@dministración electrónica

eni Esquema Nacional de Interoperabilidad

POLÍTICA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS

(3ª EDICIÓN)

9. Guía de aplicación de eliminación

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA
MINISTERIO DE POLÍTICA TERRITORIAL Y FUNCIÓN PÚBLICA

TÍTULO: 9. Guía de aplicación de eliminación

Elaboración y coordinación de contenidos:
Grupo de Trabajo de PGD-e, en el marco del Plan de Acción de Transformación Digital

Impulsa: Grupo de trabajo para la Coordinación de Archivos de MINHAC y Comisión Ministerial de Administración Digital (CMAD)

Dirige: Subdirección General de Información, Documentación y Publicaciones de MINHAC
Responsable edición digital: Subdirección General de Información, Documentación y Publicaciones
Edición electrónica (versión 0): julio de 2019
Esta guía constituye un borrador abierto a aportaciones.
Disponible esta publicación en el Portal de Administración Electrónica (PAe):
http://administracionelectronica.gob.es/

Edita:
© Ministerio de Hacienda
Secretaría General Técnica
Subdirección General de Información, Documentación y Publicaciones
NIPO: 185-19-074-2

© Ministerio de Política Territorial y Función Pública
Secretaría General de Administración Digital
NIPO: 277-19-040-6

ÍNDICE

1. ANTECEDENTES 5

2. INTRODUCCIÓN 6

3. OBJETIVO Y ALCANCE DE LA GUÍA 8

3.1. Qué NO incluye la Guía 9

4. ÁMBITO DE APLICACIÓN Y DESTINATARIOS 10

5. ELIMINACIÓN 11

5.1. Normativa de interés 11

5.2. Diferencia entre borrado, destrucción y eliminación 12

5.2.1. Borrado 12

5.2.2. Borrado seguro 13

5.2.3. Destrucción segura 13

5.2.4. Eliminación segura 13

5.3. Metadatos a considerar 14

5.4. Trazabilidad 18

5.4.1. Metadato eEMGDE21 - TRAZABILIDAD 19

5.4.2. Metadato eEMGDE21.1 - ACCIÓN 19

5.4.3. Metadato eEMGDE21.1.1 – FECHA DE LA ACCIÓN 21

5.4.4. Metadato eEMGDE21.1.2 – ENTIDAD DE LA ACCIÓN 21

5.4.5. Metadato eEMGDE21.2 – MOTIVO REGLADO 22

5.4.6. Metadato eEMGDE21.3 – USUARIO DE LA ACCIÓN 22

5.4.7. Metadato eEMGDE21.6 – HISTORIA DEL CAMBIO 23

5.4.9. Metadato eEMGDE21.6.2 – VALOR ANTERIOR 24

5.5. Justificación y alcance 24

5.5.1. Ejecución de un dictamen de eliminación 25

5.5.2. Transferencia a archivo 26

5.5.3. Cambio de soporte 26

5.6. Nivel de protección de la información 26

5.7. Soportes de almacenamiento 27

5.7.1. Tipos de soportes de almacenamiento 28

5.7.2. Contexto de los soportes 28

5.7.3. Tipo de gestión de los soportes 29

5.8. Técnicas y métodos de borrado y destrucción seguros 29

5.8.1. Sobrescritura 30

5.8.2. Comandos a nivel firmware 30

5.8.3. Borrado criptográfico 30

5.8.4. Desmagnetización 31

5.8.5. Trituración 31

5.8.6.Desintegración 31
5.8.7.Aplastamiento 31
5.8.8.Pulverización 31

6. PROCESO DE ELIMINACIÓN 32

7. ETAPAS DEL PROCESO DE ELIMINACIÓN DE DOCUMENTOS ELECTRÓNICOS 36

8. DEFINICIONES Y ACRÓNIMOS 37

8.1. Definiciones 37

8.2. Acrónimos 37

9. REFERENCIAS 38

9.1. Legislación 38

9.2. Otros 38

ANEXO I. NORMATIVA 39

EQUIPO RESPONSABLE DE LA ELABORACIÓN DE LA POLÍTICA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS 48

ÍNDICE DE TABLAS

Tabla 1. Metadatos relacionados con la eliminación segura de documentos electrónicos 14

Tabla 2. Proceso de eliminación 32

Histórico de versiones del documento			
Versión	**Nombre del documento**	**Fecha**	**Descripción**
0	1. Guía de aplicación de eliminación	16/07/2019	Versión 0 aprobada por el grupo de trabajo GTPGD-e, en el marco del PATD

1. ANTECEDENTES

1. En el año 2014 se publicó la Política de Gestión de Documentos electrónicos del Ministerio, la primera que se ha elaborado en el entorno de la Administración General del Estado. Por haber sido consensuada entre los diferentes organismos del Ministerio, así como por la Subdirección General de los Archivos Estatales del Ministerio de Educación Cultura y Deportes y el Ministerio de la Presidencia, se ha convertido en un referente para las políticas de gestión de documentos electrónicos posteriores, tanto de la AGE como de las comunidades autónomas y entidades locales.
2. En el año 2016 se aprobó la segunda edición de la Política de Gestión de Documentos Electrónicos del entonces Ministerio de Hacienda y Función Pública, que fue galardonada con el premio al mejor proyecto archivístico en el VII Congreso de Archivos de Castilla y León (25-27 de mayo de 2016).
3. Pasados cuatro años desde la publicación de la Política de Gestión de documentos electrónicos, se hace necesaria una actualización de la misma, sobre todo, teniendo en cuenta las experiencias que se han tenido en administración electrónica en las aplicaciones de tramitación y archivo electrónico. También es necesaria la adaptación a la nueva normativa: la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, sin olvidar que en fechas próximas será aprobado el nuevo reglamento de administración electrónica, que desarrollará las dos leyes citadas.
4. En esta guía se aborda el proceso de gestión documental de destrucción o eliminación, recogido en la Política de Gestión de Documentos Electrónicos del MINHAP en su apartado “2.5.9 Destrucción o eliminación”. Se tratan aspectos como la distinción entre distintos niveles de borrado de documentos electrónicos, los tipos de soportes de almacenamiento, la gestión interna o externa de los mismos, los métodos y técnicas de borrado y destrucción seguros, el nivel de protección de la información y se exponen las pautas para ejecutar un proceso de eliminación segura en función de su alcance y de los motivos que han llevado a ponerlo en marcha.

2. INTRODUCCIÓN

5. Según los principios de la gestión documental, los documentos no son algo muerto o inactivo, sino que tienen una vida propia, un “ciclo vital” que contempla, a semejanza de cualquier otro, el nacimiento (creación), crecimiento (mantenimiento y uso) y decrecimiento y muerte (expurgo o eliminación) de los mismos. En este sentido, la gestión documental culmina con la decisión de conservación permanente o eliminación de los documentos.

6. De acuerdo con la legislación vigente en materia de documentos, archivos y patrimonio documental estatal, una vez transcurridos los plazos legales, la eliminación de los documentos de titularidad pública (incluidos aquéllos en soporte electrónico), en razón de su condición de patrimonio documental español, sólo y exclusivamente puede realizarse mediante autorización de la Comisión Superior Calificadora de Documentos Administrativos (CSCDA), siguiendo los procedimientos establecidos en la normativa que regula el funcionamiento de dicha comisión, y siempre y cuando se dictamine que los documentos han perdido todos sus valores primarios (jurídicos, administrativos, fiscales) y no poseen valores informativos ni históricos.

7. **No podrán eliminarse**, por tanto, los documentos o expedientes en los que se dé alguna de las siguientes circunstancias:

    i. Estén calificados como de “conservación permanente” de acuerdo con los dictámenes de la CSCDA.

    ii. No haya transcurrido el plazo establecido para su conservación, durante el cual pueda subsistir su valor probatorio de derecho y obligaciones de personas físicas o jurídicas.

    iii. No tengan la autorización previa establecida en la legislación vigente en materia de documentos, archivos y patrimonio documental.

