, adoptarán las medidas necesarias para la difusión de la Política de Gestión de Documentos Electrónicos y de los procedimientos relacionados con la gestión documental entre todo el personal a su cargo, para que conozca las normas que afecten al desarrollo de sus funciones.

27. Además, determinarán sus necesidades en cuanto a períodos temporales de utilización de la información, contribuyendo así a la elaboración de las Normas de Conservación de las series documentales que son fruto de los procesos que gestionan.

1.4.2.3. Responsables de planificación, implantación y administración del programa de tratamiento de documentos

28. La categoría de personal responsable de la planificación, implantación y administración del programa de tratamiento de documentos y sus operaciones incluye tanto a archiveros y expertos en gestión documental como a administradores de sistemas y desarrolladores de aplicaciones. Los profesionales de la gestión de documentos son responsables de todos los aspectos relacionados con ella, incluidos el diseño, la implementación y el mantenimiento de los sistemas de gestión así como de la formación de usuarios en dicha materia y en las operaciones que afecten a las prácticas individuales.

29. Los archiveros y expertos en gestión documental, en colaboración con los responsables de los procesos de gestión, llevan a cabo la identificación y valoración documental, establecen los Cuadros de Clasificación y las Normas de Conservación de las diferentes series documentales que posteriormente serán dictaminadas por las autoridades archivísticas y participan en la planificación y la implementación de las políticas y los procedimientos de gestión de documentos.

30. Los administradores de sistemas serán responsables de garantizar que toda la información sea precisa y legible y que esté a disposición del personal autorizado para acceder a ella siempre que se necesite.

1.4.2.4. Personal implicado en las tareas de gestión

31. El personal implicado en las tareas de gestión, categoría que incluye a todos los empleados no encuadrados en las anteriores, es responsable de mantener documentos de archivo precisos y completos sobre sus actividades, de hacer un uso apropiado de los sistemas de información que tratan documentos electrónicos, y de suministrar la información requerida por el Sistema de Gestión Documental a efectos de trazabilidad o cumplimiento de normativa.

1.4.2.5. Otros recursos humanos implicados

32. La organización puede contar con personal externo a la misma para cubrir una necesidad puntual de la organización (técnicos de empresas externas en el marco de un contrato de servicios con dicha empresa, alumnos en prácticas, becarios, etc.). Todos ellos deben ser informados de los deberes inherentes a crear, mantener y custodiar los documentos electrónicos en el contexto del Sistema de Gestión Documental del MECD.

    Los recursos humanos externos deben cumplir con las normas establecidas en las políticas de gestión documental y en el marco legal existente (por ejemplo, protección de datos, confidencialidad sobre información sensible, etc.).

1.5. Procesos de gestión documental

33. El punto V de la Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos establece que la gestión de los documentos electrónicos se concretará en un programa de tratamiento específico dentro de la política de gestión de documentos de cada organización.

34. Según la citada NTI y su Guía de Aplicación, el programa de tratamiento concretará el diseño, desarrollo e implantación de los procesos, técnicas y operaciones de gestión de documentos electrónicos, siendo aplicado de manera continua sobre todas las etapas del ciclo de vida de los documentos y expedientes electrónicos.

35. Los procesos de gestión que generen documentos y expedientes electrónicos en la organización deben aplicar esta política y el programa de tratamiento de documentos electrónicos que garantice su materialización. Las características y funcionalidades de los sistemas de gestión de documentos se definen a continuación, aclarando previamente que la gestión de documentos electrónicos debe comprender dos momentos:

- Un primer momento, en el que los documentos todavía no han alcanzado su estado definitivo. En esta etapa, los documentos son objetos dinámicos de información, creados mediante diversas aplicaciones, admiten versiones y cambios y está previsto que su información sea compartida. Se controlan y gestionan mediante Sistemas de Gestión de Documentos Electrónicos (en adelante, SGDE), si bien estas funciones también pueden llevarse a cabo, en la práctica, por las propias aplicaciones de gestión de procesos.
- En un segundo momento, los documentos han alcanzado ya su forma definitiva, se han integrado en sus respectivos expedientes o agregaciones documentales, han sido provistos de mecanismos que aseguran su autenticidad e integridad, de manera que son inalterables, salvo, en su caso, para añadirles metadatos de gestión y conservación o para corregir errores, y se gestionan mediante Sistemas de Gestión de Documentos Electrónicos de Archivo (en adelante, SGDEA).

36. Para facilitar la comprensión de lo expuesto, el Anexo XII recopila un conjunto de diagramas de flujo que muestran el proceso de gestión del documento electrónico en las distintas fases que comprende su ciclo vital.

37. Se recogen a continuación las características y funcionalidades básicas que deben tener los sistemas de gestión de documentos mencionados:
    - SGDE. Siguiendo las especificaciones de MoReq-2, está orientado básicamente al control, almacenamiento y gestión de la documentación de los archivos de oficina y tiene las siguientes características:
        - Permite la modificación de los documentos.
        - Permite la existencia de varias versiones de los documentos.
        - Puede permitir el borrado de los documentos por parte de sus gestores.
        - Puede incluir controles de retención de los documentos.
        - Puede incluir estructuras de almacenamiento de los documentos, bajo el control de los usuarios.
        - Está orientado primariamente a dar soporte a la gestión diaria de los documentos para el desarrollo de los procesos de negocio.
    - SGDEA. Un SGDEA, por el contrario, se caracteriza por lo siguiente:
        - Impide que los documentos de archivo sean modificados.
        - Sólo permite la existencia de una versión final de los documentos.
        - Impide el borrado de los documentos salvo en determinadas circunstancias estrictamente controladas.

- Incluye controles de conservación y eliminación rigurosos.
- Facilita una estructura de organización de los documentos rigurosa, mediante el Cuadro de Clasificación.
- Está dirigido principalmente a proporcionar un repositorio seguro a los documentos fruto de los procesos de negocio aunque, ocasionalmente, puede dar soporte al trabajo de las oficinas.

38. Además, un SGDEA debe poder gestionar calendarios de conservación, seleccionar de modo automático expedientes y documentos para llevar a cabo las acciones dictaminadas para su serie documental, así como detectar aquellos documentos que, por sus circunstancias, deban ser objeto de acciones específicas de conservación. Asimismo, debe poder gestionar el acceso a los expedientes y documentos mediante listas y perfiles de usuario, así como disponer de sistemas de seguimiento y control de las acciones que se realicen sobre los documentos y expedientes.

39. De las características mencionadas anteriormente se desprende que un SGDE se correspondería más con un archivo de oficina, mientras que un SGDEA albergaría documentos y expedientes en sus versiones finales, es decir, en fase de archivo central, intermedio e histórico. Partiendo de la normativa vigente, deben determinarse las condiciones en que debe producirse la transferencia de documentos entre ambos sistemas.

40. Sin embargo, en el momento actual se dan algunas peculiaridades que han de tenerse en cuenta:
    - No es posible establecer una frontera nítida entre los distintos sistemas de gestión de los documentos existentes en el MECD, ya que un mismo sistema alberga documentos de archivo y documentos aún no definitivos.
    - Es frecuente que los controles propios de un SGDEA de cara a la integridad y control de acceso a los documentos no los proporcione un sistema de gestión, sino las propias aplicaciones de gestión.
    - Los documentos no cumplen en muchas ocasiones los requisitos del ENI, ya que se considera que éstos únicamente deben implementarse para la interoperabilidad de los mismos.

41. En consecuencia, se propone que el SGDEA comience en la fase de Archivo Central, momento en que los expedientes y documentos que se transfieran al mismo deberán tener implementados, al menos, los metadatos obligatorios para intercambio del ENI y además los

que se establecen en el perfil de metadatos del MECD como obligatorios para la transferencia con cambio de responsabilidad de la custodia y la gestión.

42. Dicho programa de tratamiento se aplicará de manera continua sobre todas las etapas o periodos del 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 física y lógica de los documentos y su contexto.

43. En el futuro, se tenderá, en la medida de lo posible, al uso de las mismas aplicaciones de gestión documental en el ámbito del Ministerio y sus organismos dependientes, en función de la que se determine de máxima utilidad para los objetivos pretendidos y de mayor grado de interoperabilidad.

44. En el Anexo I a este documento, y como relación actualizable periódicamente, sin necesidad de modificar el documento, se incluye una lista de programas de gestión documental existentes en el Ministerio y sus organismos y entidades dependientes.

45. Cuando se precise formalizar contratos con empresas para la externalización de determinados procesos de gestión documental (como podrían ser la digitalización de archivos en papel, la destrucción segura de documentos…), se recomienda incluir una cláusula por la que se exija a las empresas adjudicatarias acreditar los niveles de idoneidad técnica establecidos en los estándares sectoriales que sean de aplicación. En todo caso, se recogerá una cláusula de confidencialidad de obligado cumplimiento para las empresas adjudicatarias.

1.5.1. Captura

46. La captura del documento electrónico es el proceso que señala su entrada en un sistema de gestión de documentos electrónicos y garantiza su identificación unívoca. En el momento de la captura se establece una relación entre el documento, su productor o creador y el contexto en que se originó. Este propósito se consigue mediante la asignación de los metadatos mínimos obligatorios definidos en la NTI de Documento Electrónico, así como mediante la asignación al documento de un identificador único.

47. La captura de un documento electrónico puede venir precedida por un proceso de digitalización del documento, así como por un proceso de conversión de formato entre documentos, ambos procedimientos con arreglo a sus respectivas Normas Técnicas de Interoperabilidad. Asimismo, la captura, una vez llevada a cabo, se puede completar con otros

procesos y operaciones de gestión de documentos, tales como el registro administrativo, la clasificación o su inclusión en el índice de un expediente electrónico.

48. No obstante, hay que insistir en que el proceso de captura es independiente del resto de procedimientos mencionados anteriormente, los cuales pueden o no tener lugar sobre el mismo documento.

49. La fecha de captura del documento se corresponderá con la fecha de su ingreso en el sistema de gestión documental (SGDE) empleado en la organización. Esta fecha puede diferir de su fecha de digitalización. También podrá diferir de la fecha de registro administrativo del documento, cuando se verifique el mismo.

50. El identificador único asignado a los documentos electrónicos capturados seguirán la codificación:

ES_<ÓRGANO>_<AAAA>_<ID_ESPECIFICO>	
<ÓRGANO>	Se codificará según lo establecido en el Directorio Común (DIR3)
Ejemplos	E04921401 Ministerio de Educación, Cultura y Deporte E00123603 Museo Nacional del Prado E03019905 Dirección Provincial de Educación de Ceuta
<AAAA>	Año de la fecha de captura del documento
<ID_ESPECIFICO>	Código alfanumérico[8] que identifica de forma única al documento dentro de los generados por la administración responsable, con tamaño máximo de 30 caracteres

51. Se señalan a continuación aquellos metadatos mínimos obligatorios definidos por la NTI de Documento Electrónico que deben completarse en el momento de la captura del documento, cuyos valores sería difícil o imposible recuperar en fases posteriores de la gestión documental.

Metadato	Asignación en punto de captura de SGDE	Asignación en cualquier momento
Versión NTI	✓	
Identificador	✓	
Órgano	✓	
Fecha de captura	✓	

[8] Se recomienda utilizar un código secuencial o un identificador automático generado por el propio programa de tratamiento (SGDE).

Metadato	Asignación en punto de captura de SGDE	Asignación en cualquier momento
Origen	✓	
Estado de elaboración	✓	
Nombre del Formato	✓	
Tipo documental		✓
Tipo de firma	✓	
Valor CSV[9]	✓	
Definición generación CSV[10]	✓	
Identificador del documento origen[11]	✓	

52. Del mismo modo, se cumplimentarán los metadatos mínimos obligatorios de los expedientes electrónicos en el momento de su creación, ya que con respecto al expediente electrónico no se puede hablar en sentido estricto de fase de captura. Tales metadatos, que aparecen relacionados en la NTI de Expediente Electrónico, son los siguientes:

Metadato	Asignación en momento de creación	Asignación en cualquier momento
Versión NTI	✓	
Identificador	✓	
Órgano	✓	
Fecha apertura expediente	✓	
Clasificación	✓	
Estado		✓
Interesado		✓
Tipo de firma	✓	
Valor CSV[8]	✓	
Definición generación CSV[9]	✓	

[9] Estos metadatos sólo aparecen si el "Tipo de Firma" es CSV.
[10] Ídem a nota anterior.
[11] Este metadato sólo aparece si el "Estado de elaboración" es "Copia electrónica auténtica con cambio de formato" o "Copia electrónica parcial auténtica".

1.5.2. Registro

53. A los efectos de la presente Política de Gestión de Documentos Electrónicos, se entiende por Registro el proceso de control mediante la correspondiente inscripción registral de los documentos generados o recibidos por los órganos administrativos del MECD.

54. 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 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. De acuerdo con dicha ley, 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.

55. El sistema de registro del MECD está constituido por el Registro General, ubicado en los Servicios Centrales, por los Registros Auxiliares del Registro General, ubicados en los diferentes órganos y Dependencias del Departamento, así como por los Registros Electrónicos creados con arreglo al artículo 25 de la Ley 11/2007.

56. El proceso de registro deberá adecuarse a lo establecido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, una vez la misma entre en vigor y, más concretamente, a lo dispuesto en su artículo 16 relativo al Registro Electrónico General de la AGE, a las oficinas de asistencia en materia de registros y a la conversión en formato electrónico de las solicitudes presentadas en papel.

57. Un inventario de todos los registros del MECD, así como de los Registros Electrónicos y sus disposiciones de creación, debidamente aprobados, se ha recopilado en el Anexo II de este documento y será actualizado periódicamente, sin que por ello deba modificarse el documento de Política de Gestión de Documentos Electrónicos del MECD.

58. Con el fin de garantizar la interconexión entre oficinas registrales y el acceso por medios electrónicos a los asientos registrales y a las copias electrónicas de los documentos presentados, previsto en el artículo 24.4 de la Ley 11/2007, la información mínima necesaria para realizar el intercambio de un asiento registral así como la estructura de dicha información y los requisitos tecnológicos mínimos que deben cumplirse durante el intercambio y se adaptarán a los requisitos que se especifican en la Norma Técnica de Interoperabilidad de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales, aprobada por Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública.

1.5.2.1. Documentación en soporte papel

59. Todo documento en soporte papel que se presente en las Oficinas de Registro del Departamento deberá producir un asiento registral y la copia a devolver al interesado deberá llevar el correspondiente acuse de recibo que acredite la presentación del mismo, salvo que no pudiera obtenerse en el momento, en cuyo caso se deberá estampar en dicha copia un sello de registro en el que figure la fecha de entrada del documento.

60. Recibida la documentación se procederá a realizar el asiento registral, cumplimentando los datos solicitados por la aplicación informática de acuerdo con la información disponible en las oficinas de registro.

61. Salvo en los supuestos previstos en el ordenamiento jurídico, de acuerdo con lo dispuesto en el artículo 27.4 del Real Decreto 1671/2009, por el que se desarrolla parcialmente la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos, los dispositivos de recepción de fax no tendrán la consideración de registro electrónico. No obstante, los documentos recibidos vía fax podrán ser digitalizados a los meros efectos de obtener una imagen de los mismos que incorporar, en su caso, al expediente electrónico.

62. Todos los documentos en soporte papel presentados en las oficinas de registro podrán ser digitalizados con el fin de obtener una copia electrónica auténtica, de acuerdo con lo previsto en el artículo 50 del Real Decreto 1671/2009. En la medida de lo posible, se dotará a las oficinas de Registro con los medios técnicos necesarios para la digitalización.

63. Se exceptúan de lo previsto en el párrafo anterior los siguientes supuestos:
    - Los sobres cerrados presentados en las oficinas de Registro en el marco de licitaciones públicas, ya sean enajenaciones forzosas en procedimientos de recaudación o en procedimientos de contratación pública, que no se abrirán ni escanearán.
    - Otras excepciones específicas que puedan existir en cada centro o entidad.
    - En este caso, los documentos deberán ser remitidos inmediatamente a sus destinatarios, en sobre cerrado.

64. El procedimiento de digitalización se llevará a cabo en cualquier caso cumpliendo las especificaciones de las Normas Técnicas de Interoperabilidad de Digitalización y de Documento Electrónico, y en particular, el protocolo de digitalización a que se refiere el apartado 2.2 de esta Política.

1.5.2.2. Metainformación del asiento registral y de los documentos anexos

65. La metainformación descriptiva referente al asiento registral que debe ser introducida de modo automático o manual en el ámbito de la Unidad de Registro es la que se contempla en el *ap*artado IV.2 *Estructura y contenido del mensaje de datos de intercambio*, de la NTI de Modelo de Datos de Intercambio de asientos registrales entre unidades SICRES 3.0. Los niveles de obligatoriedad de la cumplimentación de cada metadato serán los indicados en la mencionada Norma para cada uno de los siete segmentos de los que consta la estructura del asiento.

66. En caso de incluirse como anexos documentos digitalizados conforme a la NTI de Digitalización de Documentos, la metainformación referente a estos últimos (según apartado III.1.b de la mencionada Norma) será la definida como mínima obligatoria en el Anexo I de la NTI de Documento Electrónico, aprobada por Resolución de la misma fecha de dicha Secretaría de Estado. Podrán asociarse, además, de forma complementaria, metadatos relacionados con el proceso de digitalización que reflejen las características técnicas de la imagen electrónica capturada.

1.5.3. Clasificación

1.5.3.1. Criterios de formación de expedientes electrónicos y agregaciones de documentos

67. En el Anexo del ENI se define un documento electrónico como "información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado". El documento electrónico constituye la base para conformar tanto expedientes como agregaciones de documentos electrónicos.

    Siempre que sea posible, dichos expedientes y agregaciones estarán constituidos exclusivamente por documentos electrónicos, excepto cuando por la naturaleza del procedimiento fuera necesario mantener expedientes híbridos que contengan documentación en soporte no electrónico.

    Para evitar la generación de expedientes híbridos, se digitalizarán y se obtendrán copias electrónicas auténticas de los documentos en papel, de modo que serán estas copias las que se incorporen al expediente electrónico.

68. Los expedientes electrónicos y agregaciones de documentos electrónicos producidos por la entidad atenderán a los siguientes criterios de formación y patrones:

- Expedientes electrónicos:
  - Están definidos en el artículo 32 de la Ley 11/2007 como el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan.
  - Según el artículo 41.2 del Real Decreto 1671/2009 y el apartado IV de la NTI de Documento Electrónico, los documentos administrativos electrónicos, y aquellos susceptibles de formar parte de un expediente, tendrán siempre asociada al menos una firma electrónica de acuerdo con la normativa aplicable.
  - En el expediente electrónico se integran aquellos documentos, administrativos o no, que deban formar parte del mismo por ser el resultado de las actuaciones de la Administración encaminadas a la resolución administrativa de un asunto. No se integrarán en el expediente las versiones de documentos salvo que deban figurar por razón de su normativa específica, en cuyo caso deberán firmarse electrónicamente.
  - En el caso de documentos con anexos, se tratarán, a efectos de validación, como un único documento, o como documentos independientes, vinculados entre sí.
  - Una vez cerrado, el expediente electrónico quedará foliado mediante un índice electrónico en el que se relacionarán todos los documentos que lo componen. Dicho índice será firmado por la Administración, órgano o entidad actuante, que garantiza así la integridad del expediente.
  - El índice electrónico de los expedientes objeto de intercambio reflejará al menos:
    - Fecha de generación del índice (ya que refleja el estado del expediente en un determinado momento).
    - Para cada documento electrónico: su identificador, su huella digital, la función resumen y, opcionalmente, la fecha de incorporación al expediente.
  - La fecha de incorporación al expediente es opcional porque:
    - En algunos casos se desconoce.
    - En la mayoría, cobra más importancia la fecha de firma o publicación del documento, momento en que empieza el plazo legal.
  - El orden del documento en el expediente será un tipo cadena de caracteres, no necesariamente un índice entero.
  - Si es el caso, la disposición de los documentos en carpetas y expedientes electrónicos anidados.
  - Firma del índice electrónico por la Administración, órgano o entidad actuante, mediante los sistemas de firma previstos en el artículo 18 (sello electrónico de

administración pública o código seguro de verificación) ó 19 (firma electrónica del personal al servicio de las Administraciones públicas) de la Ley 11/2007. Los órganos administrativos podrán añadir elementos complementarios a la estructura del índice, siempre que ello no afecte a la interoperabilidad del expediente.

- Agregaciones documentales:

  De acuerdo con lo dispuesto en el apartado II.2 de la NTI de Expediente Electrónico, entendemos por "agregaciones documentales" aquellos conjuntos de documentos electrónicos que, habiendo sido creados al margen de un procedimiento reglado, se hubiesen formado mediante agregación, como resultado de una secuencia de actuaciones coherentes que conducen a un resultado específico.

  Dado que no son consecuencia de un procedimiento, podrán carecer de valor jurídico y, por ello, su formalización como documentos administrativos electrónicos (con contenido, firma y metadatos) seguramente será excepcional.

  No obstante, su tratamiento a efectos de gestión documental debería ser análogo al de los expedientes sujetos a un procedimiento, lo que exigiría que reunieran las siguientes características:

  - Sólo deben integrarse en la agregación documentos finales, se deben excluir los borradores.
  - Los documentos deben estar dotados de un identificador único.
  - Todos los documentos deben estar fechados.
  - La agregación documental debe considerarse cerrada en un momento determinado, sin admitir nuevos documentos.
  - Los documentos deben reseñarse también en un índice electrónico.
  - Aunque no tengan firma, se debe obtener el *hash* del documento, lo que garantizaría, al menos, su integridad.
  - El índice electrónico recopilará el identificador, la huella, la fecha de los documentos y el orden dentro de la agregación, si es relevante.
  - En la medida de lo posible, se asignarán metadatos análogos a los obligatorios de expediente electrónico. El e-EMGDE, incluye, de hecho, la Agregación como una categoría más de la entidad Documento.

- Documentos simples:

  También es posible aplicar la Clasificación documental a documentos simples, que no estén integrados en un expediente electrónico ni en una agregación documental. Su tratamiento a efectos de gestión documental deberá reunir las características siguientes:

- Sólo se deben almacenar documentos finales, excluyendo los de otra naturaleza, como los borradores de documento.
- Los documentos deben estar dotados de un identificador único.
- Todos los documentos deben estar fechados.
- Todos los documentos deben estar firmados electrónicamente.
- En el caso de documentos con anexos, se tratan, a efectos de validación, como un único documento, o como documentos independientes, vinculados entre sí.
- El documento debe tener asignados los metadatos correspondientes según la NTI relativa al Documento Electrónico.

1.5.3.2. Cuadro de clasificación funcional

69. El Cuadro de Clasificación funcional aparece claramente definido en:

- El artículo 21 del ENI establece que:

  "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:

  …

  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 Real Decreto 1708/2011, 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 NTI 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 agregación 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. La Clasificación funcional aplicada sobre los documentos

no debe perder, en ningún caso, la información de contexto sobre el productor que ha generado o recibido los documentos objeto de clasificación."

- La Norma UNE-ISO 15489, por su parte, al tratar el proceso de gestión de Clasificación en su apartado 9.5.1., dice:

  "La Clasificación de las actividades de la organización representa una poderosa herramienta para el desarrollo de las mismas y para muchos procesos de gestión, como:

  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 modo 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 disposición apropiados."

70. La clasificación de los documentos y expedientes atenderá a los pertinentes cuadros de clasificación, desarrollados específicamente por el MECD y sus organismos autónomos. Dichos cuadros de clasificación se incorporarán como anexo a este documento (en concreto, el Anexo III) y serán actualizados sistemáticamente siempre que haya alguna modificación normativa, estructural o funcional que les afecte, sin necesidad de modificar el documento de Política de Gestión de Documentos Electrónicos.

71. El Cuadro actual de Clasificación elaborado para el MECD es de naturaleza orgánico-funcional, considerando tanto el órgano o unidad que origina el documento como la finalidad del mismo.

72. El Cuadro de Clasificación funcional se realizará en el plazo máximo de un año desde la aprobación de este documento de gestión de política documental. La Alta Dirección de la organización impulsará la sensibilización de las diferentes oficinas que producen y gestionan los documentos y expedientes con el fin de que proporcionen los datos necesarios para poder materializar el citado cuadro.

1.5.3.3. Repertorio de series documentales

73. En tanto se apruebe el Cuadro de Clasificación, para la puesta en marcha del sistema de gestión de documentos se elaborará un repertorio de series documentales del MECD, que se incorporará como Anexo III a este documento desde el mismo momento de su aprobación. El Anexo del repertorio de series será actualizado periódicamente, sin necesidad de que dicha actualización implique modificación de este documento de Política de Gestión de Documentos Electrónicos.

1.5.3.4. Situación transitoria hasta la elaboración del Cuadro de Clasificación funcional

74. Dada la necesidad de contar con algún tipo de clasificación que permita poner en marcha el sistema de gestión de documentos, ésta se realizará sobre la base del Repertorio de Series, identificadas, en su caso, por su código SIA, en tanto no se disponga de un Cuadro de Clasificación.

75. Tanto las series identificadas como el posterior Cuadro de Clasificación figurarán en anexos al documento de Política de Gestión (en el caso que nos ocupa, el III), de manera que puedan ser modificados sin alterar el contenido del documento.

1.5.4. Descripción

76. La descripción de los documentos y expedientes electrónicos permitirá la recuperación de los mismos y su contexto, y atenderá a la aplicación del esquema institucional de metadatos.

77. El proceso de descripción archivística se realizará fundamentalmente sobre los Paquetes de Información de Archivo (PIA) en las fases de archivo central y, sobre todo, de archivo intermedio e histórico con el fin de facilitar la recuperación de la información y la investigación histórica.

1.5.4.1. Orientaciones y requisitos tenidos en cuenta para la construcción de un esquema de metadatos

78. De acuerdo con el apartado VII de la NTI de Política de Gestión de Documentos Electrónicos:
    - Las organizaciones garantizarán la disponibilidad e integridad de los metadatos de sus documentos electrónicos, manteniendo de manera permanente las relaciones entre cada documento y sus metadatos.

- 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 Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE), disponible en el Centro de Interoperabilidad Semántica, que incluye los metadatos mínimos obligatorios, definidos en las Normas Técnicas de Interoperabilidad de Documento Electrónico y Expediente Electrónico, así como otros metadatos complementarios pertinentes en una política de gestión y conservación de documentos electrónicos, podrá ser utilizado como referencia para la adecuación a los requisitos de interoperabilidad en materia de gestión documental.

79. En concordancia con las directrices de la ISO 23081, para una organización es más eficaz y sencillo adoptar un esquema normalizado de metadatos (como el e-EMGDE) ya existente, que esté bien diseñado, y cuente con apoyo institucional, que construir un esquema específico. La construcción de un esquema nuevo implicaría la necesidad de gestionarlo y mantenerlo durante el tiempo de vida de los documentos, incluyendo la actualización del esquema y la verificación 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.

80. Por los motivos expuestos, y dado que el esquema de metadatos recomendado por el ENI es el e-EMGDE, partiremos del mismo para establecer un perfil de metadatos para el MECD, 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 ENI con un esfuerzo de desarrollo moderado.

81. Siempre que sea posible, se deberá evitar introducir un elemento nuevo, dado que reduce la interoperabilidad. En consecuencia, si fuera necesario introducir algún cambio, se limitarían a introducir:
    - Mejoras específicas, es decir, subelementos adicionales.

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

82. El Anexo IV recoge el perfil de aplicación del MECD, con una selección de los metadatos considerados más importantes y de uso más generalizado. No obstante, cada centro o entidad podrá adoptar los metadatos que considere necesarios o aconsejables en su gestión, y en este sentido todo el e-EMGDE se considera metadatos recomendados.

83. Aunque el e-EMGDE se pensó en un inicio como un modelo multientidad, el desarrollo posterior del mismo por parte del Ministerio de Hacienda y Administraciones Públicas se ha limitado a un modelo monoentidad. Con el fin de optimizar los recursos que proporcionaría el modelo relacional, se avanzará progresivamente y en colaboración con otros departamentos ministeriales para estructurar el Modelo de Metadatos Multientidad y fortalecer el contexto de producción de los documentos y expedientes electrónicos.

1.5.4.2. Perfil de aplicación para el MECD del Esquema institucional de metadatos[12]

METADATOS OBLIGATORIOS NTI DE DOCUMENTO Y EXPEDIENTE ELECTRÓNICO
e-EMGDE2 – IDENTIFICADOR e-EMGDE2.1 - SECUENCIA DE IDENTIFICADOR
e-EMGDE4 - FECHAS e-EMGDE4.1 - FECHA INICIO
e-EMGDE14 - CARACTERÍSTICAS TÉCNICAS e-EMGDE14.1 – FORMATO e-EMGDE14.1.1 – NOMBRE DEL FORMATO e-EMGDE14.1.2 – EXTENSIÓN DEL FICHERO
e-EMGDE17 – FIRMA e-EMGDE17.1 - TIPO DE FIRMA e-EMGDE17.2 – VALOR DEL CSV *(Si tipo de firma es TF01 (CSV))* e-EMGDE17.3 - DEFINICIÓN GENERACIÓN CSV
e-EMGDE18 - TIPO DOCUMENTAL
e-EMGDE20 - ESTADO DE ELABORACIÓN

[12] Se toma como referencia el borrador del documento Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE) correspondiente al 20 de noviembre de 2014.

METADATOS OBLIGATORIOS NTI DE DOCUMENTO Y EXPEDIENTE ELECTRÓNICO
e-EMGDE22 – CLASIFICACIÓN ***(Para expediente)***   e-EMGDE22.1 - CÓDIGO DE CLASIFICACIÓN
e-EMGDE23 – VERSIÓN NTI
e-EMGDE24 – ÓRGANO
e-EMGDE25 – ORIGEN DEL DOCUMENTO
e-EMGDE26 – IDENTIFICADOR DEL DOCUMENTO ORIGEN ***(Si estado de elaboración es EE02, EE03 o EE04)***
e-EMGDE27 – ESTADO DEL EXPEDIENTE
e-EMGDE28 – INTERESADO

METADATOS COMPLEMENTARIOS MÍNIMOS NECESARIOS PARA LA TRANSFERENCIA DE DOCUMENTOS Y EXPEDIENTES ELECTRÓNICOS ENTRE REPOSITORIOS CON CAMBIO DE CUSTODIA
e-EMGDE1 – CATEGORIA
e-EMGDE4.2 - FECHA FIN
e-EMGDE8 – SEGURIDAD e-EMGDE8.4 - SENSIBILIDAD DATOS DE CARÁCTER PERSONAL e-EMGDE8.5 - CLASIFICACIÓN ENS e-EMGDE8.6 - NIVEL DE CONFIDENCIALIDAD DE LA INFORMACIÓN SEGÚN GUIA CCN-STIC-803
e-EMGDE9 - DERECHOS DE ACCESO, USO Y REUTILIZACIÓN e-EMGDE9.1 –TIPO DE ACCESO e-EMGDE9.1.1 – CÓDIGO CAUSA LIMITACIÓN e-EMGDE9.1.2 – CAUSA LEGAL/NORMATIVA DE LIMITACIÓN e-EMGDE9.2– CONDICIONES DE REUTILIZACIÓN
e-EMGDE13 – CALIFICACIÓN e-EMGDE13.1 – VALORACIÓN e-EMGDE13.1.1 – VALOR PRIMARIO e-EMGDE13.1.1.1. TIPO DE VALOR e-EMGDE13.1.1.2. PLAZO e-EMGDE13.1.2 – VALOR SECUNDARIO e-EMGDE13.2 – DICTAMEN e-EMGDE13.2.1 - TIPO DE DICTAMEN e-EMGDE13.2.2 - ACCIÓN DICTAMINADA e-EMGDE13.2.3 – PLAZO DE EJECUCIÓN DE LA ACCIÓN DICTAMINADA e-EMGDE13.3 –TRANSFERENCIA e-EMGDE13.3.1 – FASE DE ARCHIVO e-EMGDE13.3.2. – PLAZO DE TRANSFERENCIA e-EMGDE13.4. – DOCUMENTO ESENCIAL
e-EMGDE22 – CLASIFICACIÓN e-EMGDE22.2 DENOMINACIÓN DE CLASE e-EMGDE22.3 TIPO DE CLASIFICACIÓN (SIA/FUNCIONAL)

METADATOS COMPLEMENTARIOS RECOMENDADOS PARA LA GESTIÓN ÓPTIMA DE DOCUMENTOS Y EXPEDIENTES ELECTRÓNICOS
e-EMGDE29 – ASIENTO REGISTRAL e-EMGDE 29.1 – TIPO DE ASIENTO REGISTRAL e-EMGDE 29.2 – CÓDIGO DE LA OFICINA DE REGISTRO e-EMGDE 29.3 – FECHA DEL ASIENTO REGISTRAL e-EMGDE 29.4 – NÚMERO DE ASIENTO REGISTRAL
e-EMGDE3 - NOMBRE e-EMGDE3.1 - NOMBRE NATURAL e-EMGDE3.3 – NOMBRE DEL FICHERO
e-EMGDE5 – DESCRIPCION
e-EMGDE11 – IDIOMA
e-EMGDE12 - PUNTOS DE ACCESO e-EMGDE12.1 - TÉRMINO PUNTO DE ACCESO e-EMGDE12.2 - ID PUNTO DE ACCESO e-EMGDE12.3 - ESQUEMA PUNTO DE ACCESO
e-EMGDE14 – CARACTERÍSTICAS TÉCNICAS e-EMGDE14.2 - VERSIÓN DE FORMATO e-EMGDE14.3 – RESOLUCIÓN e-EMGDE14.4 – TAMAÑO e-EMGDE14.4.2 – TAMAÑO LÓGICO e-EMGDE14.5– PROFUNDIDAD DE COLOR
e-EMGDE15 – UBICACIÓN e-EMGDE15.1 – SOPORTE e-EMGDE15.2 – LOCALIZACIÓN
e-EMGDE16 – VERIFICACIÓN DE INTEGRIDAD e-EMGDE16.1 – ALGORITMO e-EMGDE16.2 – VALOR
e-EMGDE17 – FIRMA e-EMGDE17.1 - TIPO DE FIRMA e-EMGDE17.4 – FIRMANTE e-EMGDE17.4.1 - NOMBRE Y APELLIDOS O RAZÓN SOCIAL e-EMGDE17.4.2 - NUMERO DE IDENTIFICACIÓN DEL/DE LOS FIRMANTE/S e-EMGDE17.4.3 - EN CALIDAD DE e-EMGDE17.4.4 - NIVEL DE FIRMA e-EMGDE17.5.5 – INFORMACIÓN ADICIONAL

METADATOS COMPLEMENTARIOS RECOMENDADOS PARA LA GESTIÓN ÓPTIMA DE DOCUMENTOS Y EXPEDIENTES ELECTRÓNICOS
e-EMGDE21 – TRAZABILIDAD e-EMGDE21.1 – ACCIÓN e-EMGDE21.1.1 – FECHA DE LA ACCIÓN e-EMGDE21.1.2 – ENTIDAD DE LA ACCIÓN e-EMGDE21.2 - MOTIVO REGLADO e-EMGDE21.3 - USUARIO DE LA ACCIÓN e-EMGDE21.4 -HISTORIA DEL CAMBIO e-EMGDE21.4.1 – NOMBRE DEL ELEMENTO e-EMGDE21.4.2 – VALOR ANTERIOR

84. Para la descripción de los documentos y expedientes se tendrán en cuenta recursos como los siguientes:
    - Tesauros.
    - Vocabularios de lenguaje controlado.
    - Índices de materias.
    - Otros.