8. Por otro lado, la eliminación, borrado o destrucción de documentos electrónicos afecta directamente a la seguridad de los datos, especialmente a los de carácter personal. El acceso o difusión no autorizados de los datos que un proceso de eliminación incompleto o mal ejecutado podría ocasionar, pone en riesgo su seguridad y vulnera la confidencialidad de la información.

9. Los documentos electrónicos, como ficheros codificados de forma binaria, se guardan de manera permanente en los denominados soportes de almacenamiento.

10. Existen distintos tipos de soportes, magnéticos, ópticos o memorias de estado sólido, algunas de cuyas características pueden limitar el éxito de una operación de borrado de documentos electrónicos, cuando se pretende que sea exhaustiva o irreversible:

    i. En algunos discos duros magnéticos hay sectores que están protegidos u ocultos o que son defectuosos. Los comandos de borrado que incorporan los distintos sistemas operativos o las aplicaciones informáticas que gestionan documentos electrónicos no pueden acceder a estos sectores, por lo que los datos presentes en ellos no se eliminan cuando se borra un fichero.

    ii. En soportes de acceso secuencial, por ejemplo cintas magnéticas, no sería posible borrar físicamente un fichero que se encuentra entre otros ficheros sin afectar a estos, por lo que debería borrarse todo el contenido del soporte.

iii. En las memorias de estado sólido las operaciones de borrado sólo se pueden aplicar a bloques enteros. Cuando la porción a borrar es más pequeña, la información se marca como borrada pero los datos permanecen en el soporte. Un borrado seguro de una memoria solida debería afectar necesariamente a todo el dispositivo.

11. Esto supone que mediante el uso de determinadas técnicas sería posible acceder a estos ficheros o documentos electrónicos una vez eliminados y recuperarlos. Además, los procesos de destrucción de los documentos en papel no pueden aplicarse a la eliminación de los electrónicos, lo que hace necesario contar con procedimientos específicos y adaptados a la nueva realidad de la Administración electrónica, teniendo presente como mínimo las particularidades de los soportes de almacenamiento, el alcance y los motivos de la eliminación y el nivel de protección de la información. En definitiva, la eliminación de un documento electrónico debería ser tan segura como lo es la destrucción de un documento en papel.

3. OBJETIVO Y ALCANCE DE LA GUÍA

12. El objetivo de esta guía de aplicación es desarrollar los conceptos en relación con la eliminación de documentos electrónicos que establece la Política de Gestión de Documentos electrónicos, publicada en el año 2014:

    i. Distinción entre eliminación y borrado seguro de documentos electrónicos y destrucción de soportes.

    ii. Justificación y alcance de la eliminación

    iii. Clasificación de los soportes de almacenamiento.

    iv. Nivel de protección de la información.

    v. Selección de los métodos y técnicas de borrado o destrucción seguros más adecuados teniendo en cuenta los tipos de soportes de almacenamiento, su contexto y el tipo de gestión de los mismos.

13. Aunque los sistemas de almacenamiento son el entorno adecuado para la conservación de los documentos electrónicos, esta guía podría aplicarse asimismo a la eliminación segura de información de soportes asociados a dispositivos móviles o soportes locales de ordenadores portátiles, PC o servidores.

14. Un sistema de almacenamiento está formado básicamente por una cabina de almacenamiento como mínimo (o una librería robótica) y redes de comunicaciones (que conectan los distintos servidores al almacenamiento), y permite la interconexión de un conjunto de soportes, de forma que puedan proporcionar espacio de almacenamiento a diversas plataformas tecnológicas como *clusters* de servidores, *mainframes*, plataformas virtualizadas, NAS, etc.

15. Entre las características que convierten a los sistemas de almacenamiento en el entorno más adecuado para garantizar la conservación a largo plazo de los documentos electrónicos, están:

    i. Proporcionar una capacidad de almacenamiento flexible ante una demanda creciente y muy exigente en cuanto a espacio. El aumento de la capacidad en estos sistemas no es disruptiva en cuanto al servicio que ofrecen.

    ii. Garantizar la accesibilidad y disponibilidad de los datos ante posibles fallos (gracias a la redundancia de sus elementos físicos).

    iii. Ofrecer un rendimiento acorde a las necesidades de distintas aplicaciones y en función del ciclo de vida de los documentos electrónicos.

    iv. Separar el nivel físico del soporte del nivel lógico con el que trabajan las aplicaciones (lo que se denomina virtualización del almacenamiento).

    v. Replicar los datos contra sistemas similares.

16. Esto no impide que puedan aplicarse las técnicas de borrado seguro o destrucción segura de soportes a dispositivos de almacenamiento no vinculados a sistemas de almacenamiento, como discos duros de ordenadores personales, por ejemplo, o memorias de estado sólido de teléfonos móviles. Sin embargo, estos casos deberían contemplarse fuera de un proceso de eliminación reglado ya que los soportes de almacenamiento de dispo-

sitivos móviles o el almacenamiento local de un servidor, no son los medios más adecuados para garantizar la conservación a largo plazo de los documentos electrónicos. La aplicación de estas técnicas se justificaría simplemente como una medida de seguridad por las características de la información que contienen.

3.1. Qué NO incluye la Guía

17. Esta guía aporta únicamente recomendaciones o aspectos a considerar en relación con la eliminación de documentos electrónicos. No busca ser un manual de los procesos a aplicar para la eliminación de documentos electrónicos que, como el resto del Sistema de Gestión Documental, deberán desarrollarse de acuerdo con las directrices establecidas en la Política de Gestión Documental aplicable.

4. ÁMBITO DE APLICACIÓN Y DESTINATARIOS

18. Esta guía tendrá su ámbito de aplicación en los servicios centrales y periféricos del Ministerio de Hacienda y del Ministerio de Política Territorial y Función Pública. También será de aplicación en las entidades u organismos dependientes o vinculados al ministerio que así lo deseen.

19. Dentro del ámbito de aplicación definido anteriormente, los destinatarios del contenido de esta guía son los siguientes:

    i. Responsables de gestión, conservación y archivo de documentos y expedientes electrónicos.

    ii. Desarrolladores de aplicaciones de gestión, conservación y archivo de documentos y expedientes electrónicos.

5. ELIMINACIÓN

5.1. Normativa de interés

20. Esta sección identifica las normas y articulado de interés para la eliminación, destrucción o borrado de documentos electrónicos. En el Anexo 1 de esta Guía se incluye el texto de los artículos mencionados.

    i. El marco normativo general de la administración electrónica se establece con las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

    ii. El artículo 17 de la Ley 39/2015, Archivo de documentos, además de tratar el archivo electrónico de expedientes finalizados menciona que la eliminación de los documentos electrónicos deberá ser autorizada.

    iii. El artículo 13 de la Ley 39/2015, Derechos de las personas en sus relaciones con las Administraciones Públicas, establece asimismo la obligación de la Administración de proteger los datos de carácter personal de los ciudadanos que figuren en sus archivos.

    iv. El artículo 49 de la Ley 16/1985, de Patrimonio Histórico Español, establece que forman parte del Patrimonio Documental los documentos “generados, conservados o reunidos en el ejercicio de su función por cualquier organismo o entidad de carácter público”.

    v. El Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original, define el procedimiento de eliminación de documentos.

    vi. El Real Decreto 1401/2007, de 29 de octubre, por el que se regula la composición, funcionamiento y competencias de la Comisión Superior Calificadora de Documentos Administrativos, define su finalidad y funciones.

    vii. El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, incluye una medida de protección específica (borrado y destrucción mp.si.5) relativa a los soportes de información: “borrado seguro” para aquellos que se puedan reutilizar y “destrucción de forma segura” cuando las características de un soporte de información impidan su borrado seguro o cuando el tipo de información que contengan así lo requiera.

    viii. El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el marco de la Administración Electrónica, contempla la destrucción reglamentaria como la fase final del ciclo de vida de los documentos electrónicos que no han sido seleccionados para su conservación permanente, señalando que “si el resultado del procedimiento de evaluación documental así lo establece, borrado de la información, o en su caso, destrucción física de los

soportes, de acuerdo con la legislación que resulte de aplicación, dejando registro de su eliminación."

ix. La NTI de Política de Gestión Documental, aprobada por resolución de 28 de junio de 2012 de la Secretaría de Estado de Administraciones Públicas, incluye entre los procesos de gestión de documentos electrónicos, la calificación de los documentos, la transferencia y la destrucción o eliminación.

x. La Guía de Aplicación de la NTI de Política de Gestión de Documentos Electrónicos, considera que "el proceso de eliminación de documentos electrónicos constituye un proceso clave en la gestión de documentos y tiene como objetivo impedir su restauración y posterior reutilización. Para ello, es necesario aplicar un proceso que incluya tanto el borrado de la información (el propio documento y sus metadatos) como la destrucción física del soporte, en función de las características del formato y las del propio soporte".