85. Se tendrá en cuenta en el futuro el desarrollo de recursos de este tipo que ayuden en la gestión documental, y se añadirán como anexo (en el presente documento corresponde al V) al documento, de manera que su actualización o alteración no supondrá modificación del documento de Política de Gestión de Documentos Electrónicos. Mientras tanto, podrán usarse las herramientas existentes en las distintas unidades, si bien hay que tener en cuenta que al no estar normalizados, estos recursos específicos de las unidades pueden carecer de utilidad para el archivo receptor una vez realizadas las transferencias.

1.5.5. Acceso y Trazabilidad

86. El acceso a los documentos y expedientes electrónicos, sus índices y metadatos asociados deben ser sometidos a un control de acceso en función de los datos contenidos en los documentos almacenados. El SGDE/SGDEA debe asegurar la identificación de los usuarios y el control de acceso, sus permisos y responsabilidades, así como el cumplimiento de las garantías previstas en la legislación relativa a restricciones en materia de acceso. Además, debe asegurar que quede traza de todas las acciones que se realicen sobre cada uno de los documentos y expedientes electrónicos y sus metadatos asociados, siguiendo lo establecido en la política de seguridad adoptada por parte de la organización.

87. El sistema debe ser capaz de resistir, con un determinado nivel de confianza, los accidentes y las acciones ilícitas o mal intencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o trasmitidos y de los servicios ofrecidos, o a través de los cuales se realiza el acceso.

88. Se deberán establecer los criterios que determinen los privilegios y las restricciones de acceso a las distintas entidades relacionadas con los documentos, de manera que se garantice la protección lógica y física de las mismas.

89. Desde el punto de vista operativo, la implementación de la seguridad deberá realizarse estableciendo los correspondientes perfiles, roles y derechos de los usuarios en las aplicaciones de gestión documental.

1.5.5.1. Requisitos de Seguridad y Acceso

90. La seguridad de la información es un proceso transversal que tiene como objetivo final la preservación de la confidencialidad, la integridad y la disponibilidad de la información.

91. Los requisitos de seguridad y acceso que hay que tener en cuenta afectan:
    - A los propios documentos donde habrá que implementar metadatos que informen sobre las restricciones de acceso incluyendo, además, mecanismos que permitan ofrecer un acceso parcial a los mismos, ocultando los datos y contenidos objeto de protección.
    - Al SGDE/SGDEA en su conjunto con el fin de evitar el acceso a usuarios no autorizados a los documentos y expedientes, según lo establecido en la norma ISO 15489.

92. Las Tablas de Acceso y Seguridad son el instrumento formal que contempla la norma ISO 15489, en su apartado 4.2.5, para la identificación de los derechos de acceso y el régimen de restricciones aplicables a los documentos. Se conforman como una clasificación de categorías de documentos en función de sus restricciones de acceso y condiciones de seguridad.

93. De acuerdo con la Política de Seguridad de la organización, cada uno de los documentos almacenados en el SGDE/SGDEA tendrá asignado un nivel de acceso. Este nivel de acceso determinará el grado de confidencialidad de la información que contiene y, como consecuencia, qué personas están autorizadas para consultar y modificar el documento.

94. Previamente, y con el fin de definir dichos niveles y posteriormente poder establecer las bases para elaborar tablas de acceso y seguridad, es recomendable:

- Recopilar las fuentes jurídicas y políticas que han de gobernar el acceso y la seguridad de la información presente en los documentos de la organización.
- Definir las categorías de información susceptibles de protección y los plazos de acceso a cada una de ellas a tenor de las fuentes recopiladas, así como los requisitos de seguridad de la información que afectan a la organización.
- Identificar las categorías de información susceptibles de protección que contiene cada serie documental y asignar a cada una de ellas los controles de acceso y uso acordes al nivel de seguridad correspondiente a dichas categorías.
- Aprobar la tabla de acceso y seguridad y plasmar sus requisitos en las herramientas del sistema.

1.5.5.2. Requisitos de acceso a la información contenida en la entidad Documento

1.5.5.2.1. Categorías de acceso

95. Según el elemento 9.1 del e-EMGDE (Tipos de acceso), las categorías de acceso existentes son: "Libre acceso" y "Acceso restringido".

96. Además de las anteriores, se debería contemplar una nueva categoría, "Parcialmente restringido", aunque dicho valor no figure como tal en el elemento mencionado. Su inclusión responde a la necesidad de reflejar aquellos casos en los que un expediente de libre acceso puede contener uno o más documentos de acceso restringido. Por lo tanto, la categoría tipo de acceso se definirá, con carácter general, al nivel más bajo posible: el de Documento simple, tal y como se refleja en las categorías del e-EMGDE para la entidad Documento.

1.5.5.2.1.1. Libre acceso

97. Será de aplicación a la citada entidad el elemento 9.1 del e-EMGDE, elemento obligatorio para la información de libre acceso y particularmente relevante cuando la información contenida esté sujeta a un régimen de especial publicidad. Se debe incluir información sobre los contenidos afectados y la referencia normativa correspondiente, especialmente a la Ley 19/2013. En concreto, se utilizará el elemento 9.2 del e-EMGDE cuando la información contenida sea objeto de transparencia activa o reutilización.

1.5.5.2.1.2. Acceso restringido

98. La inclusión de los metadatos relativos a acceso es necesaria para todos los documentos inscritos en esta categoría.

1.5.5.2.1.2.1. Contenidos susceptibles de protección.

99. Es necesario incluir información sobre los contenidos susceptibles de protección y la referencia normativa correspondiente. Para ello, tal y como se definen en la LTAIBG y excluyendo la información con datos de carácter personal, se puede utilizar para codificar los contenidos afectados el esquema de valores definido para el metadato e-EMGDE 9.1.1 (Código de la causa de limitación), incluido en la siguiente tabla:

Cód.	Código y contenidos de información con acceso restringido	Art. LTAIBG
A	Seguridad nacional	14.1.a
B	Defensa	14.1.b
C	Relaciones exteriores	14.1.c
D	Seguridad pública	14.1.d
E	Prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios	14.1.e
F	Igualdad de las partes en los procesos judiciales y tutela judicial efectiva	14.1.f
G	Funciones administrativas de vigilancia, inspección y control	14.1.g
H	Intereses económicos y comerciales	14.1.h
I	Política económica y monetaria	14.1.i
J	Secreto profesional. Propiedad intelectual e industrial	14.1.j
K	Garantía de la confidencialidad o secreto requerido en procesos de toma de decisión	14.1.k
L	Protección del medio ambiente	14.1.l
M	Otros intereses públicos susceptibles de protección	-
N	Otros intereses privados susceptibles de protección	-

100. El e-EMGDE recoge en el Apéndice 11 valores específicos para la información especialmente reservada, que podrán ser aplicados sobre la tabla anteriormente mencionada.

101. Para la entidad documento se aplicarán los elementos 9.1.1 (Código de la causa de limitación) y 9.1.2 (Causa legal/normativa de limitación) del e-EMGDE.

1.5.5.2.1.2.2. Acceso a la información afectada o regulada por normativa específica.

102. En aquellos casos en que las materias tratadas en la serie documental tengan previsto un régimen jurídico específico de acceso a la información, se debe especificar la norma reguladora, tal y como define el elemento e-EMGDE 9.1.2. (Causa legal/normativa de limitación). La tabla que se incluye a continuación recopila un conjunto de valores que se pueden utilizar como referencia, ya que, de conformidad con el segundo apartado de la Disposición adicional primera de la LTAIBG, se regirán por su normativa específica, y por dicha Ley con carácter supletorio,

aquellas materias que tengan previsto un régimen jurídico específico de acceso a la información.

Régimen	Normativa reguladora
Información ambiental	Ley 27/2006, de 18 de julio, por la que se regulan los derechos de acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente.
Información catastral	Ley del Catastro Inmobiliario (texto refundido aprobado por Real Decreto Legislativo 1/2004, de 5 de marzo).
Secreto censal	Ley Orgánica 5/1985, de 19 junio, del Régimen Electoral General.
Secreto fiscal o tributario	Ley 58/2003, de 17 de diciembre, General Tributaria.
Secreto estadístico	Ley 12/1989, de 9 de mayo, de la función estadística pública.
Secreto sanitario	Ley 14/1986, de 25 de abril, General de Sanidad. Ley 41/2002, de 14 noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
Materias clasificadas	Ley 9/1968, de 5 de abril, sobre secretos oficiales.
Datos de Carácter Personal	Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la LOPD.
Intimidad y honor	Ley Orgánica 1/1982, de 5 de mayo sobre protección civil del derecho al honor, intimidad personal y familiar y a la propia imagen.

1.5.5.2.1.2.3. Protección de datos de carácter personal.

103. Cuando un documento contenga datos de carácter personal protegidos por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (en adelante, LOPD) que no tengan la consideración de "fuentes accesibles al público" (tal y como se establece en el artículo 11), deberá tener asignado un nivel de sensibilidad de datos de carácter personal.

    Los niveles de sensibilidad en la clasificación del documento según la LOPD se recogen en la siguiente tabla:

	Datos de carácter personal	Disposición
DP1	Datos especialmente protegidos/sensibles/núcleo duro	15.1 LTABG/ LOPD
DP2	Otros datos de carácter personal susceptibles de protección	15.3 LTABG/LOPD
DP3	Otros datos de carácter personal	LOPD

Para asociar a cada documento el nivel que corresponda, se utilizará el metadato e-EMGDE 8.4 "Sensibilidad de datos de carácter personal", cuyos valores se recogen en la tabla que se muestra a continuación, en consonancia con la notación propia de la LOPD, el apéndice 12 del e-EMGDE (Clasificación de sensibilidad) y el metadato del e-EMGDE 8.6 (Nivel de confidencialidad de la información).

Nivel	**Datos de carácter personal**
Alto	Datos especialmente protegidos/sensibles/núcleo duro
Medio	Otros datos de carácter personal susceptibles de protección
Básico	Otros datos de carácter personal

104. El cumplimiento de la LOPD y el acceso a la información contenida en el Documento Electrónico son elementos independientes entre sí, por lo que, en caso de duda, se impondrá siempre el más restrictivo.

1.5.5.2.2. Mecanismos para el acceso parcial a información restringida

105. Con el fin de favorecer el acceso a la información contenida en la entidad documento de acceso restringido, en los casos en que exista la posibilidad y modalidad de disociación de datos o acceso parcial, se deben incluir aquellas medidas propuestas para favorecer el acceso a la información de acceso restringido. Como referencia, se puede utilizar la siguiente tabla:

Denominación	**Definición**
Enmascaramiento de datos	Copia del documento en la que se han ocultado los datos susceptibles de protección.
Despersonalización o anonimización	Copia del documento en la que se han ocultado los datos que identifican o permiten identificar fácilmente a las personas afectadas.
Exclusión de documentos para acceso parcial	Retirada de consulta pública de documentos concretos cuando se pueda ofrecer un acceso parcial al expediente, sin que resulte una información distorsionada o carente de sentido.
Limpieza de metadatos	Borrado o modificación de los datos de autor, localización, aplicación o sistema de origen, etc.

106. En estos casos, a la hora de la consulta, se proporcionará el documento al destinatario con carácter de copia electrónica parcial auténtica, tal y como se define en el apartado 2.3 Copiado auténtico de documentos.

1.5.5.2.3. Mecanismos para la consulta y para la puesta a disposición con fines de reutilización

107. El SGDEA facilitará la búsqueda y recuperación de la información contenida en el mismo a ciudadanos e investigadores. El SGDEA del MECD debe permitir la creación de un Interface de Usuarios Externos, para ciudadanos e investigadores, aspecto de especial relevancia en la fase de archivo intermedio e histórico. Los documentos objeto de interés por parte de los usuarios externos se estructurarán y servirán mediante la creación de Paquetes de Información de Consulta (PIC).

108. Por otra parte, con el fin de favorecer la puesta a disposición y reutilización de los documentos electrónicos generados por el MECD y sus organismos autónomos por parte de terceros, se deben implementar los metadatos pertinentes y ampliar su Aplicabilidad a la entidad Agente, para consolidar entre los organismos generadores de activos de información reutilizable la voluntad de una política de transparencia y de datos abiertos (e-EMGDE 9 - Derechos de acceso, uso y reutilización[13]).

109. Los recursos puestos a disposición de terceros por parte del MECD, con fines de reutilización, deberán aportar información sobre los propios recursos disponibles, las condiciones de su uso, avisos legales, licencias, etc. Se utilizará el metadato e-EMGDE 9.2 - Condiciones de Reutilización para aportar esta información[14].

1.5.5.3. Requisitos de seguridad en el acceso a la información contenida en el SGDE/SGDEA

110. Se aplicarán aquellos mecanismos propios de los SGDE/SGDEA para evitar el acceso no autorizado a la información, así como, todas las directrices establecidas por el Esquema Nacional de Seguridad (en adelante, ENS, regulado por el Real Decreto 3/2010) en sus artículos 16 (Autorización y control de accesos), 21 (Protección de la información almacenada y en tránsito) y 23 (Registro de actividad), que se concretan en las medidas op.acc (Control de acceso) y mp.info (Protección de la información).

111. El Acceso seguro al SGDE/SGDEA comprenderá dos operaciones sucesivas: la autenticación y la autorización.
    - La autenticación consiste en que el usuario que pretende acceder al sistema proporcione unas credenciales para que sea posible verificar su identidad. Hay dos formas principales de completar la autenticación en un SGDE/SGDEA:

[13] Una descripción detallada de este metadato se puede consultar en el anexo IV, página 160.
[14] Una descripción detallada de este metadato se puede consultar en el anexo IV, página 162.

- Proporcionando un par usuario/contraseña que habrá sido previamente registrado por el administrador del SGDE/SGDEA. Cuando se utilice esta alternativa, el SGDE/SGDEA debería implementar unas normas de seguridad básicas: almacenar las contraseñas previamente cifradas, establecer reglas de complejidad de las contraseñas y su caducidad periódica, limitar el número de intentos fallidos de entrada al sistema, registrar estos intentos y no proporcionar información detallada del motivo por el que se rechazan los mismos.
- Delegando la autenticación en el sistema operativo o red corporativa en la que está ejecutándose el SGDE/SGDEA. En este caso, el usuario se habrá autenticado previamente en dicho sistema o red, donde con su credencial se determina que tiene acceso al SGDE/SGDEA y se le franquea dicho acceso sin necesidad de volver a identificarse (mecanismos conocidos técnicamente como "*Single Sign-On*"). Éste es el medio recomendado por simplificar considerablemente la gestión de identidades en la organización.

- La autorización se aplica una vez realizada con éxito la autenticación. A partir de la identidad verificada del usuario, se comprueba a qué recursos del SGDE/SGDEA está autorizado a acceder y qué operaciones puede efectuar en cada recurso concreto. La autorización será proporcionada por el SGDE/SGDEA, e irá acompañada de un registro de todas las operaciones que modifiquen algún recurso o consulten recursos especialmente protegidos, lo que servirá como evidencia en las labores de auditoría de seguridad del SGDE/SGDEA y su contenido.

112. El SGDE/SGDEA debe proporcionar medidas técnicas para asegurar las siguientes dimensiones de la seguridad:
    - Confidencialidad: Mediante el mecanismo de autorización proporcionará acceso a cada recurso exclusivamente a las personas expresamente autorizadas (mediante su pertenencia a "listas blancas"). Además, los recursos especialmente protegidos se guardarán cifrados.
    - Integridad: La firma electrónica de documentos permite asegurar su integridad. Adicionalmente, la integridad, se puede asegurar mediante el cálculo sobre el contenido del elemento y almacenamiento de una función resumen ("*hash*").
    - Autenticidad: Se preservará la identidad de las personas u organismos que han generado el documento. Cuando hayan sido varios los actores que hayan intervenido en su generación, se guardará un registro de las partes del documento que hayan producido o modificado cada uno de ellos.

- La identidad de los actores deberá garantizarse mediante alguno de los mecanismos de identificación recogidos en el artículo 9 de la Ley 39/2015, de 1 de octubre.
    - Cuando el documento sea firmado electrónicamente con alguno de los sistemas de firma previstos en el apartado 2.1 de la Política, el hecho de la firma electrónica garantiza esta dimensión.
    - Cuando el documento no esté firmado electrónicamente, el mecanismo de trazabilidad y versionado descrito en el apartado 1.5.7.1 conjuntamente con el aseguramiento de la identidad de los actores será suficiente para garantizar esta dimensión.
- Disponibilidad: Esta dimensión suele garantizarla la infraestructura de red en la que se aloja el SGDE/SGDEA. Adicionalmente, se pueden recomendar instalaciones balanceadas o en "*cluster*" del SGDE/SGDEA que proporcionen alta disponibilidad y permitan distribuir picos de trabajo.
- Trazabilidad: De forma complementaria a la información proporcionada por los metadatos, el SGDE/SGDEA mantendrán registros de auditoría ("*logs*") de aquellas acciones de los usuarios que se consideren más relevantes para la investigación de posibles incidentes de seguridad (como se mencionó más arriba) o cuyo registro sea obligatorio en virtud de una norma.

113. Otras medidas de seguridad adicionales, como la política de copias de seguridad, estarán delegadas en las infraestructuras comunes de la organización.

114. En función de los niveles de acceso a la información contenida en cada documento, se adoptarán las medidas de protección indicadas en su correspondiente categoría, así como en las inferiores, recogidas en la tabla del Anexo VI. Estos aspectos se complementan con las directrices de la Política de Seguridad de la organización, tal y como se recoge en el Anexo VII del presente documento.

115. Además, habrá que tener en cuenta que aquellos documentos que puedan salir del ámbito de la organización y contengan datos especialmente sensibles, pueden conllevar la adopción de medidas que eviten la indexación en los buscadores de Internet. Se recomienda someter cada uno de estos documentos a un proceso de limpieza de metadatos de archivo, que aseguren el borrado de la información relacionada con el autor, la aplicación, el sistema operativo en que se ha creado, etc.

1.5.5.3.1. Acceso a los expedientes y documentos electrónicos

116. La consulta del contenido del documento se realizará una vez cotejado el permiso efectivo del usuario en relación al mismo. Se registrará, si es posible, el acceso de cada uno de los usuarios a los documentos de aquellas categorías que impliquen un acceso limitado, pero no necesariamente cada una de las operaciones de consulta que realice. Se recomienda, además, el registro de las denegaciones de lectura, de cara a permitir realizar labores de auditoría de intentos de acceso no permitidos.

117. Si es factible, esta información se registrará mediante los metadatos opcionales e-EMGDE21, registrando la acción ("Accede a", "Cambia", "Borra", etc., tal y como figuran en el apéndice 7 del e-EMGDE), la fecha, la entidad afectada, etc.

1.5.5.3.2. Establecimiento y modificación del nivel de acceso a la información

118. El nivel de acceso a la información se establece en el momento de incorporación de un documento al SGDE de la Organización.

119. Cada categoría documental ("serie documental") del Cuadro de Clasificación o Repertorio de Series Documentales de la Organización tendrá establecido un nivel de acceso mínimo (nivel "por defecto"), que se asignará automáticamente el documento en el momento de su incorporación al SGDE.

120. A aquellos documentos que, en el momento de ser incorporados, no se les pudiera asignar una categoría, se considerarán de libre acceso.

1.5.6. Calificación

1.5.6.1. Documentos esenciales

121. Se entiende por documentos esenciales aquellos que resultan indispensables y vitales para que la entidad pueda alcanzar sus objetivos, cumplir con sus obligaciones diarias de servicio y respetar la legalidad vigente y los derechos de las personas.

122. La categorización del sistema (tal y como establece el Anexo I del ENS), 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.

123. Cada organismo, centro o entidad decidirá cuáles son los documentos que cumplen estos requisitos y deben considerarse esenciales. Una vez identificados, se deberán adoptar las

medidas necesarias para asegurar especialmente su confidencialidad, integridad, disponibilidad y autenticidad.

124. A nivel orientativo o de mera recomendación, se considera que los documentos electrónicos que podrían ser calificados como esenciales son aquellos que:
    - Informan de las directrices, estrategias y planificación de la organización.
    - Recogen derechos de la organización, singularmente relativos a convenios y documentos de propiedad.
    - Recogen información sobre los edificios, instalaciones y sistemas de la organización.
    - Dejan constancia de los acuerdos y resoluciones de los órganos de gobierno de la organización, tanto colegiados como unipersonales.
    - Contienen datos necesarios para la protección de los derechos civiles, profesionales, financieros, jurídicos u otros derechos de los individuos u otras instituciones de la propia organización.
    - Contienen elementos de prueba de las actividades presentes y pasadas de la organización para cumplir las obligaciones de rendición de cuentas.[15]

125. La gestión de los documentos calificados como esenciales requerirá:
    - La obtención de una réplica según lo dispuesto en el procedimiento de copiado auténtico de documentos.
    - El tratamiento y conservación, en su caso, de original y copia, teniendo en cuenta que básicamente pueden darse tres circunstancias en relación a los soportes:
        - El documento original es electrónico.
        - El original es en soporte papel.
        - El expediente es híbrido, es decir en soporte papel y electrónico.

126. En todos los casos, se adoptarán las medidas necesarias para que exista una réplica del documento electrónico o una copia auténtica y se adopten las medidas necesarias para garantizar las condiciones de protección recogidas en el punto anterior.

[15] Como ejemplos, se pueden considerar los siguientes: documentos sobre directrices generales de política del Gobierno en materias autonómica y local, inventarios, planos y proyectos de obras mayores de edificios y locales adscritos al Ministerio, convenios suscritos por el Departamento con otras Administraciones o personas jurídicas, el Registro de Personal, auditorías, inspecciones extraordinarias, etc.

127. Cuando se trate de un documento esencial cuyo original está en soporte papel, una vez realizada la copia electrónica auténtica, el original en papel será objeto de estudio de valoración junto con su serie documental.

128. Si se trata de documento esencial que forma parte de un expediente que se conserva íntegramente en papel, se realiza una copia electrónica auténtica. El original en papel continuará conservándose en dicho formato en el expediente, mientras no haya un dictamen de la Comisión Superior Calificadora de Documentos Administrativos de sustitución de soporte para toda la serie documental.

129. Si se trata de un documento esencial que forma parte de un expediente híbrido, se realizará una copia electrónica auténtica del mismo y se adoptarán las medidas necesarias para garantizar las condiciones de protección recogidas en el punto 125.

130. La caracterización de un documento como esencial se refleja en el elemento 13.4 del e-EMGDE. En una organización, los documentos esenciales de la misma deben estar previamente identificados. En ese caso, los metadatos se asignarán en el momento de su captura o incorporación al SGDE. No obstante, este metadato se podrá incorporar en cualquier momento del proceso si la organización no contase con una identificación previa de los documentos esenciales o se produjesen cambios en la normativa que dispusieran que un documento previamente no identificado como tal pasase a convertirse en documento esencial.

1.5.6.2. Valoración

131. La valoración documental es un proceso que permite determinar los valores de los documentos producidos y/o conservados por la organización, a través del análisis contextual de los mismos, y que dará como resultado el establecimiento de plazos de conservación, transferencia y acceso de las series documentales estudiadas.

132. La Comisión Superior Calificadora de Documentos Administrativos (CSCDA), órgano consultivo superior adscrito a este Departamento ministerial, establece en el documento Criterios generales para la valoración de los documentos de la Administración General del Estado que la serie documental se constituye como la unidad de trabajo de valoración, por tanto, los plazos de transferencia, acceso y conservación o, en su caso, eliminación total o parcial se establecerán para las series documentales, no para documentos o expedientes individualmente considerados.

133. La valoración documental consiste en el estudio y análisis de las características históricas, administrativas, jurídicas, fiscales e informativas de las series documentales.

134. En la determinación del valor de los documentos de archivo con vistas a su conservación en soporte original o alternativo o a su posible eliminación se tendrán en cuenta los siguientes criterios de carácter general:
    - Criterio de procedencia: se primarán los documentos y series documentales procedentes de los órganos que ocupan una posición más elevada dentro de la jerarquía administrativa.
    - Criterio funcional: se primarán las series documentales producidas por los órganos administrativos en el ejercicio de funciones que les son propias y específicas.
    - Criterio de producción: se primarán las series documentales producidas por los órganos que realizan el seguimiento completo del procedimiento.
    - Criterio diplomático: los documentos originales, terminados y validados, son más valiosos que las copias.
    - Criterio de contenido: se primarán los documentos y series que contengan la información en forma sintética.
    - 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; así como aquellos documentos y series documentales que por su origen, periodo cronológico que abarcan o contenido se espera que sean objeto de consulta por parte de los usuarios potenciales.

135. Determinando los valores de la serie documental se fijan los criterios relativos a los tres ámbitos siguientes:
    - Los plazos de transferencia entre los distintos archivos responsables dentro del Sistema de Archivos de la AGE.
    - Los plazos de conservación o eliminación total o parcial de la serie, así como el cambio de soporte.
    - Los plazos de acceso.

136. 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. El Calendario de Conservación del Departamento se incluye en el Anexo VIII, y se modificará a medida que se vaya construyendo.

137. Las propuestas de dictamen de conservación y eliminación corresponden a la Comisión Calificadora departamental, y deben ser elevadas a la Comisión Superior Calificadora de Documentos Administrativos para su dictamen preceptivo y vinculante.

138. Según la norma ISO 23081-2:2011, los propios metadatos para la gestión de documentos deben ser objeto de valoración. La valoración determina no sólo qué metadatos deben capturarse acerca del documento, sino durante cuánto tiempo deben conservarse.

139. En lo que respecta a los metadatos, a medida que se vaya disponiendo de la información, se cumplimentarán los elementos:

- 13.1 - Valoración.
  - 13.1.1 - Valor primario.
    - 13.1.1.1 - Tipo de valor.
    - 13.1.1.2 – Plazo.
  - 13.1.2 - Valor secundario del e-EMGDE.

140. Por ejemplo, el valor primario y el plazo (valor fiscal, cuatro años) es una información que se puede proporcionar desde el momento de creación o incorporación de la entidad documento al sistema de gestión documental, pero hay otra información que no siempre es posible incorporar hasta la elaboración y aprobación de los correspondientes calendarios de conservación o, en su caso, la existencia de un dictamen por parte de la autoridad calificadora.

1.5.6.3. Dictamen

141. La Comisión Superior Calificadora de Documentos Administrativos, como autoridad calificadora, emite, en función de los plazos de conservación propuestos o resultantes del proceso de valoración documental, un dictamen favorable o desfavorable referido a la transferencia (apartado 1.5.8), conservación (apartado 1.5.7), eliminación (apartado 1.5.9) o acceso (apartado 1.5.5) de las series documentales que queda recogido en el Calendario de Conservación de documentos de la entidad.

142. Estudiados los valores de cada serie documental, siguiendo los criterios utilizados en la fase de valoración, se pueden establecer las propuestas de dictamen siguientes:

- Conservación total.

- Eliminación parcial, cuando se conservan parcialmente los expedientes o una muestra de los mismos de acuerdo con diferentes métodos de muestreo.
- Eliminación total, en el caso de series documentales sin valor secundario, por ejemplo histórico, y cuya información está recogida en otras series documentales o no es necesaria su conservación.

143. Se entiende por muestreo la técnica de selección, según criterios sistemáticos (numéricos, alfabéticos, topográficos) o cualitativos, de una cierta proporción de documentos en representación de un conjunto, utilizando como métodos:

Ejemplar o testigo	Se selecciona un expediente dentro de una serie documental para ilustrar la práctica administrativa del momento.
Cualitativo o selectivo	Método subjetivo que se basa en 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) de expedientes, dependiendo de la organización de la serie documental.
Aleatorio	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.

144. Una vez aprobada la propuesta de dictamen elevada por parte de la Comisión Calificadora departamental por la Comisión Superior Calificadora de Documentos Administrativos, se incluirá su contenido en los metadatos siguientes:
    - 13.2 – Dictamen.
        - 13.2.1 - Tipo de dictamen.
        - 13.2.2 - Acción dictaminada
        - 13.2.3 - Plazo de ejecución de la acción dictaminada del e-EMGDE, una vez aprobada la propuesta de dictamen.

1.5.7. Conservación

145. La conservación de los documentos y expedientes electrónicos atenderá a los plazos legales y en su caso a los establecidos en el dictamen de la autoridad calificadora y a lo dispuesto en la estrategia de conservación implantada por este Departamento ministerial.

146. Atendiendo a lo dispuesto en el ENS, y proporcionalmente a los riesgos a los que estén expuestos los documentos, el MECD contará con un plan de continuidad para preservar los documentos y expedientes electrónicos conservados, así como sus metadatos asociados, que incluirá lo previsto en el Anexo II del ENS sobre 'Copias de seguridad (*backup*) [mp.info.9]' ; junto con las medidas de protección de la información [mp.info], de protección de los soportes

de información [mp.si] del citado Anexo II, y, en cualquier caso, las medidas de protección de datos de carácter personal según lo dispuesto en la LOPD y su normativa de desarrollo.

147. Para prevenir riesgos de pérdida física de los documentos o de su valor probatorio, el Departamento y cada organismo, centro o entidad debe definir un Plan de Preservación de los Documentos Electrónicos de la organización que incorporará un análisis y gestión de riesgos en el ámbito de la gestión documental. Este Plan de Preservación detallará los aspectos siguientes:
    - Los actores implicados en el proceso de conservación del documento electrónico.
    - Los elementos a proteger (activos), detallando sus características, las interdependencias entre ellos y las medidas de protección ya adoptadas o disponibles.
    - El análisis e identificación de riesgos sobre los activos, mediante la elaboración de un Informe o Tabla de Evaluación de Riesgos que incluya los riesgos identificados, y por cada uno de ellos sus consecuencias e impacto, su escala de gravedad y de probabilidad o frecuencia y el tratamiento de los mismos.
    - Las medidas de prevención que se adopten para cada tipo o grupo de riesgos.

148. Este Plan de Preservación garantizará la accesibilidad, autenticidad, disponibilidad, integridad, trazabilidad, inteligibilidad y legibilidad de los documentos electrónicos a lo largo de su ciclo de vida, frente a los siguientes grupos de riesgos:
    - Los derivados de la continua evolución de la tecnología y la consiguiente obsolescencia de la misma.
    - 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.
    - Los que proceden de una posible descontextualización de los documentos electrónicos.
    - Los que forman parte del ámbito de la seguridad de las TIC y que pueden suponer una alteración intencionada de los documentos electrónicos o su misma desaparición (accesos no permitidos, ataques, robo de soportes, etc.).
    - Los 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.

149. La ley 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 autoridad calificadora 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. El proceso de eliminación debe seguir la metodología descrita en el apartado 1.5.9 de este documento.

150. El SGDE/SGDEA 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.

1.5.7.1. Trazabilidad de los documentos electrónicos

151. El SGDE utilizado en la organización deberá asegurar la trazabilidad de las acciones que se realicen sobre los documentos almacenados en el sistema. Como mínimo, los eventos que se registrarán sobre cada documento almacenado en el SGDE serán los siguientes:
    - La creación del documento.
    - La modificación y versionado del documento (creando nuevas versiones).
    - El borrado físico del documento.
    - La transferencia del documento a otro SGDE o SGDEA con cambio de custodia.
    - El acceso al contenido del documento, cuando dicho documento tenga un nivel de control de acceso a la información con una categoría de seguridad con el nivel de confidencialidad más alto.

152. En el caso de los expedientes electrónicos, los eventos que se registrarán en el SGDE son:
    - La creación del expediente electrónico y su índice.
    - La incorporación de nuevos elementos (documentos u otros expedientes) al expediente y modificación del índice electrónico.
    - La retirada de elementos (documentos u otros expedientes) del expediente y la consiguiente modificación de su índice electrónico.
    - El cierre del expediente y del índice electrónico, sin posibilidad de agregar o eliminar más elementos.
    - La transferencia del expediente a otro SGDE o SGDEA con cambio de custodia.
    - La eliminación física del expediente.

153. En un entorno multientidad, tal y como se propone en esta Política, se establecerán las adecuadas relaciones con las entidades Actividad, Regulación, Documento y Agente pertinentes. En este sentido, se contemplarán diferentes aspectos relativos a la trazabilidad, tales como:

- Indicador de tipo de acción (e-EMGDE21.1 – Acción): debe establecerse una relación con la entidad Actividad[16].
- Razón por la que se lleva a cabo la acción asociada (e-EMGDE21.2 – Motivo reglado): debe establecerse una relación con la entidad Regulación.
- Identificación del usuario que ha realizado la Acción (e-EMGDE21.3 – Usuario de la acción): debe establecerse una relación con la entidad Agente.
- Explicación de la Acción (e-EMGDE21.4 – Descripción): debe cumplimentarse en todas las entidades.
- Información que registra la autoría y la fecha de los posibles cambios que han sufrido los metadatos de una entidad, una vez realizada la acción (e-EMGDE21.5 – Modificación de los metadatos): debe cumplimentarse en todas las entidades.
- Información que registra el elemento de metadato que ha sido modificado sobre una determinada entidad y su valor anterior (e-EMGDE21.4 – Historia del cambio): debe cumplimentarse en la entidad Relación.

154. Al completarse cada uno de los eventos anteriores, el SGDE generará los metadatos que se indican más abajo, en el punto 157, como necesarios para una "óptima gestión documental", con el formato especificado en el e-EMGDE, y los registrará como metadatos asociados al propio documento, o al índice electrónico asociado al expediente. Estos metadatos podrán custodiarse en un repositorio diferente al del SGDE, manteniendo en todo momento su relación con el documento o expediente electrónico al que se refieren.

155. En el caso de las series documentales incluidas en los procesos archivísticos de transferencia, los metadatos obligatorios se acompañarán de los metadatos complementarios necesarios e imprescindibles para una correcta gestión documental, que se desglosan en el Anexo IV, del perfil de metadatos institucional, y que se refieren también en el apartado 1.5.8 Transferencia.

156. Cuando se complete la eliminación física de un documento/expediente, deberá mantenerse una referencia al mismo en el SGDE o en otro repositorio externo a la que estén asociados todos los eventos registrados durante la vida útil del documento. Esta referencia se mantendrá de manera permanente en la entidad Documento, categoría Serie, pudiéndose eliminar en la categoría Expediente/Documento en los plazos marcados por la resolución pertinente de la

[16] Para su cumplimentación véase el Apéndice 7 (Esquema de nombres de relaciones de acciones de gestión de documentos – extensible) del e-EGMDE.

Comisión Calificadora Departamental y la Comisión Superior Calificadora de Documentos Administrativos.

157. Los metadatos para la información de auditoría que se registrarán de estos eventos son los siguientes:

Metadato	**Elemento e-EMGDE**	**Contenido**	**Obligatorios/ Necesarios**
Acción	e-EMGDE21.1	Tipo de actuación realizada sobre el documento	Sí
Fecha de la acción	e-EMGDE21.1.1	Fecha y hora en que se produce la actuación	Sí
Entidad de la acción	e-EMGDE21.1.2	Elemento del documento (parte del documento, metadato…) al que se limite la actuación. Cuando no se informe este metadato, se entiende que la actuación afecta al documento completo.	Sí
Motivo Reglado	e-EMGDE21.2	Razón o disposición legal/reglamentaria o procedimiento por el que se lleva a cabo la actuación	Sí
Usuario de la acción	e-EMGDE21.3	Identidad del usuario que realiza la actuación, utilizando cualquier atributo que lo identifique de forma inequívoca (nombre de red, IP, DNI…)	Sí
Modificación de los metadatos	e-EMGDE21.5	Información que registra la autoría y la fecha de los posibles cambios	Sí
Historia del cambio	e-EMGDE21.6	Información que registra el elemento de metadato que ha sido modificado	Sí
Nombre del elemento	e-EMGDE21.6.1	Nombre de elemento o sub-elemento de metadato cuyo valor ha sido modificado	Sí
Valor anterior	e-EMGDE21.6.2	Contenido anterior de un elemento o sub-elemento de metadato que ha sido modificado.	Sí

158. En el caso del SGDEA, se registrarán los eventos de:

- Incorporación de un nuevo documento/expediente/serie por cambio de custodia desde el SGDE.
- Eliminación física de un documento/expediente/serie, con obligatoriedad en este caso de informar el metadato “Motivo reglado”.
- Consulta de un documento con el nivel más alto de confidencialidad, siempre que no hubiera expirado esa condición.