5.2. Diferencia entre borrado, destrucción y eliminación

21. Aunque en la normativa de referencia los términos eliminación, borrado o destrucción de documentos electrónicos se usan indistintamente, para expresar la eliminación física de un documento electrónico, tanto de su contenido informativo como de su entidad como fichero informático, desde un punto de vista técnico estos términos representan dimensiones distintas.

22. Teniendo en cuenta la normativa, a los efectos de esta guía, se define cada uno de estos términos, borrado, destrucción y eliminación, en los apartados siguientes.

5.2.1. Borrado

23. Sería la operación técnica de eliminación del fichero o ficheros correspondientes a un documento electrónico, de un soporte o conjunto de soportes de almacenamiento. Se realiza mediante comandos específicos del sistema operativo o de las aplicaciones que gestionan estos documentos.

24. En cuanto a su alcance, puede afectar sólo a uno o a un conjunto determinado de documentos, y a una parte o a la totalidad de un soporte (si se borra toda la información que contiene).

25. El borrado de un documento electrónico consiste básicamente en marcar como libre el espacio que ocupa en un soporte, de forma que pueda ser empleado por el sistema operativo más adelante. Sin embargo, este tipo de borrado sería el mínimo recomendado siempre y cuando el alcance de la eliminación no afecte a la totalidad de un soporte o conjunto de soportes[1] y existan otras medidas de seguridad de la información, como una política de accesos conforme a las características de la dicha información y a su nivel de protección. Obviamente permite la reutilización de los soportes de almacenamiento.

26. En esta guía de aplicación lo denominaremos como **borrado de nivel 0.**

[1] *Ver la medida de protección mp.si.5 del Esquema Nacional de Seguridad.*

5.2.2. Borrado seguro

27. Se trataría de un procedimiento basado en técnicas especiales como la sobrescritura, la desmagnetización, etc., cuyo objetivo es eliminar por completo un conjunto de documentos electrónicos previamente seleccionados, de un soporte o conjunto de soportes de almacenamiento, de manera que **sea prácticamente imposible recuperar la información que contenían ni siquiera mediante técnicas especiales**. **No siempre permite la reutilización del soporte,** ya que algunas técnicas, como la desmagnetización, lo pueden dejar inservible.
28. En cuanto a su alcance este tipo de borrado afecta a la totalidad de un soporte, nunca a una parte.
29. **Este tipo de borrado es el recomendable** para asegurar la confidencialidad de la información de los documentos electrónicos borrados. También puede efectuarse como paso previo a la destrucción de los soportes.
30. En función de las técnicas o métodos que se apliquen podrá ser más o menos exhaustivo o seguro, por lo que éstos deberán seleccionarse teniendo en cuenta las características de la información y del soporte de almacenamiento, de si será destruido o no posteriormente o reutilizado, del alcance de la eliminación, de la gestión interna o externa de los soportes, etc.
31. Distinguiríamos en función de su exhaustividad dos niveles, a los que denominaremos de menor a mayor**, borrado de nivel 1 y nivel 2.**

5.2.3. Destrucción segura

32. Se definiría como el procedimiento de **destrucción física de un soporte de almacenamiento** que ha contenido documentos electrónicos, mediante técnicas específicas, que garanticen que la información no pueda ser recuperada. Para aumentar la seguridad del procedimiento puede combinarse con un borrado seguro previo a la misma.
33. La destrucción segura se justificaría por la **imposibilidad de reutilización del soporte**, por un cambio de soporte por obsolescencia o fallo del mismo, o porque las características de la información de los documentos aconsejen esta destrucción (por ejemplo, por su elevado nivel de confidencialidad).

5.2.4.Eliminación segura

34. En el contexto de esta guía la eliminación segura de documentos electrónicos sería el **proceso que englobaría la utilización de técnicas y métodos de borrado o destrucción seguros,** en función del tipo de soporte empleado, del nivel de protección de la información, de las causas que motivan la eliminación de los documentos electrónicos y del alcance de la misma. La eliminación segura también incluiría los procedimientos de verificación del resultado del borrado seguro y de la destrucción de soportes.

5.3. Metadatos a considerar

35. Los metadatos del "Esquema de Metadatos para la Gestión y del Documento Electrónico (e-EMGDE)" que se podrían consultarse o procesarse durante el proceso de eliminación se han recogido en la tabla 1.

Tabla 1. Metadatos relacionados con la eliminación segura de documentos electrónicos

METADATO	TIPO	DESCRIPCIÓN	CÓMO CUBRIRLO
eEMGDE2.1 – identificador – Secuencia de identificador	Obligatorio	Secuencia de caracteres que identifica la entidad dentro de un dominio local o global	
eEMGDE3.1 –Nombre -Nombre natural	Obligatorio para la transferencia	Nombre real que se da a la entidad	
eEMGDE3.2 –Nombre -Nombre del fichero	Opcional	Título o nombre del fichero de datos que constituye el documento	
eEMGDE4.1 – Fechas – Fecha inicio	Obligatorio	Fecha en la que una entidad inicia su existencia	
eEMGDE4.2 – Fechas – Fecha fin	Condicional	Fecha en la que una entidad finalizó su existencia, se disolvió o se destruyó	Debe utilizarse una vez que una entidad finaliza o se disuelve, se borra o se destruye y siempre que se vaya a realizar su transferencia, en caso de una entidad documento
eEMGDE8.1.1 – Seguridad – Nivel de seguridad - Nivel de acceso	Condicional	Término normalizado de acuerdo con un esquema de valores que indica el nivel de acceso de la entidad	Secreto, Reservado, Confidencial, No clasificado
eEMGDE8.1.2 – Seguridad – Nivel de seguridad -Código de la política de control de acceso	Condicional	Nivel de la Política de control de acceso de organizaciones individuales o, si se desarrolla, de la Política de control de acceso nacional, autonómica, local, sectorial, etc.	A, B, C, E
eEMGDE8.2.1 – Seguridad – Advertencia de Seguridad - Texto de la advertencia	Condicional	Palabra o palabras que conforman la advertencia de seguridad de que un Documento, Actividad o Regulación requiere un tratamiento especial, y que sólo las personas autorizadas pueden tener acceso	
eEMGDE8.2.2 – Seguridad – Advertencia de Seguridad – Categoría de la advertencia	Condicional	Naturaleza de una advertencia de seguridad	

METADATO	TIPO	DESCRIPCIÓN	CÓMO CUBRIRLO
eEMGDE8.3 – Seguridad - Permisos	Condicional	Autorización o acreditación de un agente o actividad, que determina sus derechos de acceso, uso y reutilización de los documentos	
eEMGDE8.4 - Seguridad – Sensibilidad Datos Carácter Personal	Condicional	Término normalizado de acuerdo con los niveles de clasificación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y normativa de desarrollo	Básico, Medio, Alto
eEMGDE8.5 – Seguridad - Clasificación ENS	Condicional	Término normalizado que denota el nivel de seguridad de un sistema de información de conformidad con los criterios del Esquema Nacional de Seguridad (ENS)	Bajo, Medio, Alto
eEMGDE8.6 – Seguridad - Nivel de confidencialidad de la información	Condicional	Evaluación, en cuanto al nivel de la dimensión de seguridad "confidencialidad", de la información recogida en un documento, de acuerdo con el Esquema Nacional de Seguridad	Bajo, Medio, Alto
eEMGDE9.1 – Derechos de acceso, uso y reutilización - Tipo de acceso	Obligatorio para la transferencia	Indica si el documento se rige por el régimen general de libre acceso o si, por el contrario, está sujeto a alguna de las limitaciones recogidas en la legislación o normativa de aplicación	Libre, Parcialmente restringido, Restringido
eEMGDE9.2 – Derechos de acceso, uso y reutilización - Código de la causa de limitación	Condicional	Asignar una codificación a la causa de restricción de acceso para facilitar las consiguientes acciones automáticas precisas sobre el documento	A,B,C,D,E,F,G,H,I,J,K,L,M Valores A - La seguridad nacional B - La defensa C - Las relaciones exteriores D- La seguridad pública E- La prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios F- La igualdad de las partes en los procesos judiciales y la tutela judicial efectiva G- Las funciones administrativas de vigilancia, inspección y control H- Los intereses económicos y comerciales I - La política económica y monetaria J - El secreto profesional y la propiedad intelectual e industrial