- Así como cualquier otra acción recogida en el Apéndice 7 (Esquema de nombres de relaciones de acciones de gestión de documentos – extensible) del e-EMGDE que permita una gestión óptima de los documentos.

1.5.8. Transferencia

159. La transferencia[17] es el "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". Tiene como objetivo facilitar el paso de los documentos a través de las distintas fases de archivo del sistema, de manera que puedan recibir el tratamiento adecuado en cada momento de su ciclo de vida.

160. En este sentido, se contemplan dos escenarios posibles:
    - Transferencia de custodia con cambio de repositorio.
    - Traspaso de responsabilidad de la custodia y gestión sin cambio en el repositorio.

161. De toda transferencia deberá quedar constancia de los movimientos efectuados, preferiblemente mediante metadatos de trazabilidad.

162. De conformidad con lo previsto en el apartado V.6. de la NTI de Expediente Electrónico y en el apartado VII.5. de la NTI de Documento Electrónico, en caso de intercambio de expedientes electrónicos entre Administraciones Públicas que suponga una transferencia de custodia o traspaso de la responsabilidad de la gestión de expedientes y documentos que deban conservarse permanentemente, el órgano o entidad remitente será la responsable de verificar la autenticidad e integridad del expediente en el momento de dicho intercambio, mediante la firma electrónica de los índices de los expedientes y de los documentos electrónicos.

    Por otra parte, la NTI de Política de Gestión de Documentos Electrónicos en el apartado VI relativo a Procesos de Gestión de Documentos electrónicos, en su punto 8 establece que "la transferencia de documentos incluirá las consideraciones para la transferencia entre repositorios, así como las responsabilidades en cuanto a su custodia".

163. Asimismo, cuando la transmisión se realice mediante soportes físicos, deberán tenerse presentes en el proceso de transferencia las medidas de 'Protección de los soportes de información [mp.si]' previstas en el ENS (en particular las referidas a su transporte y a los

[17] http://www.mecd.gob.es/cultura-mecd/areas-cultura/archivos/mc/dta/diccionario.html

mecanismos que relacionados con la integridad y la trazabilidad) y en el resto de la normativa que pueda ser de aplicación.

164. Para la creación de un archivo electrónico único de la AGE, según lo dispuesto en la Ley 39/2015 Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la Política del MECD atenderá a lo establecido en su Exposición de Motivos V, que recoge literalmente: *"la creación de este archivo electrónico único resultará compatible con los diversos sistemas y redes de archivos en los términos previstos en la legislación vigente, y respetará el reparto de responsabilidades sobre la custodia o traspaso correspondiente. Asimismo, el archivo electrónico único resultará compatible con la continuidad del AHN, de acuerdo con la LPHE y su normativa de desarrollo".* Por lo tanto, será de aplicación la LPHE y el Real Decreto 1708/2011, que regula el Sistema de Archivos de la AGE.

    Según lo dispuesto en el art. 20 del citado Real Decreto, deberá transferirse la responsabilidad de la custodia y gestión de los documentos y expedientes electrónicos desde los diferentes archivos centrales de los departamentos ministeriales y de sus organismos autónomos al archivo intermedio (Archivo General de la Administración) y posteriormente al archivo histórico (Archivo Histórico Nacional) de la AGE para su adecuada conservación y tratamiento archivístico, así como para facilitar su consulta por parte de los ciudadanos y de la investigación histórica.

165. A tal efecto, se arbitrarán las soluciones técnicas adecuadas y se proporcionarán los permisos de acceso y gestión necesarios a los responsables del Archivo General de la Administración y, en su caso, del Archivo Histórico Nacional, como archivos intermedio e histórico del Sistema de Archivos de la AGE, con el fin de que se garantice para generaciones futuras la contextualización y conservación de los documentos electrónicos y sus metadatos asociado.

166. La transferencia entre repositorios debe estar definida y controlada por reglas en el SGDE y en el SGDEA, a partir de lo dispuesto en los calendarios de conservación. Además, debe disponerse de mecanismos de bloqueo para aquellos expedientes o documentos que deban exceptuarse de la aplicación de las reglas generales por algún motivo, por ejemplo, porque forman parte de un recurso abierto.

167. Los metadatos del documento electrónico deben ser transferidos asociados al documento para permitir su identificación, su autenticidad y los procedimientos de conservación.

168. El proceso de transferencia de agrupaciones documentales establecido en la Política se realizará mediante la creación de los Paquetes de Información de Transferencia (en adelante PIT) contemplados en la norma UNE-ISO 14721:2015 vigente, como estructura de datos que contiene toda la información necesaria para llevar a cabo la transferencia entre el agente remitente y el agente receptor según el ciclo de vida de los documentos del Sistema de Archivos de la AGE.

1.5.8.1 *Planificación de la Transferencia*

169. El proceso de transferencia deberá articularse coordinadamente entre la unidad remitente y el agente receptor, mediante:

- Identificación de Responsables. El proceso de transferencia requerirá la identificación de un responsable por parte de la unidad remitente y receptora debidamente autorizados para ello.
- Contacto fluido entre las partes. El flujo de trabajo se desarrollará en coordinación y con el conocimiento de la unidad receptora, con la que existirá el debido contacto desde la unidad remitente para su correcta planificación.
- Determinación de Calendarios. La transferencia de las diferentes agrupaciones documentales se ajustará a los plazos establecidos en los calendarios de conservación y/o transferencia aprobados en las diferentes Administraciones públicas.
- Acuerdo de envío.

1.5.8.2. *Preparación y revisión previa del contenido de los PITs*

170. La generación correcta de los PITs será responsabilidad del agente remitente, para ello:

- Se verificará que los formatos de los documentos y expedientes electrónicos que integrarán el PIT son los contemplados en la NTI de Catálogo de Estándares.
- Los documentos y expedientes electrónicos a transferir no estarán cifrados o protegidos por contraseña u otros medios que impidan acceder a su contenido sin poseer una clave o el *token* para el descifrado.
- El remitente asegurará que todos los elementos a integrar en el PIT estén libres de "*malware*" (virus, documentos que contienen *scripts* o macros dañinos, etc.).
- Se verificará la correcta inclusión de los elementos de autenticación de los documentos y expedientes electrónicos que conformarán los PIT (firmas electrónicas, sellos de tiempo, códigos seguros de verificación, índice electrónico, etc.).

- Se comprobará que los documentos y expedientes electrónicos que compondrán el PIT no han sufrido accesos no deseados o modificaciones no permitidas (trazabilidad y verificación de la integridad).
- Se verificará que todos los documentos y expedientes electrónicos que conformarán el PIT incorporan los metadatos mínimos obligatorios establecidos en el ENI.
- Además, se incluirán los metadatos complementarios necesarios relativos a los diferentes procesos de gestión documental y se revisarán y actualizarán los metadatos relativos a condiciones de acceso y de utilización. De acuerdo con la legislación vigente en materia de acceso, general y sectorial, las condiciones que rigen el acceso pueden cambiar según el ciclo de vida de los documentos y las distintas fases de archivo (oficina, central, intermedio e histórico).
- Se incluirá la información pertinente sobre el contexto de producción de los documentos y expedientes electrónicos que integrarán los PIT.

171. Para las transferencias de paquetes de información realizadas con la finalidad de su conservación a medio y largo plazo, los documentos que integran los PIT se deberán adecuar a formatos longevos recogidos en la NTI de Catálogo de Estándares, incluyendo aquellas migraciones o cambios de formato que sean pertinentes.

172. Se verificará que la autenticación de los mismos se realizará mediante la incorporación de mecanismos de firma que puedan ser verificados a largo plazo y se podrán incluir indicaciones sobre procedimientos de conservación en relación al deterioro de los soportes y la obsolescencia tecnológica.

1.5.8.3 Encapsulado del PIT

173. Una vez preparadas y revisadas las agrupaciones documentales objeto de transferencia, se encapsularán en el PIT.

174. La estructura del PIT se adecuará a los estándares, normas internacionales y paneuropeas y buenas prácticas en materia archivística que cumplan las condiciones de interoperabilidad técnica establecidas en el ENI.

175. Cualquier PIT deberá a su vez responder a unos criterios de calidad:

- El formato de un PIT debe ser lo más simple posible.
- El formato de un PIT debe permitir una gestión eficiente del proceso de transferencia.

- Cuando las agrupaciones documentales objeto de transferencia sean excesivamente voluminosas, éstas pueden ser fraccionadas en varios PITs.
- La estructura del PIT debe ser extensible y poder integrar nuevos metadatos o formatos de datos.
- El PIT contará con los metadatos obligatorios de: identificador del PIT; tipo de paquete de información de OAIS; el identificador de la organización y de la unidad responsable del envío; identificador de la persona de contacto responsable del proceso de transferencia; sello de tiempo del PIT.
- El PIT debe incorporar un mapa que describa la estructura jerárquica de los objetos digitales que integran el paquete de información.

1.5.8.4 Protocolo para la aceptación de la custodia

176. El agente remitente de un PIT conservará una copia del mismo hasta que la transferencia haya sido aceptada por el archivo de destino y se obtenga el documento correspondiente de aceptación.

177. El archivo de destino comprobará la correcta remisión del paquete de información transferida.

178. En caso de detectarse errores en las acciones de preparación y revisión previa del contenido del PIT y de elaboración del paquete de información contempladas en los epígrafes 1.5.8.2 y 1.5.8.3, el archivo de destino podrá rechazar la custodia del mismo y elaborar una relación de los errores identificados.

179. El PIT será aceptado para su custodia una vez subsanados los mismos.

180. La aceptación de la custodia quedará validada mediante un documento de aceptación que deberá elaborarse en el propio sistema de gestión de manera automatizada y se podrá incorporar también como información relativa al propio PIT.

181. Este protocolo será aplicable en cada uno de los cambios de responsabilidad de la gestión y la custodia de los PITs, o de parte de los mismos, a lo largo de todo el ciclo de vida de los documentos y expedientes que lo integran.

1.5.8.5 Documentación del evento de transferencia

182. Los metadatos de transferencia contemplados en el e-EMGDE serán de obligada inclusión en todos los eventos/procesos de transferencia.

183. Los cambios de responsabilidad de la custodia y la gestión que se realicen entre repositorios o en el seno de un mismo repositorio o sistema de gestión a lo largo del tiempo, se documentarán mediante la inclusión de los metadatos de transferencia.

184. Los metadatos de transferencia se incorporarán a los documentos electrónicos y expedientes electrónicos que integran el PIT y también a los propios paquetes de información de transferencia.

185. En el caso de la transferencia física, deberá quedar constancia de la remisión de los expedientes y documentos por parte del órgano o aplicación emisora de los mismos y de su recepción en el archivo de destino.

186. El SGDEA deberá poder realizar informes sobre los expedientes ingresados en el archivo receptor por series documentales, con mención del órgano remitente, la identificación de los expedientes, sus fechas extremas y la fecha de ingreso en el archivo. Con los informes elaborados podrá generarse un Registro General de entrada de fondos, como instrumento de control del archivo.

187. En el caso de que se remita al archivo documentación en soporte papel como parte de expedientes híbridos, deberá ir acompañada de la oportuna Relación de entrega, que quedará consignada en el Registro General de entrada de documentos del archivo receptor, tras el cotejo de dicha documentación. La vinculación en los expedientes híbridos entre los documentos en soporte papel y electrónicos no se debe perder.

188. A continuación se incluye un listado de los metadatos complementarios mínimos necesarios para la transferencia de documentos y expedientes electrónicos, que serán incorporados en el SGDE/SGDEA en la entidad Documento en los hitos de los procesos en los que se produce transferencia física o transferencia de la responsabilidad de la custodia y gestión, es decir, en las transferencias de los Archivos de Oficina a los Archivos Centrales del Departamento, de los archivos centrales al archivo intermedio (Archivo General de la Administración) y del archivo intermedio al archivo histórico (Archivo Histórico Nacional):

- e-EMGDE 4.2 - Fecha fin
- e-EMGDE 8 – Seguridad
  - e-EMGDE 8.4 - Sensibilidad datos de carácter personal
  - e-EMGDE 8.6 - Nivel de confidencialidad de la información
- e-EMGDE 9 - Derechos de acceso, uso y reutilización
  - e-EMGDE 9.1 – Tipo de acceso

        - e-EMGDE 9.1.1 – Código causa limitación
        - e-EMGDE 9.1.2 – Causa legal/normativa de limitación
    - e-EMGDE 9.2 – Condiciones de reutilización
- e-EMGDE 13 – Calificación
    - e-EMGDE 13.1 – Valoración
        - e-EMGDE 13.1.1 – Valor primario
            a. e-EMGDE 13.1.1.1 – Tipo de valor
            b. e-EMGDE 13.1.1.2 – Plazo
        - e-EMGDE 13.1.2 – Valor secundario
    - e-EMGDE 13.2 – Dictamen
        - e-EMGDE 13.2.1 - Tipo de dictamen
        - e-EMGDE 13.2.2 - Acción dictaminada
        - e-EMGDE 13.2.3 – Plazo de ejecución de la acción dictaminada
    - e-EMGDE 13.3 –Transferencia
        - e-EMGDE 13.3.1 – Fase de archivo
        - e-EMGDE 13.3.2 – Plazo de transferencia
    - e-EMGDE 13.4 – Documento esencial
- e-EMGDE21 – TRAZABILIDAD
    - e-EMGDE21.1 - ACCIÓN
        - e-EMGDE21.1.1 –FECHA DE LA ACCIÓN
        - e-EMGDE21.1.2 - ENTIDAD DE LA ACCIÓN
- e-EMGDE21.2 – MOTIVO REGLADO
- e-EMGDE21.3 – USUARIO DE LA ACCIÓN
- e-EMGDE21.5 – MODIFICACIÓN DE LOS METADATOS
- e-EMGDE21.6 – HISTORIA DEL CAMBIO
    - e-EMGDE21.6.1 – NOMBRE DEL ELEMENTO
    - e-EMGDE21.6.2 – VALOR ANTERIOR
- e-EMGDE26. IDENTIFICADOR DEL DOCUMENTO ORIGEN

189. Los metadatos relativos al acceso a los documentos que se han señalado en el punto 1.5.4 tienen especial relevancia en los procesos de transferencia. Recordemos que la Comisión Superior Calificadora de Documentos Administrativos tiene competencia para determinar en sus dictámenes los plazos de acceso según la legislación vigente.

190. Además de los metadatos obligatorios y necesarios para los documentos y los expedientes electrónicos que conforman los PITs, se considera necesario incluir los metadatos pertinentes para los propios paquetes de información. Todo ello, de conformidad con lo establecido en la UNE-ISO 14721:2005 y su familia de normas, así como en consonancia con lo determinado en otros estándares, normas y buenas prácticas de ámbito internacional y paneuropeo en materia archivística.

1.5.9. Destrucción o eliminación

191. Los escenarios en los que se podrá realizar la destrucción física de la información almacenada en documentos/expedientes electrónicos son los siguientes:
    - Destrucción de información como última fase de un procedimiento reglado de eliminación y destrucción, realizado con las formalidades del Real Decreto 1164/2002, 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. Este hecho figurará en los dictámenes correspondientes a la serie documental.
    - Cambio de soporte o formato como consecuencia de obsolescencia del formato anterior o fin de la vida útil del soporte previo. En este caso, se realizará la destrucción o borrado de la información en el soporte o formato inicial.
    - Transferencia con cambio de custodia a otro organismo o archivo. En el caso de que la transferencia suponga una duplicación de los documentos que son objeto de la misma, el órgano remitente, una vez obtenida la conformidad del nuevo responsable de la custodia, deberá proceder al borrado de sus propios ejemplares.

192. En los dos últimos escenarios, y siempre que se realicen copias auténticas de los documentos electrónicos con/sin cambio de formato con las exigencias del ENI, el marco normativo de aplicación será dicho Real Decreto y las Normas Técnicas de Interoperabilidad que lo desarrollan.

1.5.9.1. Pasos previos a la destrucción de la información

193. La eliminación de documentos requerirá el dictamen preceptivo de la Comisión Superior Calificadora de Documentos Administrativos (CSCDA).

194. 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 del Ministerio de Educación, Cultura y Deporte, y se atendrán al procedimiento establecido en el Real Decreto 1164/2002.

195. A instancias de lo dictaminado por la Comisión Superior Calificadora de Documentos Administrativos, se iniciará el proceso de eliminación, respetando el procedimiento dictado por el artículo 7 del Real Decreto 1164/2002, para lo cual se generará el expediente de eliminación que comprende, según el artículo 8 del mismo, los siguientes documentos:
    - Iniciativa para poner en marcha el procedimiento.
    - Informe del órgano proponente.
    - Memoria de la documentación.
    - Acuerdo de iniciación de la Comisión Calificadora Departamental de Documentos Administrativos.
    - Informe preceptivo de la Comisión Superior Calificadora de Documentos Administrativos.
    - Resolución.
    - Notificaciones, en su caso.
    - Publicaciones de la Resolución.
    - Recursos, si se han interpuesto.
    - Resoluciones de los recursos presentados.
    - Acta de eliminación.

196. El acta de eliminación de la documentación se remitirá a la Secretaría Permanente de la CSCDA y en ella se recogerá el número de dictamen; la fecha de publicación en el Boletín Oficial del Estado de la Resolución por la que se autoriza la eliminación de documentos, sin que hubiese constancia de interposición de recurso alguno contra la decisión adoptada y cumplidos los plazos obligados de conservación; lugar, fecha y hora en que se ha producido la eliminación; procedimiento utilizado; la firma del empleado público fedatario y el listado del personal que ha intervenido en la eliminación.