METADATO	TIPO	DESCRIPCIÓN	CÓMO CUBRIRLO
			K - La garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión L - La protección del medio ambiente M - Otros
eEMGDE9.3 – Derechos de acceso, uso y reutilización - Causa legal / Normativa de limitación	Condicional	Referencia de la ley o norma específica que afecta al documento o expediente en cuanto a su régimen de acceso	
eEMGDE13.1.1.1 Calificación – Valoración -Valor primario - Tipo de valor	Obligatorio para la transferencia	Identificación de los diferentes valores primarios que poseen los documentos, expedientes y series	Administrativo, Fiscal, Jurídico, Otros
eEMGDE13.1.1.2 Calificación – Valoración - Valor primario –Plazo	Obligatorio para la transferencia	Determinación del plazo de prescripción de los valores primarios de los documentos, expedientes y series documentales	Indicar plazo en años
eEMGDE13.1.2 – Calificación – Valoración -Valor secundario	Obligatorio para la transferencia	Determinación de la existencia de valores secundarios en los documentos	Sí / No / Sin cobertura de calificación
eEMGDE13.2.1 – Calificación – Dictamen - Tipo de dictamen	Obligatorio para la transferencia	Tipo de decisión emitida por la autoridad calificadora que debe aplicarse sobre los documentos a lo largo de su ciclo de vida y una vez realizada su valoración	CP: Conservación Permanente. *(Continúa)* EP: Eliminación parcial. ET: Eliminación total. PD: Pendiente de dictamen.
eEMGDE13.2.2 – Calificación – Dictamen - Acción Dictaminada	Condicional	Acción concreta que se aplica al documento en base al dictamen adoptado por una autoridad calificadora	
eEMGDE13.2.3 – Calificación – Dictamen - Plazo de ejecución de la acción dictaminada	Condicional	Plazo en el que se tiene que ejecutar la acción concreta que se aplica al documento y que figura en el sub-elemento eEMGDE13.2.2 – Acción dictaminada	Introducir un valor numérico relativo a años
eEMGDE13.3.1 – Calificación – Transferencia - Fase de Archivo	Obligatorio para la transferencia	Indicación de la fase de archivo correspondiente al momento del ciclo de vida del documento que se transfiere	Archivo Central / Archivo Intermedio / Archivo Histórico

METADATO	TIPO	DESCRIPCIÓN	CÓMO CUBRIRLO
eEMGDE13.3.2 – Calificación – Transferencia - Plazo de Transferencia	Obligatorio para la transferencia	Plazo de tiempo en que se traspasa la custodia de las diversas fracciones de series documentales, en cumplimiento del calendario de conservación resultante del proceso de valoración documental	Valor numérico en años
eEMGDE15.1 – Ubicación - Soporte	Condicional	Objeto físico sobre el que se almacena un documento	Opcional para documentos electrónicos
eEMGDE15.2 – Ubicación -Localización	Opcional	Localización actual (física o de sistema) del documento	
eEMGDE21.1.1 – Trazabilidad -Acción -Descripción acción	Opcional	Descripción del tipo de acción realizada sobre una o varias entidades del sistema	
eEMGDE21.1.2 – Trazabilidad – Acción - Fecha de la acción	Opcional	Indicador del momento en que la acción señalada en eEMGDE21.1 – Acción ha sido ejecutada	
eEMGDE21.1.3 – Trazabilidad – Acción - Objeto de la acción	Opcional	Indicador del componente del documento sobre el que se ejecuta la acción señalada en eEMGDE21.1.1 – Descripción de la acción	
eEMGDE21.2 - Trazabilidad - Motivo reglado	Opcional	Razón por la que se lleva a cabo la acción asociada expresada en eEMGDE21.1 - Acción	
eEMGDE21.3- Trazabilidad - Usuario de la acción	Opcional	Identificación del usuario que ha realizado la acción determinada en eEMGDE21.1 - Acción	
eEMGDE21.4 - Trazabilidad -Descripción	Opcional	Explicación detallada en texto libre de la acción determinada en eEMGDE21.1.1 – Descripción de la acción	
eEMGDE22.1 – Clasificación – Código de clasificación	Obligatorio para expediente	Identificador único codificado que determina una categoría en un cuadro de clasificación o en el SIA	
eEMGDE22.2 – Clasificación – Denominación de clase	Obligatorio para la transferencia	Indicador en lenguaje natural que identifica de forma unívoca la clase asignada dentro de un Cuadro de Clasificación	

METADATO	TIPO	DESCRIPCIÓN	CÓMO CUBRIRLO
eEMGDE22.3 – Clasificación – Tipo de clasificación (SIA / Funcional)	Obligatorio para la transferencia	Término que señala si los valores del elemento corresponden a una clasificación administrativa del procedimiento de acuerdo con el SIA, y en cumplimiento con el metadato obligatorio correspondiente de la NTI de Expediente electrónico, o si se refieren a la adscripción de la entidad a una categoría funcional dentro del cuadro de clasificación funcional de documentos de la organización	

5.4. Trazabilidad

36. En relación a la trazabilidad del proceso de eliminación de documentos, entre los metadatos a considerar en el proceso de eliminación de documentos, del "Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE)", se dispone de un **metadato específico de trazabilidad (eEMGDE21)**, que contiene información acerca de las acciones de gestión documental realizadas sobre las distintas entidades y sus metadatos, las fechas en las que se produjeron dichas acciones, la base normativa para realizarlas, y el usuario que las llevó a cabo. Este metadato aplica tanto a documentos, como a expedientes o a series.

37. El metadato mencionado consta de los siguientes subelementos:

    i. eEMGDE21.1 Acción
    ii. eEMGDE21.1.1 Fecha de la acción
    iii. eEMGDE21.1.2 Entidad de la acción
    iv. eEMGDE21.2 Motivo reglado
    v. eEMGDE21.3 Usuario de la acción
    vi. eEMGDE21.6 Historia del cambio

38. Debido a la importancia de este metadato y con vistas a facilitar la comprensión de su función y su estructura, se recoge a continuación la definición de este metadato, y de sus subelementos, tal y como figuran en el Anexo 7 de la "Política de Gestión de Documentos Electrónicos":

5.4.1. Metadato eEMGDE21 - TRAZABILIDAD

eEMGDE21 - TRAZABILIDAD						
Nombre formal	eEMGDE.Trazabilidad					
Sub-elemento de	No aplica.					
Definición	Información acerca de las acciones realizadas sobre las distintas entidades y metadatos de las mismas, las fechas de realización, la base normativa para realizarlas, y el usuario que las realizó.					
Aplicabilidad	Documento/Expediente/Serie					
Obligación	Opcional.					
Automatizable	-	**Repetible**	✓	**En el punto de captura**	-	
Sub-elementos	eEMGDE21.1 - Acción eEMGDE21.1.1 - Fecha de la acción eEMGDE21.1.2 - Entidad de la acción eEMGDE21.2 - Motivo reglado eEMGDE21.3 - Usuario de la Acción eEMGDE21.6 - Historia del cambio					
Valores	**Esquema**	Sin definir				
	Valor por defecto	Sin definir				
Compatibilidad	**ISO 23081**	Historial de eventos.				
Finalidad	Mantener una pista de auditoría inalterable de las acciones realizadas en el sistema.					
Comentarios	La trazabilidad equivale a lo que se conoce como pista de auditoría de tal modo que la implantación de este elemento y sus subelementos dependerá de implantaciones específicas que deben respetar las buenas prácticas y normas técnicas relativas a seguimiento de acciones.					
Ejemplos	-					