197. No se podrá eliminar ningún documento o expediente electrónico en los casos excepcionales establecidos por el Real Decreto 1164/2002:
    - Si está calificado como de “valor histórico”, “valor artístico”, “carácter relevante” o “investigación”.
    - Si no ha transcurrido el plazo establecido para su conservación, durante el cual pueda subsistir su valor probatorio de derechos y obligaciones de personas físicas o jurídicas.

- Si no existe dictamen previo de la autoridad calificadora competente, tal y como se ha descrito en el apartado “Borrado del Documento Electrónico”.

198. En los expedientes y documentos afectados por estos procedimientos se incluirán los siguientes metadatos:
    - e-EMGDE21 – Trazabilidad.
        - e-EMGDE 21.1 - Acción: “Destruye” o “Elimina”
            - e-EMGDE 21.1.1 - Fecha de la acción.
            - e-EMGDE 21.1.2 - Entidad de la acción.
        - e-EMGDE 21.2 - Motivo reglado.
        - e-EMGDE 21.3 - Usuario de la acción.

1.5.9.2. Aspectos técnicos relacionados con la destrucción de la información

199. De lo expuesto hasta ahora se deduce la necesidad de incluir en la Política un procedimiento de borrado seguro de los documentos electrónicos, en el que se distingan dos posibles acciones:
    - La eliminación de los ficheros que contiene los datos del soporte en que se almacenan, liberando así el espacio que ocupaban para su reutilización, pero de forma que se impida la reconstrucción posterior de la información eliminada. A esta acción la llamaremos "borrado seguro". Esta tarea se ejecutará en los siguientes casos:
        - Por aprobación de la eliminación del documento o expediente que lo contiene.
        - Por cambio de formato en el documento.
        - Por transferencia entre sistemas de gestión documental.
    - La destrucción física del soporte, que impida la recuperación futura del contenido del mismo y su reutilización. A esta acción la llamaremos "destrucción segura". Esta situación se produce cuando se sustituye el soporte de almacenamiento, por obsolescencia o migración, y no sea posible completar el borrado seguro de la información contenida en el mismo. También se produce en el caso de soportes que no admiten la reutilización del espacio borrado (como los discos ópticos).

200. Considerando la metodología habitual de trabajo en la Administración, los procedimientos de borrado o destrucción deben incluir:
    - Los dispositivos de almacenamiento local: disco duro del puesto de usuario, dispositivos móviles, dispositivos removibles como discos duros externos, memorias USB, tarjetas de memoria, etc.

- Los soportes de almacenamiento en red: accesibles mediante protocolos para compartir ficheros (CIFS o NFS), redes SAN, almacenamiento en la nube, etc.

201. De acuerdo con la clasificación establecida por el CCN (Guía CCN-STIC 404[18]), distinguiremos los niveles siguientes de borrado /destrucción de la información:
    - Nivel 0: Borrado usando comandos/utilidades estándar del sistema operativo. Estas técnicas generalmente marcan el espacio ocupado por los archivos a borrar como disponible, pero no eliminan realmente el contenido almacenado. Por este motivo, no impide la recuperación posterior de la información borrada ni proporciona ninguna garantía frente a la revelación no autorizada de la información.
    - Nivel 1 (*'clearing'*): Borrado usando mecanismos de sobre-escritura del espacio ocupado por los archivos a borrar. La recuperación de la información borrada sólo puede realizarse usando técnicas avanzadas.
    - Nivel 2 (*'sanitizing'*): Borrado seguro. Impide la recuperación de la información borrada incluso utilizando mecanismos avanzados. Algunas de las técnicas que se pueden utilizar para realizar este borrado son: la desmagnetización del soporte; el borrado seguro mediante 'firmware' incorporado al soporte físico; la sobre-escritura de la información con protocolos que hagan imposible su reconstrucción (generalmente mediante una serie consecutiva de sobre-escrituras); o el cifrado de la información con criptografía fuerte y ofuscación de la clave de cifrado empleada.
    - Nivel 3: Destrucción física del soporte (destrucción segura): Se realiza por procesos industriales como: triturado, incineración, pulverización, fusión de los materiales de que constan los soportes,…

202. En todo caso, se respetarán las previsiones del ENS, en especial para la medida mp.si.5 (Borrado y destrucción).

1.5.9.3. Recomendaciones para la elección del nivel destrucción de la información

203. A fin de determinar el nivel de borrado más adecuado para un caso específico, hemos de tener en cuenta los siguientes parámetros:
    - El nivel de confidencialidad de la información que va a destruirse. Dicho nivel será el más elevado de entre los dos siguientes:
        - La categoría del sistema de información según lo establecido en el Anexo I del ENS.

[18] Documento de acceso restringido.

- El nivel de seguridad de la información según el Reglamento de desarrollo de la LOPD.

- El proceso de borrado va a ser gestionado y realizado por la propia organización (internamente), o por el contrario va a ser realizado por una empresa externa en el marco de un contrato de prestación de servicios. En este ámbito, se deben tener en cuenta dos casos concretos:
  - Tendrá la consideración de gestión externa cualquier procedimiento de borrado que se realice en el contexto de servicios en nube cuya infraestructura no sea de gestión privada de la organización.
  - En el caso de la cesión a terceros de la destrucción física de los dispositivos, se recomienda realizar previamente un borrado de nivel 2 sobre su contenido.
- El hecho de si se va a reutilizar o no el soporte de información tras el borrado de la misma.

204. De acuerdo con estos parámetros, el nivel mínimo de borrado que se recomienda realizar es el que expresa la tabla del Anexo IX.

205. Se recomienda, siempre que sea posible, optar por técnicas de borrado que puedan ser realizadas dentro de la propia organización (tales como: el borrado por *firmware*, la sobre-escritura, el cifrado seguro….). De esta manera, se impedirá la entrega de soportes de información a agentes externos, con el consiguiente peligro de ruptura en la cadena de custodia.

206. En caso de realizar la destrucción a través de la contratación de servicios externos, a la empresa se le debe exigir un certificado de destrucción de los documentos donde conste que la información ya no existe, y dónde, cuándo y cómo ha sido destruida. Resulta imprescindible dejar constancia de las actividades realizadas, y sirve para la auditoría y evaluación del cumplimiento de los requisitos acordados. Asimismo, se exigirá que un empleado público fedatario de este departamento ministerial presencie la destrucción de los documentos y compruebe las condiciones en que se realiza y los resultados, para firmar la correspondiente Acta de eliminación.

1.6. Asignación de metadatos

207. Se asignarán a los documentos y expedientes electrónicos los metadatos mínimos obligatorios ENI y, en su caso, los obligatorios para la transferencia, además de los opcionales si se considera oportuno, de conformidad con el perfil de aplicación de metadatos de la organización, tal como se describe en el apartado 1.5.4.2.

208. Se garantizarán la disponibilidad e integridad de los metadatos de los documentos y expedientes electrónicos, manteniendo de manera permanente las relaciones entre cada documento o expediente y sus metadatos.

1.6.1. Consideraciones sobre los metadatos mínimos obligatorios

209. Según lo indicado en el punto 1.5.1, la información necesaria para completar los metadatos mínimos obligatorios de un documento/expediente electrónico deberá generarse durante su captura, es decir, en el momento de su incorporación al SGDE de la organización. No será obligatorio en ese momento que los metadatos sigan la codificación y formato previsto en las correspondientes Normas Técnicas de Interoperabilidad, siempre y cuando puedan transformarse a dicho formato en un momento posterior.

210. En la medida de lo posible, el SGDE generará y completará de forma automática la información precisa para la generación de los metadatos mínimos obligatorios.

211. Los metadatos mínimos asociados a un documento o expediente electrónico deberán custodiarse en el repositorio físico utilizado por el SGDE.

212. Las diferentes técnicas de almacenamiento de los metadatos contemplan desde el encapsulado, donde el documento se convierte en una entidad que incorpora documento y metadatos, hasta la incrustación de los metadatos como cabecera del documento.

213. Asimismo pueden custodiarse en el repositorio físico utilizado por el SGDE de forma separada siempre y cuando se garantice el mantenimiento de una referencia unívoca entre los documentos y expedientes electrónicos y sus metadatos correspondientes.

214. Una vez realizada la captura, los metadatos mínimos no podrán ser modificados en ninguna fase posterior, excepto cuando sea necesaria la corrección de errores u omisiones en los valores inicialmente asignados. Por este motivo, el SGDE mantendrá una auditoría de las modificaciones realizadas en los metadatos mínimos de un documento/expediente con posterioridad a su captura, dejando constancia del valor anterior, la fecha y hora de modificación, el motivo justificado y el usuario que la realizó.

215. El SGDE deberá generar los metadatos mínimos obligatorios con el formato y conforme a la estructura (esquema XSD) establecida en las NTI de Expediente Electrónico y Documento Electrónico, en los casos siguientes:

- Cuando se produzca el intercambio del documento/expediente con otra Administración pública.
- Cuando el documento/expediente sea puesto a disposición de los ciudadanos por medio de la Sede Electrónica corporativa o de otro canal de comunicación que se establezca.

1.6.2. Consideraciones sobre los metadatos complementarios

216. Los metadatos complementarios de documentos y expedientes electrónicos deberán respetar el formato y la nomenclatura indicados en el esquema institucional de metadatos de la organización.

217. Estos metadatos podrán generarse en el momento de la captura del documento/expediente electrónico o en una fase posterior, y podrán modificarse durante la vida administrativa del documento/expediente.

218. Algunos metadatos complementarios deben ser generados obligatoriamente en el momento de su captura en el SGDE, por ejemplo para documentos esenciales de la organización o en relación a documentos y expedientes reservados o con restricciones de acceso, etc.

219. Cuando se produzca la transferencia del documento/expediente con cambio de custodia al archivo central, intermedio e histórico con arreglo a los calendarios de conservación ciertos metadatos complementarios se convierten también en necesarios en el contexto de una correcta política de gestión de documentos y expedientes electrónicos con el fin de garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad.

220. En aquellos casos en que se han realizado procesos de valoración, dictamen y análisis de acceso, los metadatos relativos a estos procesos deben ser consignados, convirtiéndose en metadatos necesarios e imprescindibles para la materialización de la transferencia física o de responsabilidad de custodia de la serie.

221. Como en el caso de los metadatos mínimos obligatorios, deberán ser custodiados en el repositorio físico del SGDE/SGDEA formando parte del documento o expediente electrónico o separado de éste, con las mismas garantías respecto a la univocidad entre ambos elementos.

1.7. Documentación

222. Los procesos expuestos en el apartado 1.5 deben estar documentados. Se tendrán en cuenta las directrices que puedan establecer las autoridades calificadoras y archivísticas competentes, de acuerdo con la legislación de archivos que sea de aplicación en cada caso.

1.8. Formación

223. Dado que la implantación de la Administración electrónica supone cambios muy importantes con respecto a la gestión administrativa tradicional, anualmente, se incluirán en el Programa de Formación del Departamento actuaciones destinadas a la formación continua y capacitación del personal responsable tanto de la ejecución y del control de la gestión de los documentos electrónicos, como de su tratamiento y conservación en repositorios o archivos electrónicos.

224. Se diseñarán, en concreto, acciones formativas específicas para cada uno de los tipos de actores involucrados en los diferentes procesos de gestión documental contemplados en la presente Política.

225. Asimismo, se diseñarán acciones formativas encaminadas a difundir el conocimiento de la cultura digital, el documento electrónico, el expediente electrónico y tramitación electrónica en general, partiendo de la base de que sin una comunicación interna y formación adecuadas el conocimiento e implementación de la tramitación electrónica sería inviable.

1.9. Supervisión y auditoría

226. Los procesos de gestión de documentos electrónicos, el programa de tratamiento de documentos electrónicos y la presente Política serán objeto de auditorías con una periodicidad de 5 años. Estas auditorías podrán ser abordadas en el contexto de las auditorías del ENS.

227. Para la realización de estas auditorías se tendrán en cuenta las siguientes Normas y Estándares internacionales aplicables a las auditorías de Gestión documental: ISO 30300 e ISO 15489.

1.10. Gestión de la Política

228. El mantenimiento, actualización y publicación electrónica del presente documento corresponderá al Gestor de la Política identificado en el apartado 1.3.2.

229. Se promoverá la constitución de una comisión técnica de carácter multidisciplinar, con presencia de los gestores de la Política, de gestores de procedimiento administrativo y de los organismos autónomos, con el objetivo de realizar un seguimiento de la implantación de la Política y proponer las revisiones necesarias sobre la misma.

2. PROCEDIMIENTOS INSTRUMENTALES PARA LA GESTIÓN DE DOCUMENTOS

2.1. Firma electrónica

230. Todos los documentos electrónicos que formen parte de un procedimiento administrativo deberán expedirse y firmarse electrónicamente, tal como establece el artículo 41.2 del Real Decreto 1671/2009.

El índice asociado a un expediente electrónico se firmará electrónicamente cuando se cierre dicho expediente.

231. La firma electrónica realizada sobre los documentos electrónicos administrativos deberá reunir los requisitos de la firma electrónica avanzada en el sentido que indica la Ley 59/2003 de firma electrónica. En concreto, el sistema de firma que se utilice deberá garantizar:
    - La identificación precisa del firmante, lo que garantiza la autenticidad.
    - La posibilidad de detectar cualquier cambio del documento con posterioridad a la firma, permitiendo certificar su integridad.
    - La vinculación unívoca de la firma tanto al firmante como al documento firmado, necesaria para asegurar el no repudio.
    - Su realización por medios que el firmante mantenga bajo su control exclusivo[19].

232. Los sistemas de firma electrónica de los documentos electrónicos comprendidos en esta Política se dividen en dos modalidades:
    - Firma electrónica avanzada basada en certificados reconocidos. Esta firma electrónica se realizará con arreglo a la Política de Firma Electrónica y de Certificados de la Administración General del Estado. Los formatos y clases que se utilicen para la firma deberán estar incluidos expresamente en dicha Política.
    - Otros sistemas de firma electrónica, con arreglo al artículo 16 de la LAECSP. Estos sistemas de firma deben aprobarse mediante Orden Ministerial, Resolución del titular del Organismo Público o acuerdo del Consejo de Ministros, tal y como establece el artículo 11 del Real Decreto 1671/2009.

[19] Este requisito, que se pensó originariamente para los sistemas de firma basados en certificado electrónico, debe interpretarse en un sentido más amplio para acomodar otros sistemas de firma. Proponemos la interpretación siguiente: Para que la firma se complete, es indispensable que el firmante proporcione al dispositivo de firma un elemento de información que esté asociado unívocamente a él y que solamente él conozca o posea. Tal elemento de información puede ser la clave privada de un certificado, un *token*, una contraseña robusta…

233. En el Anexo X se referencian tanto la Política de Firma Electrónica y de Certificados actualmente vigente como las disposiciones que aprueban otros sistemas de firma electrónica en el ámbito del MECD. La actualización de este Anexo no exigirá la modificación formal del presente documento.

234. Los documentos que se firmen electrónicamente deberán haberse generado o transformado a alguno de los formatos recogidos en la NTI del Catálogo de Estándares. Como excepción, las Sedes Electrónicas podrán admitir la firma por los ciudadanos de documentos en otros estándares abiertos o de uso generalizado por los ciudadanos, con arreglo al artículo 11 del ENI.

235. Los documentos administrativos firmados deberán incorporar una referencia temporal que informe de la fecha y hora en que se produjo la firma. Esta referencia temporal puede ser:
    - "Marca de tiempo", en la que se toma la fecha y hora del equipo del firmante o de otro dispositivo al que tenga acceso.
    - "Sello de tiempo", en la que la fecha y hora de la firma está certificada por un prestador de servicios de certificación que asegure su exactitud e integridad. Es el sistema que se recomienda adoptar en esta Política.

236. Los escenarios que se contemplan para la firma electrónica de documentos administrativos y los medios recomendados se detallan en los siguientes apartados.

2.1.1. Firma electrónica de documentos por el ciudadano

237. En este escenario, una persona física o jurídica utiliza la firma electrónica para la presentación de solicitudes por medio de alguna de las Sedes Electrónicas gestionadas por el MECD o sus Organismos Autónomos dependientes.

238. La firma electrónica se utiliza en este caso para asegurar tanto la identidad del solicitante como la integridad de la propia solicitud y de los documentos electrónicos que la acompañan.

239. Establecemos las siguientes consideraciones sobre este supuesto:
    - El ciudadano podrá utilizar cualquiera de los sistemas de firma (basada en certificado reconocido o en otros medios) contemplados en esta Política. Los sistemas de firma admitidos deben aparecer descritos en la información publicada en la propia Sede, tal y como establece el artículo 6.1.e del Real Decreto 1671/2009.
    - La firma electrónica de los documentos electrónicos adjuntos a la solicitud se puede verificar por cualquiera de estos medios:
        - Firmando electrónicamente cada documento por separado.

- Incorporando a la solicitud electrónica una huella o resumen digital ("*hash*") de cada documento y firmando electrónicamente dicha solicitud, la cual deberá incorporar los resúmenes anteriores.

240. La solicitud firmada se considerará un documento electrónico siempre que incluya al menos la información suficiente para identificar el trámite al que se vincula, la identidad del solicitante y las referencias de los documentos que se adjunten (o sus huellas digitales, cuando su firma se realice junto a la propia solicitud).

241. Sin decantarse por ninguna tecnología de firma, esta Política recomienda que los responsables de las Sedes tomen todas las medidas técnicas a su alcance para que la operación de firma electrónica resulte lo más amigable y sencilla posible al interesado, limitando al máximo la dependencia de la descarga y ejecución de componentes "software" en el equipo o dispositivo en que el ciudadano realice la firma.

242. Tanto la realización como la verificación de la firma por el ciudadano no deben exigir el uso de aplicaciones o productos "*software*" propietarios, de acuerdo con el principio de neutralidad tecnológica. Las propias Sedes electrónicas deben proporcionar o referenciar a servicios sencillos, gratuitos y fiables para completar esta verificación.