5.4.2. Metadato eEMGDE21.1 - ACCIÓN

eEMGDE21.1 - ACCIÓN					
Nombre formal	eEMGDE.Trazabilidad.Accion				
Sub-elemento de	eEMGDE21 - Trazabilidad				
Definición	Indicador del tipo de acción realizada sobre una o varias entidades del sistema				
Aplicabilidad	Documento/Expediente/Serie				
Obligación	Opcional				
Automatizable	✓	**Repetible**	✓	**En el punto de captura**	-
Sub-elementos	eEMGDE21.1.1 - Fecha de la acción eEMGDE21.1.2 - Entidad de la acción				
Valores	**Esquema**	Sin definir.			
	Valor por defecto	Sin definir.			
Compatibilidad	**ISO 23081**	Historial de eventos.			

eEMGDE21.1 - ACCIÓN	
Finalidad	Denominar el tipo de acción realizada sobre una determinada entidad en un momento determinado del tiempo.
Comentarios	Para definir el esquema de valores se puede tomar como base el Apéndice 7 del eEMGDE (*)
Ejemplos	*Accede a, Cambia, Borra*

(*) Adaptación del apéndice 7 del eEMGDE a las necesidades del Departamento en un entorno mono-entidad

39. El esquema de valores del metadato eEMGDE 21.1 –ACCION que se define en la “Política de Gestión de Documentos Electrónicos” es el siguiente:

Acción de gestión de documentos	Descripción
Accede a	Ejecuta el proceso de acceso a documentos.
Adjunta a	Crea un enlace entre dos objetos, generalmente documentos.
Borra	Acción que elimina (no modifica) los valores de un elemento de metadatos.
Cambia	Modificación del valor o estado de un elemento de metadatos o el contenido de un documento (incluye adiciones).
Cierra	Declara finalizada o terminada una agregación o actuación, cuando ya no puede contener más documentos o datos, o el valor no puede aplicarse a documentos actuales.
Contribuye a	Realización de una aportación al contenido del documento.
Convierte	Cambio del documento digital de un formato a otro.
Copia	Acto o proceso de duplicar un objeto, a partir de un proceso de reproducción
Crea	Responsabilidad de redactar el contenido del documento.
Descarga	Proceso de copiar datos de su localización de almacenamiento a un dispositivo local (o interno o externo a la organización).
Descifra	Proceso de volver a convertir datos cifrados a su forma original para que puedan comprenderse.
Destruye	Proceso de destruir físicamente el contenido de una entidad documento.
Elimina	Destrucción de un documento.
Cifra	Proceso de aplicar un protocolo de encriptación que representa datos digitales no legibles, excepto para aquellos que poseen la clave para descifrarlos.
Envía	Proceso de distribuir copias de un documento a uno o múltiples receptores.
Finaliza	Momento en que una entidad deja de existir, se cierra, se destruye.
Firma	Acto o proceso de adjuntar, incrustar o vincular un documento con un mecanismo que le da validez, en sus distintas variantes.
Imprime	Proceso de representar un documento sobre papel.
Incorpora	Añade una entidad a un determinado nivel de agregación del que debe formar parte.
Migra	Proceso de transferir documentos de un sistema a otro, manteniendo la autenticidad y sin conversión ni introducción de datos relevantes.
Reemplaza	Proceso de volver a copiar físicamente un documento a su almacenamiento después de su reutilización o edición por un agente particular.
Revisa	Proceso de examen que implica un chequeo del contenido contra criterios externos establecidos.
Transfiere	Proceso de mover un documento de una localización de almacenamiento a otra, incluida la transferencia fuera de línea.
Visualiza	Proceso de recuperar información en pantalla (no de copiarla ni de descargarla a un almacenamiento local).

40. Existen dos valores del metadato e-EMGDE21.1 relacionados con la eliminación de documentos:

    i. Destruye

    ii. Elimina

41. Dado que estos dos valores no permiten efectuar una trazabilidad de los distintos tipos de eliminación que se pueden llevar a cabo, y además la destrucción se efectúa sobre soportes, no sobre documentos, se propone la sustitución de esos dos valores por los siguientes, actualizando el Apéndice 7 del "Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE)":

    i. Borrado nivel 0

    ii. Borrado nivel 1

    iii. Borrado nivel 2

    iv. Destrucción de soporte

5.4.3. Metadato eEMGDE21.1.1 – FECHA DE LA ACCIÓN

eEMGDE21.1.1 - FECHA DE LA ACCIÓN						
Nombre formal	eEMGDE.Trazabilidad.Accion.FechaAccion					
Sub-elemento de	eEMGDE21.1. Acción					
Definición	Indicador del momento en que la acción señalada en eEMGDE21.1 ha sido ejecutada					
Aplicabilidad	Documento/Expediente/Serie					
Obligación	Opcional.					
Automatizable	✓	**Repetible**	✓	**En el punto de captura**	-	
Sub-elementos	No					
Valores	**Esquema**	*[<AAAA-MM-DD>T<hh:mm:ss>].* <ISO 8601>.				
	Valor por defecto	Sin definir.				
Compatibilidad	**ISO 23081**	Historial de eventos.				
Finalidad	Registrar el momento en que la acción señalada en eEMGDE21.1. ha sido ejecutada					
Comentarios	-					
Ejemplos	-					

5.4.4. Metadato eEMGDE21.1.2 – ENTIDAD DE LA ACCIÓN

eEMGDE21.1.2 - ENTIDAD DE LA ACCIÓN					
Nombre formal	eEMGDE.Trazabilidad.Accion.EntidadAccion				
Sub-elemento de	eEMGDE21.1 - Acción				
Definición	Indicador del componente del documento sobre el que se ejecuta la acción señalada en eEMGDE21.1.1 (contenido, metadatos…)				
Aplicabilidad	Documento/Expediente				
Obligación	Opcional				
Automatizable	✓	**Repetible**	✓	**En el punto de captura**	-
Sub-elementos	No				
Valores	**Esquema**	Contenido del documento/Metadatos del documento/Metadatos del expediente			
	Valor por defecto	Sin definir.			
Compatibilidad	**ISO 23081**	Historial de eventos.			
Finalidad	Denominar el tipo de acción realizada sobre una determinada entidad en un momento determinado del tiempo.				
Comentarios	-				
Ejemplos	-				

42. Como se ve en la tabla anterior, el elemento eEMGDE21.1.2-ENTIDAD DE LA ACCION es repetible, por lo que **se puede recoger en un mismo metadato e-EMGDE21-TRAZABILIDAD una acción de gestión documental que implique a varios elementos a la vez (por ejemplo, un cambio que afecte a varios metadatos de un mismo documento).**

5.4.5.Metadato eEMGDE21.2 – MOTIVO REGLADO

eEMGDE21.2 - MOTIVO REGLADO						
Nombre formal	eEMGDE.Trazabilidad.MotivoReglado					
Sub-elemento de	eEMGDE21 - Trazabilidad					
Definición	Razón por la que se lleva a cabo la acción asociada expresada en eEMGDE21.1 - Acción.					
Aplicabilidad	Documento/Expediente/Serie					
Obligación	Opcional					
Automatizable	×	**Repetible**	✓	**En el punto de captura**	-	
Sub-elementos	No					
Valores	**Esquema**	Sin definir.				
	Valor por defecto	Sin definir.				

eEMGDE21.2 - MOTIVO REGLADO		
Compatibilidad	**ISO 23081**	Historial de eventos.
Finalidad	Informar acerca de la motivación reglada por la que se ha llevado a cabo una determinada acción sobre una entidad.	
Comentarios	Toda acción realizada sobre las entidades del sistema debe tener una motivación, particularmente si es una acción de gestión de documentos o que pueda afectar a las propiedades de los mismos, o de alguna otra de las entidades del sistema. Este motivo puede ser una ley o disposición de rango legal, una norma técnica, un procedimiento interno, etc. Si no se satisface simultáneamente con el resto de sub-elementos de este elemento, existen indicios de que la acción es irregular, o de que de manera maliciosa o no intencionada afecta a las propiedades de las entidades implicadas.	
Ejemplos	- En virtud de la Orden CUL/2165/2009, de delegación de competencias. - Sin motivo reglado.	