2.1.2. Firma electrónica de documentos por la Administración en el desarrollo de actuaciones automatizadas

243. En este escenario se contempla la firma de documentos utilizando un sistema de información adecuadamente programado, sin necesidad de la intervención de un empleado público. Esta firma se puede completar para actos de trámite o resolutorios de procedimientos, así como para actos de comunicación, tal y como establece el anexo de la Ley 11/2007 y la NTI de Política de Firma Electrónica y de certificados de la Administración.

244. En este sentido, podemos enfrentarnos a dos situaciones que van a recibir análogo tratamiento:
    - Firma en tiempo real de documentos individuales, generalmente mediante la invocación a un servicio web o una interfaz expuesta.
    - Firma en diferido de un conjunto extenso de documentos.

245. En ambos casos, se podrá utilizar uno de los siguientes sistemas de firma:
    - Firma con certificado reconocido utilizando un sello electrónico. El sello electrónico deberá cumplir los requisitos establecidos en el artículo 19 del Real Decreto 1671/2009.

Cuando se utilice este sistema de firma, en la Sede Electrónica corporativa deberá ofrecerse un servicio gratuito para la validación del sello electrónico.

- Firma basada en Código Seguro de Verificación (CSV), que cumpla los requisitos establecidos en el artículo 20 del Real Decreto 1671/2009.

En este caso, el documento electrónico firmado deberá poder recuperarse desde la Sede Electrónica corporativa para cotejar su validez, al menos durante el plazo que marque la disposición por la que se habilite este sistema de firma. Se exceptúa el caso en el que al documento firmado con CSV se le firme de nuevo con un sello electrónico, en donde no será necesario dicho cotejo.

2.1.3. Firma electrónica de empleados públicos en el ejercicio de sus competencias

246. Este escenario contempla los casos en que un empleado público firme electrónicamente documentos como parte de un procedimiento administrativo (gestionado total o parcialmente de forma electrónica), en el ejercicio de competencias que tenga atribuidas normativamente en virtud del cargo o puesto que desempeña. Por este motivo, se supone que este escenario va a repetirse en el tiempo mientras la persona conserve dicha competencia.

247. En este contexto no se contemplan aquellos casos en que un empleado público firme de modo ocasional un documento, en especial para iniciar una solicitud dentro de un procedimiento vinculado a su carrera administrativa (como puede ser la participación en concursos de méritos, cursos de formación, petición de permisos…). Estas situaciones se equiparan a la firma de documentos y solicitudes como ciudadanos, con la particularidad de que en estos casos podrá utilizarse el certificado de empleado público que se menciona más abajo.

248. En relación a los documentos electrónicos generados por el personal al servicio del MECD, en virtud de lo expuesto en el artículo 19 de la Ley 11/2007, así como los artículos 21 y 22 del Real Decreto 1671/2009, se emplearán:

- El certificado de empleado público, que identifica tanto al titular como al órgano en el que presta sus servicios. Esta característica lo hace idóneo para su aplicación, por lo que se recomienda esta opción siempre que se encuentre disponible.
- La firma electrónica basada en el Documento Nacional de Identidad.
- Los sistemas de firma basada en Código Seguro de Verificación, siempre que se cumplan los requisitos establecidos en el artículo 20 del Real Decreto 1671/2009. Cuando se utilice este sistema, deberá poder recuperarse el documento electrónico firmado desde un

repositorio documental corporativo para efectuar su cotejo, excepto si dicho documento fue además firmado con un sello electrónico.

2.1.4. Firma longeva

249. Se conoce como "firma longeva" aquella que permite poder comprobar la validez de la firma electrónica realizada en cualquier momento posterior a su realización y, especialmente, una vez transcurrido un tiempo prolongado, mucho más allá del período de validez del certificado digital con que se generó.

250. El SGDE que se utilice debería permitir que todas las firmas electrónicas de documentos y expedientes administrativos sean longevas desde su incorporación al gestor documental. No obstante, si la complejidad técnica de la firma longeva hiciera inviable satisfacer este requisito, se exigirá que se firmen en formato longevo en el momento de su transferencia y cambio de custodia del SGDE al SGDEA, con arreglo a los calendarios de conservación de las correspondientes series documentales.

251. La firma longeva deberá realizarse con un certificado reconocido, en alguno de los formatos para firma longeva admitidos en la Política de Firma Electrónica y de Certificados de la AGE, en los que se incluyan tanto los certificados de la cadena de confianza como las evidencias de su validez (o en su caso las referencias a los mismos), y utilizando además un sellado de tiempo.

252. Se recomienda que, para no depender de la continuidad de servicio a largo plazo de los correspondientes Prestadores de Servicios de Certificación (PSC), se utilicen formatos de firma longeva que almacenen todos los certificados electrónicos que componen la cadena de confianza –partiendo del certificado con el que se realiza la firma–, así como las evidencias –obtenidas de los correspondientes PSC– de que dichos certificados eran válidos en el momento de la firma. El anexo XIII recopila los formatos de firma longeva vigentes en la actualidad.

253. Cuando la firma longeva se realice en el momento de la transferencia con cambio de custodia del SGDE al SGDEA, podrá hacerse con uno de los siguientes tipos de certificados:
    - Certificado de sello electrónico del organismo responsable de la custodia del documento. Es el sistema recomendado, ya que facilitará enormemente la gestión del posterior resellado de modo automático como se indica más abajo.
    - Certificado de empleado público, realizado por personal con competencia en la gestión y conservación del SGDEA.

2.1.5. Resellado de documentos firmados en formato longevo

254. Los documentos firmados electrónicamente con formato de firma longeva deben ser firmados de nuevo en las siguientes situaciones:
    - Cuando haya riesgo de obsolescencia o vulnerabilidad de alguno de los algoritmos con los que se realizó la anterior firma longeva (por ejemplo, por ser necesario ampliar la longitud de las claves criptográficas).
    - Cuando el formato bajo el que se realizó la anterior firma longeva deje de estar recogido como estándar en la Política de Firma Electrónica.
    - Cuando vaya a caducar el sello electrónico con el que se firmaron.

255. En los casos anteriores:
    - La nueva firma longeva deberá realizarse durante el período de transición que se establezca, y siempre antes de que expire la validez del algoritmo o formato en que se realizó la anterior firma.
    - En lo posible, deberá generarse de forma automática, usando mecanismos de resellado con sello electrónico.

2.1.6. Resellado de documentos firmados en formato no longevo

256. Cuando el SGDE utilizado no hiciera posible utilizar formatos longevos desde la incorporación, se deberán tomar medidas para que los documentos custodiados en dicho SGDE sean firmados de nuevo, utilizando mecanismos de resellado con sello electrónico, cuando se produzca alguna de las situaciones descritas en el apartado anterior para los documentos firmados en formato longevo.

2.2. Protocolo de digitalización de documentos

257. El protocolo que se describe en el presente apartado parte de la NTI de Digitalización de Documentos, y será adoptado por cada Entidad en función de sus necesidades específicas.

258. El proceso de digitalización se llevará a cabo cuando se pretenda aportar al expediente electrónico documentos de naturaleza física, excluyendo aquellos soportes que registren sonido, video o ambos. Los escenarios con los que podemos encontrarnos son los siguientes:
    - Digitalización de documentos en soporte tradicional aportados por el propio ciudadano, y entregados en una Oficina de Registro presencial con ocasión del inicio o tramitación de una solicitud.

- Documentos en soporte tradicional digitalizados por un empleado público, durante la tramitación de un procedimiento administrativo, para su incorporación al expediente electrónico asociado.
- Digitalización masiva de volúmenes elevados de archivos administrativos con expedientes en soporte tradicional. A su vez, aquí podemos diferenciar:
  - Digitalización realizada por una Unidad administrativa con sus propios medios.
  - Digitalización realizada por un tercero prestador de servicios por cuenta de una Unidad administrativa.

259. El proceso de digitalización se puede realizar en dos modalidades:
    - En tiempo real: En el caso del primer escenario del párrafo anterior (258), esta modalidad se realizará si lo permiten los medios técnicos de la oficina de Registro. El funcionario digitaliza la documentación en papel aportada para su incorporación a un expediente electrónico y devuelve la misma al ciudadano.
    - En diferido: En el caso del primer escenario del párrafo anterior (258), el organismo podrá considerar como independientes los procesos de registro y de digitalización. Para ello, una vez recogidos los documentos en formato físico, se genera una carátula para cada uno de los mismos, de forma que el proceso de digitalización se pueda realizar con posterioridad. Dicha carátula contendrá la información necesaria para la correcta incorporación de cada documento al expediente final en la unidad tramitadora.
    - En ambas modalidades, los documentos digitalizados se podrán incorporar de forma provisional a un Expediente de Registro, que recopila los documentos con un asiento registral y se transfiere a la unidad administrativa competente para su tramitación.
    - Respecto de la validez de los documentos obtenidos como "copias electrónicas auténticas" y/o su consideración como copias electrónicas compulsadas, se seguirá lo establecido en los artículos 44 y 50 del Real Decreto 1671/2009. En ambos casos, las imágenes obtenidas deberán ser firmadas electrónicamente.

260. El formato de salida de la imagen digital se corresponderá con alguno de los recogidos en la categoría "Formatos de ficheros - Imagen y/o texto" de la NTI de Catálogo de Estándares. Se recomienda que el formato de salida predeterminado sea PDF o PDF/A (versión 1.4 o superior), a menos que el tratamiento posterior a realizar con el documento haga más aconsejable otro diferente.

261. Si el formato de salida lo admite, en el momento de la digitalización se informarán los metadatos complementarios del procedimiento de digitalización que contempla el esquema de metadatos del e-EMGDE de la organización:
    - Resolución: Se corresponde con el metadato e-EMGDE 14.3.
    - Tamaño: Se corresponde con el metadato e-EMGDE 14.4.
    - Dimensiones físicas: Se corresponde con el metadato e-EMGDE 14.4.1.
    - Unidades: Se corresponde con el metadato e-EMGDE 14.4.4.
    - Profundidad del color: Correspondiente al metadato e-EMGDE 14.5.
    - Idioma: Se corresponde con el metadato e-EMGDE 11.

Además, debe informarse el metadato e-EMGDE 15.1: Soporte con el valor 'Digitalizado'

262. La incorporación de los metadatos citados al SGDE que utilice la organización debe realizarse de forma automática, por medio de las funcionalidades ofrecidas por el propio SGDE u otro sistema que opere en una capa superior.

263. El Anexo XI incluye la tabla que recopila los requisitos mínimos recomendados para la digitalización de documentos para su tramitación administrativa.

264. A criterio de la unidad tramitadora, además del proceso de digitalización se contempla la posibilidad de la realización del proceso de reconocimiento óptico de caracteres (en sus siglas en inglés, OCR). El documento resultante del procesamiento OCR se tratará como borrador de trabajo asociado a la imagen digital, de modo que no tendrá la consideración de documento electrónico administrativo (por ejemplo, no se firmará digitalmente). Se aconseja que este proceso se realice de forma simultánea a la obtención de la imagen digital, para seleccionar la resolución más adecuada.

265. Se realizará un control de calidad de los documentos digitalizados que incluirá, como mínimo las siguientes verificaciones:
    - Corrección de las imágenes obtenidas en cuanto a calidad de la imagen o en cuanto a criterios técnicos:
        - Resolución adecuada al tipo documental.
        - Color adecuado al tipo documental.
        - Formato adecuado al tipo documental.
        - Alineación correcta de la imagen.
    - Corrección de las imágenes obtenidas en cuanto a fidelidad con el original:
        - Digitalización de todas las páginas del documento.

- Digitalización sin incluir información que no aparece en el original.
- Visualización y legibilidad de la imagen.

266. En los casos en que se realice una digitalización masiva, estos controles se realizarán a partir de una muestra estadísticamente representativa. Tal muestreo debe realizarse necesariamente para la correcta recepción de trabajos de digitalización masiva realizados por terceros por cuenta de la Administración.

2.3. Copiado auténtico de documentos

267. Una copia auténtica es un nuevo documento, expedido por una organización con competencias atribuidas para ello, con valor probatorio pleno sobre los hechos o actos que documenta, equivalente al documento original. En el momento de la expedición de una copia auténtica se acredita su autenticidad desde la perspectiva de su correspondencia con el original y tiene efectos certificantes en cuanto que garantiza la autenticidad de los datos contenidos. Según el artículo 43 del Real Decreto 1671/2009, si la copia electrónica generada no comporta cambio de formato ni de contenido, tiene la eficacia jurídica del documento electrónico original o de la copia electrónica auténtica original.

268. Como tal, los efectos de las copias auténticas de documentos públicos (ya sean generados por la Administración o por el ciudadano) no se limitan al marco de un procedimiento administrativo determinado, sino que tienen la misma validez y eficacia que los documentos originales produciendo idénticos efectos frente a las organizaciones y los interesados.

269. La copia auténtica puede consistir en la transcripción del contenido del documento original o en una copia realizada por cualesquiera medios informáticos, electrónicos o telemáticos. Se expide a partir de:
    - El documento original.
    - Una copia auténtica.

270. Tal y como dicta el Real Decreto 1671/2009 en su artículo 43, la conservación de los originales es obligatoria.

271. Además, el artículo 51 del Real Decreto 1671/2009 dicta que en el caso de que el formato de los documentos y expedientes del archivo deje de figurar entre los admitidos en la gestión por el ENI, los responsables se encargarán del copiado auténtico con cambio de formato.

2.3.1. Características de la copia electrónica auténtica

272. Una copia electrónica auténtica es un nuevo documento, incluyendo todo o parte del contenido del original. Según el Real Decreto 1671/2009 se considera copia electrónica auténtica de documentos electrónicos presentados tanto:
    - Los documentos digitalizados o provenientes de otras fuentes.
    - El documento electrónico autenticado con firma electrónica del organismo, que integra contenido variable firmado remitido por el usuario, por ejemplo, en un archivo en formato XML o PDF generado a partir de los datos suministrados por el usuario.

273. En su caso, puede ser necesario reasignar valores a los metadatos mínimos obligatorios, como el identificador, el nombre, las fechas, etc. Explícitamente, se debe incluir una referencia en el metadato "e-EMGDE26 - Identificador del documento origen".

274. El Real Decreto 1671/2009 establece que, si la nueva copia incluye algún tipo de cambio sobre el original o la copia electrónica auténtica a partir de la que se ha generado, debe cumplirse que:
    - La Administración conserve el documento electrónico original.
    - La copia se realice en los términos que establezca la Administración.
    - Debe figurar en el metadato correspondiente (e-EMGDE20 – Estado de elaboración) que es una copia, como se detallará más adelante.
    - Debe ir firmada, según establecen los artículos 18 y 19 de la Ley 11/2007. Se aplicarán aquí las directrices de la Política descritas en el apartado 2.1 Firma electrónica.

275. Por lo tanto, se admite la posibilidad de generar copias electrónicas auténticas a partir de otras copias electrónicas auténticas siempre que se observen los requisitos establecidos en los apartados anteriores.

2.3.2. Características de la copia electrónica auténtica con cambio de formato

276. La copia electrónica con cambio de formato se obtiene a partir de la conversión según el apartado VIII del Real Decreto 1671/2009, generando un nuevo documento electrónico con diferente formato o versión.

277. En el procedimiento de conversión se tendrá en cuenta:
    - La aplicación de los procedimientos de conversión descritos en la NTI de Política de Gestión de Documento Electrónico.

- La conservación del contenido, el contexto y la estructura del origen, así como la identificación de aquellos componentes que requieran tratamiento específico.
- El nuevo formato debe:
- Pertenecer al Catálogo de estándares.
- Permitir la reproducción de la información original sin pérdida de información.

278. Si se debe conformar como copia auténtica, se contemplarán los requisitos del apartado "Características de la copia electrónica auténtica".

279. En el metadato "Estado de elaboración" (e-EMGDE20) debe figurar el texto "EE02 (Copia electrónica auténtica con cambio de formato)".

2.3.3. Copia electrónica parcial auténtica

280. La copia electrónica parcial auténtica se extrae del contenido de un único documento origen, permitiendo mantener la confidencialidad de los datos que no afecten al interesado.

281. En el metadato “Estado de elaboración” (e-EMGDE20) debe figurar “EE04 (Copia electrónica parcial auténtica)”.

2.3.4. Copia electrónica auténtica de documento electrónico público administrativo

282. Según el artículo 49 del Real Decreto 1671/2009, los ciudadanos podrán ejercer el derecho a obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan condición de interesados de acuerdo con lo dispuesto en la normativa reguladora del respectivo procedimiento.

283. La obtención de la copia podrá realizarse mediante extractos de los documentos o se podrán utilizar otros métodos electrónicos que permitan mantener la confidencialidad de aquellos datos que no afecten al interesado.

284. La autenticidad de los documentos se verificará siguiendo las pautas de la NTI de Documento Electrónico.

2.3.5. Copia electrónica auténtica de documentos en soporte no electrónico

285. El artículo 44 del Real Decreto 1671/2009 regula las copias electrónicas de documentos en soporte papel o susceptible de digitalización, tanto de la Administración como del ciudadano.

286. Define como "imagen electrónica" el resultado de aplicar un proceso de digitalización a un documento en soporte papel o en otro soporte que permita la obtención fiel de dicha imagen.

287. Define como "digitalización" el proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en un fichero electrónico que contiene la imagen codificada, fiel e íntegra, del documento[20].

288. Las imágenes electrónicas que realice la Administración se consideran copias electrónicas auténticas siempre que:
    - El documento que se copia sea original o copia auténtica.
    - La copia electrónica se firme digitalmente según la Ley 11/2007 y figure su carácter de "copia" en los metadatos.
    - La imagen electrónica se codifique conforme a los formatos, niveles de calidad y condiciones técnicas especificadas en el ENI y se genere conforme a las normas establecidas.

289. Si la imagen electrónica se obtiene a partir de copia auténtica en papel, no es necesaria la intervención del órgano depositario del documento administrativo original.

290. En el metadato "e-EMGDE20 - Estado de elaboración" debe figurar "EE03 (Copia electrónica auténtica de documento papel)".