5.4.6.Metadato eEMGDE21.3 – USUARIO DE LA ACCIÓN

eEMGDE21.3 - USUARIO DE LA ACCIÓN						
Nombre formal	eEMGDE.Trazabilidad.UsuarioAccion					
Sub-elemento de	eEMGDE21 - Trazabilidad					
Definición	Identificación del usuario que ha realizado la acción determinada en eEMGDE21.1 - Acción.					
Aplicabilidad	Documento/Expediente/Serie					
Obligación	Opcional					
Automatizable	✓	**Repetible**	✓	**En el punto de captura**	-	
Sub-elementos	No					
Valores	**Esquema**	Sin definir.				
	Valor por defecto	Sin definir.				
Compatibilidad	**ISO 23081**	Historial de eventos.				
Finalidad	Mantener una pista de auditoría inalterable de las personas que ejecutan las acciones realizadas en el sistema.					
Comentarios	El usuario puede ser un nombre de usuario, el nombre completo de la persona que realiza o realizó la acción, la dirección IP del equipo del usuario, etc., dependiendo de implantaciones específicas. En cualquier caso, la persona que realiza una determinada acción en una fecha y hora determinadas debe quedar suficientemente identificada.					
Ejemplos	*12345678A, 172.16.0.45*					

5.4.7. Metadato eEMGDE21.6 – HISTORIA DEL CAMBIO

eEMGDE21.6 - HISTORIA DEL CAMBIO		
Compatibilidad	**ISO 23081**	Historial de eventos.
Finalidad	- Registrar/rastrear los cambios sobre los metadatos de una entidad a lo largo del tiempo. - Hacer posible el que se realice y mantenga una historia completa de las acciones de las entidades. - Ayudar a documentar los efectos o resultados de las relaciones entre entidades. - Identificar aquellos elementos o sub-elementos que han cambiado como resultado de una relación. - Proporcionar una historia de los cambios a los elementos y sub-elementos de metadatos resultantes de las relaciones entre entidades. - Facilitar la comprensión de los cambios realizados sobre los metadatos de una entidad a lo largo del tiempo.	
Comentarios	Este sub-elemento se utiliza para almacenar los valores anteriores de los elementos o sub-elementos cuando una relación entre dos entidades (esto es, un evento) da como resultado cambios en uno o más de los valores actuales. No todas las relaciones dan como resultado cambios a los valores actuales de los elementos o sub-elementos. El nuevo valor de un elemento o sub-elemento se registrará en ese elemento o sub-elemento como el valor actual, sobrescribiendo por tanto el valor anterior. Si de una sola relación entre dos entidades resultan múltiples cambios, este sub-elemento debe repetirse para documentar cada cambio.	
Ejemplos	-	

eEMGDE21.6 - HISTORIA DEL CAMBIO					
Nombre formal	eEMGDE.Trazabilidad.HistoriaCambio				
Sub-elemento de	eEMGDE21 - Trazabilidad				
Definición	Información que registra el elemento de metadato que ha sido modificado sobre una determinada entidad y su valor anterior.				
Aplicabilidad	Documento/Expediente/Serie				
Obligación	Opcional				
Automatizable	-	**Repetible**	✓	**En el punto de captura**	-
Sub-elementos	21.6.1 Nombre del elemento 21.6.2 Valor anterior				
Valores	**Esquema**	Sin definir.			
	Valor por defecto	Sin definir.			

5.4.8. Metadato eEMGDE21.6.1 – NOMBRE DEL ELEMENTO

eEMGDE21.6.1 - NOMBRE DEL ELEMENTO					
Nombre formal	eEMGDE.Trazabilidad.HistoriaCambio.NombreElemento				
Sub-elemento de	eEMGDE21.6 - Historia del cambio				
Definición	Nombre de un elemento o subelemento de metadato cuyo valor ha sufrido algún tipo de modificación.				
Aplicabilidad	Documento/Expediente/Serie				
Obligación	Condicional				
Automatizable	✓	**Repetible**	×	**En el punto de captura**	×
Sub-elementos	No				
Valores	**Esquema**	Las etiquetas de elemento y sub-elemento utilizadas en este esquema.			
	Valor por defecto	Sin definir.			
Compatibilidad	**ISO 23081**	Historial de eventos.			
Finalidad	Identificar aquellos elementos o sub-elementos que han cambiado como resultado de una relación.				
Comentarios	Debe utilizarse en conjunción con el sub-elemento eEMGDE21.6.2 - Valor anterior para registrar qué metadato ha cambiado como resultado de una relación, y su valor real antes del cambio. También debe utilizarse en situaciones en las que no se registró ningún valor anterior en el elemento o sub-elemento afectado.				
Ejemplos	-				

5.4.9. Metadato eEMGDE21.6.2 – VALOR ANTERIOR

eEMGDE21.6.2 - VALOR ANTERIOR					
Nombre formal	eEMGDE.Trazabilidad.HistoriaCambio.ValorAnterior				
Sub-elemento de	eEMGDE21.6 - Historia del cambio				
Definición	Contenido anterior de un elemento o subelemento de metadato de una determinada entidad que ha sido modificado en un momento del tiempo.				
Aplicabilidad	Documento/Expediente/Serie				
Obligación	Opcional				
Automatizable	✓	**Repetible**	×	**En el punto de captura**	×
Sub-elementos	No				

eEMGDE21.6.2 - VALOR ANTERIOR		
Valores	**Esquema**	Sin definir.
	Valor por defecto	Sin definir.
Compatibilidad	**ISO 23081**	Historial de eventos.
Finalidad	- Registrar y rastrear los cambios sobre los metadatos de una entidad a lo largo del tiempo. - Hacer posible el que se realice y mantenga una historia completa de las acciones de las entidades. - Ayudar a documentar los efectos o resultados de las relaciones entre entidades. - Proporcionar una historia de los cambios realizados sobre los elementos y sub-elementos de metadatos resultantes de las relaciones entre entidades. - Facilitar la comprensión de los cambios realizados sobre los metadatos de una entidad a lo largo del tiempo.	
Comentarios	Debe utilizarse en conjunción con el sub-elemento eEMGDE21.6.1 - Nombre del elemento para identificar casos individuales de un elemento o sub-elemento que ha cambiado como resultado de una relación, y para registrar el valor real de ese elemento o sub-elemento antes del cambio. Este sub-elemento también debe utilizarse en situaciones en las que no se registró ningún valor anterior en el elemento o sub-elemento afectado. En cada caso, este sub-elemento registrará un valor nulo (un campo en blanco) o la cadena de texto *Sin valor anterior*.	
Ejemplos	-	

5.5. Justificación y alcance

43. Desde el punto de vista de la gestión documental, como se ha avanzado en la introducción de la presente Guía, en el ámbito de la Administración General del Estado la eliminación de documentos de titularidad pública (incluidos aquéllos en soporte electrónico) **únicamente puede realizarse** mediante autorización de la Comisión Superior Calificadora de Documentos Administrativos (CSCDA), siguiendo los procedimientos establecidos en la legislación vigente en materia de documentos, archivos y patrimonio documental.

44. Sin embargo, por su utilidad se han incluido en esta Guía recomendaciones de borrado para determinados escenarios que van más allá del concepto estricto de “eliminación” en el ámbito de la gestión documental, como son los casos de transferencia de documentos electrónicos y de cambio de soporte de los mismos.

45. De acuerdo con la previsión anterior, pueden señalarse tres **causas que podrían originar un proceso de eliminación** de documentos electrónicos:

    i. Ejecución de un dictamen de eliminación.

    ii. Transferencia a archivo.

    iii. Cambio de soporte.

46. Cada una de ellas determinará a su vez el alcance del proceso de eliminación:

    i. En cuanto a los documentos electrónicos, podrá suponer la eliminación total de un conjunto determinado de ellos, o parcial, si en el dictamen de la Comisión Superior Calificadora de Documentos Administrativos (CSCDA) así lo determinase. En el caso de eliminación total, podrían conservarse, si así se determinase, una serie de expedientes "testigo" o incluso únicamente los metadatos de los documentos o expedientes electrónicos.

    ii. En cuanto a los soportes, podrá afectar a su totalidad o a parte de los mismos.

47. Un aspecto que debe tenerse en cuenta, además, es que un mismo documento electrónico que forme parte de varios expedientes deberá conservarse mientras se conserven alguno de estos expedientes.

48. Un segundo aspecto por considerar, en relación al alcance, es la existencia de duplicados de los documentos electrónicos: copias de seguridad y réplicas. El proceso de eliminación debería incluir estos duplicados, especialmente en el caso de expedientes de eliminación o transferencia a archivo.

49. No se ha contemplado la eliminación de documentos electrónicos por error de los mismos, ya que esta operación no se considera un proceso de eliminación sino simplemente un borrado de los mismos.

5.5.1. Ejecución de un dictamen de eliminación

50. A iniciativa de cualquier organismo o del propio Grupo de Trabajo para la Coordinación de Archivos, éste podrá acordar la iniciación de un procedimiento de eliminación de documentos electrónicos.

51. Este acuerdo de iniciación, que **incluirá** un informe del órgano proponente que justifique la necesidad de eliminación de los documentos, acreditando el resultado del proceso de valoración documental, y una memoria relativa a la documentación de que se trate, se remitirá al Presidente de la Comisión Superior Calificadora de Documentos Administrativos (CSCDA). Contendrá además una propuesta de eliminación y una petición de dictamen.

52. Sobre este acuerdo la Comisión Superior Calificadora de Documentos Administrativos (CSCDA) **emitirá** dictamen preceptivo. En el caso de ser favorable a la propuesta de eliminación, el Subsecretario del Departamento ministerial o el Presidente o Director del Organismo público **adoptará** la resolución que considere oportuna. Si la resolución autoriza la eliminación deberá ser publicada en el BOE.

53. Una vez se haga ejecutiva la autorización para la eliminación, el organismo responsable de la custodia de los documentos abrirá un expediente de eliminación, que **incluirá**:

    i. La memoria realizada sobre la documentación y cualquier otra información o documentos presentados con la propuesta de eliminación, así como el texto de esta última.

    ii. El dictamen de la Comisión Superior Calificadora de Documentos Administrativos y el de cualquier otra Comisión que se haya pronunciado previamente.

    iii. La memoria del muestreo de la documentación a expurgar.

    iv. La resolución que haya autorizado la eliminación, así como cualquier otro documento administrativo o judicial relacionado con la misma.

    v. El acta de eliminación.

5.5.2. Transferencia a archivo

54. Un dictamen de la Comisión Superior Calificadora de Documentos Administrativos (CSCDA) acerca de la transferencia de un conjunto de documentos electrónicos a otro archivo constituiría una segunda causa de eliminación. A diferencia del expediente de eliminación, en este caso los documentos electrónicos no se eliminan, sino que simplemente cambian de ubicación física y de custodia, por lo que una vez realizado el cambio podrían ser borrados en origen. Sin embargo, será necesario proceder al borrado seguro de la información o la destrucción segura de soportes en el centro o archivo que ha procedido a realizar la transferencia, en caso de que afecte a la totalidad de un conjunto de soportes.

5.5.3. Cambio de soporte

55. Un último grupo de causas que motivan la eliminación de documentos electrónicos tienen que ver básicamente con un cambio o sustitución del soporte de almacenamiento, aunque en estos casos siempre se realizará previamente una copia de los datos en los nuevos soportes.

56. Aunque estas causas no se deriven directamente de un proceso de gestión documental, se contemplan en esta Guía con la intención de servir de orientación para un proceso de eliminación de documentos electrónicos por cambio de soporte.

57. Las **razones para realizar este cambio de soporte** pueden ser variadas:

    i. Fallo de los soportes.

    ii. La sustitución completa o parcial de un sistema de almacenamiento por uno nuevo, por fin de vida útil de los soportes, por obsolescencia (de la tecnología, del tamaño de los soportes, del tiempo de acceso, etc.) o por cualquier otra causa.

    iii. Un movimiento de datos entre sistemas de almacenamiento o dentro del mismo sistema que afecte a la totalidad de un conjunto de soportes.

    iv. Cambio de formato de los documentos electrónicos que justifique una sustitución de los soportes.

58. Un cambio de soporte **supondrá** la copia de los datos a nuevos soportes o sistemas de almacenamiento y la aplicación de técnicas de borrado seguro, si se pretende reaprovechar los soportes o, en caso contrario, la destrucción segura de los soportes, independientemente del nivel de protección de la información.

5.6. Nivel de protección de la información

59. Con el objetivo de conocer las posibilidades de acceso a determinada información, es necesario conocer su nivel de protección. Se trata de un ejercicio orientado a modular el equilibrio entre la importancia o sensibilidad de la información que se maneja y de los servicios que se prestan, por un lado, y el esfuerzo de seguridad requerido, en función de los riesgos a los que están expuestos, bajo el criterio del principio de proporcionalidad, por otro lado.

60. Para facilitar la aplicación del principio de proporcionalidad, el ENS contempla, según lo explicado en su Anexo I, la categorización en tres categorías, BÁSICA, MEDIA y ALTA,

en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios a proteger con perjuicio para las dimensiones de seguridad, disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, que a su vez se valoran en tres escalones BAJO, MEDIO y ALTO. Entendiendo que la determinación de la categoría de un sistema no implica que se altere el nivel de las dimensiones de seguridad que no han influido en la determinación de la categoría del mismo; y que a continuación, la selección de las medidas de seguridad apropiadas se habrá de realizar de acuerdo con las dimensiones de seguridad y sus niveles y, para determinadas medidas de seguridad, de acuerdo con la categoría del sistema.

61. Para evaluar la exhaustividad del proceso de eliminación y la posible reutilización o no de los soportes de almacenamiento, **será necesario conocer** el nivel de protección de la información que se pretende eliminar. En este sentido hay dos criterios para determinar este nivel:

    i. Nivel de la dimensión de seguridad confidencialidad (ENS):

        a. bajo

        b. medio

        c. alto

    ii. Datos personales o categorías especiales de datos personales (RGPD):

        d. No aplica

        e. Datos personales

        f. Categorías especiales de datos personales

62. Como indica la Agencia Española de Protección de Datos, en su documento “El impacto del Reglamento General de Protección de Datos sobre la actividad de las Administraciones Públicas”, en el caso de las AA.PP., la aplicación de las medidas de seguridad estará marcada por los criterios establecidos en el Esquema Nacional de Seguridad.

63. Por otra parte, se encuentra la “información clasificada” regulada por Ley 9/1968, de 5 de abril, de Secretos Oficiales y normas de desarrollo, información explícitamente excluida del ámbito de aplicación del ENS.

64. En el ámbito de esta Guía, en cuanto a protección de la información en general y de los documentos en particular se estará, en consecuencia, a los criterios establecidos en el ENS.

5.7. Soportes de almacenamiento

65. Conocer el tipo de soporte de almacenamiento en el que se encuentran los documentos electrónicos, su contexto (ya se trate de sistemas de almacenamiento o dispositivos móviles) y el tipo de gestión, son esenciales para determinar los métodos y técnicas de borrado y destrucción seguros más adecuados:

    i. Tipos de soportes de almacenamiento

        a. Disco duro magnético (HDD).

        b. Cinta magnética.

        c. Soporte óptico.

        d. Memorias de estado sólido (SSD, memorias Flash)

ii. Contexto de los soportes

   a. Sistemas virtualizados de almacenamiento

   b. Dispositivo móvil o almacenamiento local

iii. Tipo de gestión de los soportes

   a. Gestión interna

   b. Gestión externa (SaaS, Storage as a Service o cloud público)

5.7.1. Tipos de soportes de almacenamiento

66. Los soportes más habituales en sistemas de almacenamiento son los discos duros magnéticos (HDD) y las memorias de estado sólido (SSD). Las cintas magnéticas se usan especialmente para copias de seguridad, o para almacenar grandes cantidades de datos con poco acceso. Incluso es posible que, mediante un estándar abierto como la tecnología LTFS (Linear Tape File System), puedan presentarse como un sistema de ficheros y no como un soporte.

    i. Hay que tener presente que cada soporte tiene una vida útil estimada por los fabricantes (en condiciones óptimas de conservación y mantenimiento): número de ciclos máximo de escritura para cada dispositivo SSD, 3-5 años para los HDD, 20-30 años para cintas magnéticas.

    ii. Tanto los HDD como los SSD son de acceso aleatorio. Esto permite que en estos tipos de soportes los bloques de los ficheros marcados como borrados puedan sobrescribirse con nuevos datos.

    iii. Las cintas son dispositivos de acceso secuencial. Los datos nuevos o modificados se añaden al final de la cinta, por lo que los bloques de un fichero marcado como borrado no se sobrescriben.