2.3.6. Compulsa electrónica de documentos

291. A efectos de compulsa, el Real Decreto 1671/2009 regula en el artículo 50 que, si la oficina receptora de un documento cuenta con los medios necesarios, y no es obligatoria la entrega del original, puede proceder a la obtención de una copia electrónica de los documentos a compulsar.

292. Las copias serán firmadas electrónicamente y tendrán el carácter de copia compulsada o cotejada sin que se acredite la autenticidad del documento original[21].

293. Dado que no se puede asegurar con plenas garantías la autenticidad de los documentos compulsados en origen, sólo se admitirá la compulsa en destino, es decir, aquella realizada por

[20] Los aspectos relacionados con este procedimiento se tratan en profundidad en el apartado 2.2 Protocolo de digitalización de documentos.
[21] Se tomará como base lo dispuesto en la Ley 11/2007 y el Real Decreto 772/1999.

el registro del organismo receptor de la documentación; o bien la compulsa realizada por un fedatario público. En cualquier otro caso, se tratará el documento obtenido como "Copia".

2.3.7. Copia en papel auténtica de documentos administrativos electrónicos

294. El artículo 45 del Real Decreto 1671/2009 especifica los siguientes requisitos para que las copias emitidas en papel a partir de documentos electrónicos administrativos se consideren copias auténticas:
    - Que el documento electrónico sea:
        - Documento electrónico original.
        - Copia electrónica auténtica del documento electrónico original.
        - Copia electrónica auténtica del original en soporte papel.
    - Que incluya un código u otro sistema para la verificación de la copia mediante acceso a los archivos electrónicos del órgano u organismo público (Código Seguro de Verificación o CSV).
    - Que sea obtenida conforme a las normas de competencia y procedimiento que en cada caso se aprueben, incluidas las de obtención automatizada.

2.3.8. Documentos aportados por el ciudadano

295. En el artículo 48 del Real Decreto 1671/2009 se especifica que los interesados pueden aportar a su expediente copias digitalizadas de documentos (una imagen electrónica acorde a ENI), que no tendrá carácter de copia auténtica y cuyo contenido se verificará:
    - Por parte del interesado mediante firma electrónica avanzada.
    - Mediante cotejo por parte de la Administración. Si no es posible, puede requerir la exhibición del original.

2.3.9. Destrucción de documentos en soporte no electrónico[22]

296. El artículo 46 del Real Decreto 1671/2009 establece que los documentos originales y las copias auténticas en papel o cualquier otro soporte no electrónico se pueden eliminar en los siguientes casos:

[22] Este proceso es independiente de los procedimientos descritos en el apartado 1.5.9, centrado en la eliminación de documentos electrónicos.

- Por resolución adoptada por el órgano responsable del procedimiento o custodia, con informe previo de la Comisión Calificadora de Documentos Administrativos y dictamen favorable de la Comisión Superior Calificadora de Documentos Administrativos.
- Si no se trata de documentos con valor histórico, artístico o de otro carácter relevante que aconseje su conservación y protección, o en el que figuren firmas u otras expresiones manuscritas o mecánicas que confieran al documento un valor especial.

297. El expediente de eliminación debe incluir un análisis de los riesgos relativos al supuesto de destrucción de que se trate, con mención explícita de las garantías de conservación de las copias electrónicas y del cumplimiento de las condiciones de seguridad que, en relación con la conservación y archivo de los documentos electrónicos, establezca el ENS.

298. La destrucción de cualquier tipo de documento diferente de los anteriores se regirá por lo previsto en el Real Decreto 1164/2002.

3. REFERENCIAS

3.1. Legislación y normativa

i. Ley 9/1968, de 5 de abril (BOE de 6 de abril), sobre secretos oficiales.
http://www.boe.es/buscar/pdf/1968/BOE-A-1968-444-consolidado.pdf

ii. Ley Orgánica 1/1982, de 5 de mayo (BOE de 14 de mayo), sobre protección civil del derecho al honor, intimidad personal y familiar y a la propia imagen.
http://www.boe.es/boe/dias/1982/05/14/pdfs/A12546-12548.pdf

iii. Ley Orgánica 5/1985, de 19 de junio (BOE de 20 de junio), del Régimen Electoral General.
https://www.boe.es/boe/dias/1985/06/20/pdfs/A19110-19134.pdf

iv. Ley 16/1985, de 25 de junio (BOE de 29 de junio), del Patrimonio Histórico Español.
http://www.boe.es/boe/dias/1985/06/29/pdfs/A20342-20352.pdf

v. Ley 14/1986, de 25 de abril (BOE de 29 de abril), General de Sanidad.
http://www.boe.es/boe/dias/1986/04/29/pdfs/A15207-15224.pdf

vi. Ley 12/1989, de 9 de mayo de 1989 (BOE de 11 de mayo), de la Función Estadística Pública.
http://www.boe.es/boe/dias/1989/05/11/pdfs/A14026-14035.pdf

vii. Ley 30/1992, de 26 de noviembre (BOE de 27 de noviembre), de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
http://www.boe.es/buscar/pdf/1992/BOE-A-1992-26318-consolidado.pdf

viii. Real Decreto 772/1999, de 7 de mayo (BOE de 22 de mayo), por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro.
http://www.boe.es/boe/dias/1999/05/22/pdfs/A19410-19415.pdf

ix. Ley Orgánica 15/1999, de 13 de diciembre (BOE de 14 de diciembre), de Protección de Datos de Carácter Personal.
http://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf

x. Real Decreto 1164/2002, de 8 de noviembre (BOE de 15 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.
http://www.boe.es/boe/dias/2002/11/15/pdfs/A40139-40143.pdf

xi. Ley 41/2002, de 14 de noviembre (BOE de 15 de noviembre), básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
http://www.boe.es/boe/dias/2002/11/15/pdfs/A40126-40132.pdf

xii. Ley 58/2003, de 17 de diciembre (BOE de 18 de diciembre), General Tributaria.
http://www.boe.es/boe/dias/2003/12/18/pdfs/A44987-45065.pdf

xiii. Ley 59/2003, de 19 de diciembre (BOE de 20 de diciembre), de firma electrónica.
http://www.boe.es/boe/dias/2003/12/20/pdfs/A45329-45343.pdf

xiv. Real Decreto Legislativo 1/2004, de 5 de marzo (BOE de 8 de marzo), por el que se aprueba el texto refundido de la Ley del Catastro Inmobiliario.
http://www.boe.es/buscar/pdf/2004/BOE-A-2004-4163-consolidado.pdf

xv. Ley 27/2006, de 18 de julio (BOE de 19 de julio), por la que se regulan los derechos de acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente.
http://www.boe.es/boe/dias/2006/07/19/pdfs/A27109-27123.pdf

xvi. Ley 11/2007, de 22 de junio (BOE de 23 de junio), de acceso electrónico de los ciudadanos a los Servicios Públicos.
https://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf

xvii. Real Decreto 1720/2007, de 21 de diciembre (BOE de 19 de enero de 2008), 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.
http://www.boe.es/buscar/pdf/2008/BOE-A-2008-979-consolidado.pdf

xviii. Ley 37/2007, de 16 de noviembre (BOE de 17 de noviembre), sobre reutilización de la información del sector público. Modificada en virtud de Ley 18/2015, de 9 de julio (BOE de 10 de julio).
http://www.boe.es/buscar/pdf/2007/BOE-A-2007-19814-consolidado.pdf

xix. Resolución de 24 de junio de 2009 (BOE de 20 de julio), de la Presidencia del Consejo Superior de Deportes, por la que se crea el registro electrónico del Consejo Superior de Deportes.
http://www.boe.es/boe/dias/2009/07/20/pdfs/BOE-A-2009-12001.pdf

xx. Real Decreto 1671/2009, de 6 de noviembre (BOE de 18 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. Modificado parcialmente por Real Decreto 668/2015 de 17 de julio (BOE de 18 de julio)
http://www.boe.es/buscar/pdf/2009/BOE-A-2009-18358-consolidado.pdf

xxi. Orden CUL/3410/2009, de 14 de diciembre (BOE de 19 de diciembre), por la que se regula el Registro Electrónico del Ministerio de Cultura
http://www.boe.es/buscar/pdf/2009/BOE-A-2009-20389-consolidado.pdf

xxii. Real Decreto 3/2010, de 8 de enero (BOE de 29 de enero), por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf

xxiii. Real Decreto 4/2010, de 8 de enero (BOE de 29 de enero), por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1331.pdf

xxiv. Orden EDU/947/2010, de 13 de abril (BOE de 17 de abril), por la que se crea y regula el Registro Electrónico del Ministerio de Educación.
http://www.boe.es/boe/dias/2010/04/17/pdfs/BOE-A-2010-6103.pdf

xxv. Resolución de 22 de septiembre de 2010 (BOE de 25 de octubre), de la Biblioteca Nacional de España, por la que se crea el Registro Electrónico de la Biblioteca Nacional de España.
http://www.boe.es/boe/dias/2010/10/25/pdfs/BOE-A-2010-16222.pdf

xxvi. Sistema de firma de clave concertada para actuaciones en el Registro Electrónico del Ministerio de Cultura, regulado por Orden CUL/1132/2011, de 28 de abril (BOE de 6 de mayo).
http://www.boe.es/boe/dias/2011/05/06/pdfs/BOE-A-2011-7976.pdf

xxvii. Real Decreto 1708/2011, de 18 de noviembre (BOE de 25 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.
http://www.boe.es/boe/dias/2011/11/25/pdfs/BOE-A-2011-18541.pdf

xxviii. Política de Firma Electrónica y de Certificados de la Administración General del Estado, aprobada por Resolución de 29 de noviembre de 2012 (BOE de 13 de diciembre), de la Secretaría de Estado de Administraciones Públicas.
http://www.boe.es/boe/dias/2012/12/13/pdfs/BOE-A-2012-15066.pdf

xxix. Ley 19/2013, de 9 de diciembre (BOE de 10 de diciembre), de Transparencia, Acceso a la Información Pública y Buen Gobierno.
http://www.boe.es/boe/dias/2013/12/10/pdfs/BOE-A-2013-12887.pdf

xxx. Orden PRE/1838/2014, de 8 de octubre, por la que se publica el Acuerdo de Consejo de Ministros, de 19 de septiembre de 2014 (BOE de 9 de octubre), por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas.
http://www.boe.es/boe/dias/2014/10/09/pdfs/BOE-A-2014-10264.pdf

xxxi. Ley 18/2015, de 9 de julio, por la que se modifica la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público
https://www.boe.es/boe/dias/2015/07/10/pdfs/BOE-A-2015-7731.pdf

xxxii. Ley 39/2015, de 1 de octubre (BOE de 2 de octubre), del Procedimiento Administrativo Común de las Administraciones Públicas.
https://boe.es/boe/dias/2015/10/02/pdfs/BOE-A-2015-10565.pdf

xxxiii. Ley 40/2015, de 1 de octubre (BOE de 2 de octubre), de Régimen Jurídico del Sector Público.
http://boe.es/boe/dias/2015/10/02/pdfs/BOE-A-2015-10566.pdf

3.2. Normas Técnicas de Interoperabilidad

i. Resolución de 19 de julio de 2011 (BOE de 30 de julio), de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Digitalización de Documentos.
http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011-13168.pdf

ii. Resolución de 19 de julio de 2011 (BOE de 30 de julio), de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico.
http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011-13169.pdf

iii. Resolución de 19 de julio de 2011 (BOE de 30 de julio), de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Expediente Electrónico.
http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011-13170.pdf

iv. Resolución de 19 de julio de 2011 (BOE de 30 de julio), de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración.
http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011-13171.pdf

v. Resolución de 19 de julio de 2011 (BOE de 30 de julio), de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos.
http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011-13172.pdf

vi. Resolución de 19 de julio de 2011 (BOE de 30 de julio), de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Modelo de Datos para el Intercambio de asientos entre las entidades registrales.
http://www.boe.es/boe/dias/2011/07/30/pdfs/BOE-A-2011-13174.pdf

vii. Resolución de 28 de junio de 2012 (BOE de 26 de julio), de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos.
http://www.boe.es/boe/dias/2012/07/26/pdfs/BOE-A-2012-10048.pdf

viii. Resolución de 3 de octubre de 2012 (BOE de 31 de octubre), de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Catálogo de estándares.
http://www.boe.es/boe/dias/2012/10/31/pdfs/BOE-A-2012-13501.pdf

3.3. Guías técnicas

i. Guía de aplicación de la NTI de Política de Gestión de Documentos Electrónicos.
http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/Guia_de_aplicacion_Politica_de_gestion_de_documento_electronico.pdf

3.4. Otras referencias

i. Documento ISO/TC 46/SC 11 N800R1, relativo a "orientaciones sobre la elaboración de un esquema de metadatos", y que constituye un desarrollo de la norma ISO 23081
http://isotc.iso.org/livelink/livelink/fetch/-8800112/8800136/8800147/N800R1_Construccion_de_un_esquema_de_metadatos_-_Por_Donde_Empezar_Metadatos_-_ESP.pdf?nodeid=11331471&vernum=-2

ii. Criterios generales para la valoración de los documentos de la Administración General del Estado. Documento aprobado por la Comisión Superior Calificadora de Documentos Administrativos, en sesión de 27 de noviembre de 2003.
http://www.mecd.gob.es/cultura-mecd/dms/mecd/cultura-mecd/areas-cultura/archivos/mc/cscda/documentos/MetodologiaComSup.pdf

iii. Esquema de metadatos para la Gestión del Documento Electrónico (e-EMGDE).
http://administracionelectronica.gob.es/ctt/eemgde

iv. Guía de Comunicación Digital para la Administración del Estado.
http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Guia_de_Comunicacion_Digital_para_la_Administracion_General_del_Estado.html

v. Norma UNE-ISO 15489-1:2006. Información y documentación. Gestión de documentos. Parte 1: Generalidades.
http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0035751#.VSzWc1CFn1c

vi. Norma UNE-ISO 15489-1:2016. Information and documentation -- Records management -- Part 1: Concepts and principles.
http://www.iso.org/iso/catalogue_detail.htm?csnumber=62542

vii. Norma UNE-ISO 23081-1:2008. Información y documentación. Procesos de gestión de documentos. Metadatos para la gestión de documentos. Parte 1: Principios.
http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0041438#.VSzXZVCFn1c

viii. Norma UNE-ISO 23081-2:2011. Información y documentación. Procesos de gestión de documentos. Metadatos para la gestión de documentos. Parte 2: Elementos de implementación y conceptuales.
http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0046569#.VSzX0lCFn1c

ix. Norma UNE-ISO 30300:2011. Información y documentación. Sistemas de gestión para los documentos. Fundamentos y vocabulario.
http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0048671

x. Norma UNE-ISO 30301:2011. Información y documentación. Sistemas de gestión para los documentos. Requisitos.
http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0048672

xi. Modelo de Política de gestión de documentos electrónicos del Ministerio de Hacienda y Administraciones Públicas.
http://www.seap.minhap.gob.es/dms/es/publicaciones/centro_de_publicaciones_de_la_sgt/Monografias0/parrafo/Politica_doc_electronicos/POLITICA-GESTION-Modelo/POLITICA%20GESTION%20Modelo.pdf

xii. NARA's Open government plan 2014-2016.
http://www.archives.gov/open/open-government-plan-3.0.pdf

xiii. Política de Gestión de Documentos del Ministerio de Hacienda y Administraciones Públicas.
http://www.minhap.gob.es/Documentacion/Publico/SGT/POLITICA%20DE%20GESTION%20DE%20DOCUMENTOS%20MINHAP/politica%20de%20gestion%20de%20documentos%20electronicos%20MINHAP.pdf

xiv. Requisitos del Modelo para la Gestión de Archivos Electrónicos.
http://www.moreq.info/files/moreq2010_vol1_v1_1_en.pdf

xv. Norma UNE-ISO 14641-1:2015 Archivo electrónico. Parte 1: Especificaciones para el diseño y funcionamiento de un sistema de información para la preservación de información digital.
http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0055412&PDF=Si#.VfvHL31KVkI

xvi. Norma UNE-ISO 14721:2015 Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS). Modelo de referencia.
http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0055413&PDF=Si#.VfvHvH1KVkI

xvii. E-ARK SIP Draft Specification.
http://www.eark-project.com/resources/project-deliverables/17-d32-e-ark-sip-draft-specification

3.5. Abreviaturas

AGE	Administración General del Estado.
CMIS	Content Management Interoperability Services.
CPCMAD	Comisión Permanente de la Comisión Ministerial de Administración Digital.
CSCDA	Comisión Superior Calificadora de Documentos Administrativos.
e-ARK	European Archival Records and Knowledge.
e-EMGDE	Esquema de Metadatos para la Gestión del Documento Electrónico.
ENI	Esquema Nacional de Interoperabilidad.

ENS	Esquema Nacional de Seguridad.
LAECSP	Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
LOPD	Ley Orgánica de Protección de Datos de carácter Personal.
LPHE	Ley de Patrimonio Histórico Español
MECD	Ministerio de Educación, Cultura y Deporte.
MINHAP	Ministerio de Hacienda y Administraciones Públicas.
NTI	Norma Técnica de Interoperabilidad.
PIA	Paquete de Información de Archivo.
PIC	Paquete de Información de Consulta.
PIT	Paquete de Información de Transferencia.
SG	Subdirección General.
SGDE	Sistema de Gestión de Documentos Electrónicos.
SGDEA	Sistema de Gestión de Documentos Electrónicos de Archivo.
SGTIC	Subdirección General de Tecnologías de la Información y las Comunicaciones.
TIC	Tecnologías de la Información y las Comunicaciones.

Subdirección General de Archivos Estatales

Plaza del Rey, 6 – 28004 Madrid

archivos.estatales@mecd.es

Subdirección General de Tecnologías de la Información y las Comunicaciones

Vitruvio, 4 – 28006 Madrid

secretaria.sgtic@mecd.es

MINISTERIO
DE EDUCACIÓN, CULTURA
Y DEPORTE