67. En dispositivos móviles como ordenadores portátiles, teléfonos móviles o *tablets*, el almacenamiento suele consistir en memorias de estado sólido (*flash*). Por otro lado, los soportes de tipo HDD o SSD también pueden emplearse como almacenamiento local en servidores, PC u ordenadores portátiles.

5.7.2. Contexto de los soportes

68. Los sistemas de almacenamiento se denominan sistemas virtualizados porque los soportes no se asocian a recursos de almacenamiento concretos. Esto permite aprovechar toda la capacidad de almacenamiento de que disponen estos sistemas al repartirla entre todos los servicios y usuarios que pueden hacer uso de ella. En este caso no será sencillo, pues, identificar un volumen lógico de almacenamiento (una unidad de un servidor, por ejemplo), con sus correspondientes volúmenes físicos.

69. Así el borrado de todos los datos de un recurso (un disco, un directorio o carpeta, etc.) puede afectar a un número variable de soportes, que a su vez pueden contener parte de otros múltiples recursos.

70. En cualquier caso, si la eliminación de los documentos afecta a la totalidad de un soporte o conjunto de soportes, deberán aplicarse las técnicas o métodos de borrado y destrucción seguros, en función del tipo de soporte implicado.

71. En este tipo de sistemas virtualizados, no obstante, sería posible asignar específicamente un conjunto de soportes a un sistema de información determinado, si la importancia del mismo o la naturaleza de la información justificasen hacerlo. Esto permitiría, si fuese necesario, aplicar a este conjunto de soportes métodos o técnicas de borrado seguros e, incluso, de destrucción segura de soportes.

72. En el caso de dispositivos móviles o de almacenamiento local de servidores, ordenadores portátiles o PC, los recursos de almacenamiento suelen asociarse a soportes concretos, por lo que resultará más sencillo aplicar los métodos o técnicas de borrado seguro.

5.7.3. Tipo de gestión de los soportes

73. El tipo de gestión hace referencia al propietario de los sistemas de almacenamiento y responsable de su administración y mantenimiento.

74. Cuando estos sistemas se hospedan en instalaciones propias, son propiedad del organismo, y éste se encarga directamente de su administración, hablaremos de gestión interna.

75. Cuando el almacenamiento se contrata a un proveedor hablaremos de SaaS (almacenamiento como servicio), también conocido como cloud público. El proveedor en este caso es el propietario de los sistemas de almacenamiento y quien los administra y gestiona. El organismo alquila espacio de almacenamiento y se conecta a él mediante protocolos seguros de red. En este caso la gestión es externa al propio organismo que usa estos servicios.

76. La gestión interna proporciona un mayor control sobre un proceso de eliminación segura, ya que se conocen los tipos de soportes de almacenamiento empleados, el número de copias o réplicas existentes, la ubicación de los soportes, etc., con lo que es posible seleccionar las técnicas y métodos de borrado y destrucción seguros más adecuados y verificar posteriormente su resultado.

77. La excepción en este caso lo constituye la destrucción segura cuando se realiza fuera de las instalaciones del organismo y con maquinaria de terceros. En estos casos la solicitud de certificados de destrucción debería ser un requisito obligatorio.

78. Con la gestión externa de los sistemas de almacenamiento, en cambio, puede darse el caso de desconocer los tipos de soportes empleados, el número de copias de seguridad o réplicas existentes y también la ubicación física de los sistemas de almacenamiento. Incluso las técnicas y métodos de borrado y destrucción seguros empleados pueden ser decisión del proveedor. Todo esto dificulta obviamente la verificación del resultado del proceso de eliminación.

5.8. Técnicas y métodos de borrado y destrucción seguros

79. Las técnicas y métodos de borrado y destrucción segura de soportes que se contemplan en esta guía son las siguientes:

    i. Borrado (borrado de nivel 0): cuando la eliminación no afecte a la totalidad de un soporte o conjunto de soportes, un borrado a nivel de sistema operativo o de aplicación de gestión sería el mínimo recomendado, siempre y cuando se combine con otro tipo de medidas de seguridad como el control de accesos..

ii. Borrado seguro (borrado de nivel 1 y 2)
   a. Sobrescritura
   b. Comandos a nivel de firmware
   c. Borrado criptográfico
   d. Desmagnetización
iii. Destrucción segura de soportes
   a. Trituración
   b. Desintegración
   c. Aplastamiento
   d. Pulverización

5.8.1. Sobrescritura

80. Consiste en escribir un patrón fijo o aleatorio de tipo binario o una combinación de ambos, en todos los sectores o páginas de un soporte de almacenamiento (especialmente discos duros magnéticos). Para ser efectiva esta técnica debe afectar a toda el área del soporte, incluyendo sectores defectuosos y ocultos. Puede ejecutarse en varias etapas consecutivas o ciclos, lo que mejora su resultado.
81. Exige por el contrario mucho tiempo de ejecución, que estará determinado por el número de ciclos de escritura, el patrón de sobrescritura y el tamaño del soporte. Permite además la reutilización del mismo. Según la técnica seleccionada el borrado será más o menos exhaustivo, por lo que su selección debería depender de la categoría de la información almacenada.
82. Algunas técnicas conocidas de sobrescritura son: AFSSI-5020, ISM 6.2.92, HMG Infosec Standard 5, Algoritmo de Bruce Schneier, CSEC ITSG-06, NAVSO P-5239-26, Algoritmo de Peter Gutmann, DoD 5220.22 M, BSI-VSITR y NCSC-TG-025.La mayoría de estas técnicas realizan un número de sobrescrituras de entre 3 y 7.

5.8.2. Comandos a nivel firmware

83. Este tipo de comandos, propios del firmware (que es el software que maneja directamente el hardware de un sistema informático), realizan básicamente una sobrescritura de todos los bits de un soporte. Al estar implementados a bajo nivel, son más rápidos que una sobrescritura realizada mediante una aplicación específica. Afectan a todo el soporte, permitiendo su reutilización posterior.

5.8.3. Borrado criptográfico

84. Algunos soportes de almacenamiento, especialmente dispositivos de estado sólido (SSD), incorporan circuitos especiales que cifran permanentemente su contenido. Estos soportes se denominan dispositivos auto-cifrados (SED, o “SelfEncrypting Drives”). El cifrado emplea un algoritmo criptográfico fuerte, basándose generalmente en el estándar AES (Advanced Encryption Standard), y puede emplear AES-256.

85. Para realizar un borrado seguro de un soporte de este tipo basta emplear un comando de borrado a nivel de firmware o generar una nueva clave de cifrado, lo que convierte en ilegibles todos los datos que contiene el soporte al perder la clave de cifrado original.

5.8.4. Desmagnetización

86. Este método es adecuado para borrar todos los datos de un soporte magnético, como discos duros o cartuchos de cinta. Consiste en exponer los soportes de almacenamiento a un campo magnético suficientemente potente para modificar la polaridad de las partículas magnéticas. Esto hace ilegibles e ininteligibles los datos almacenados e impide su posible recuperación. No funciona con memorias de estado sólido.

87. Después del proceso de desmagnetización, que puede durar sólo unos segundos, los soportes quedan inutilizados, por lo que el siguiente paso debería ser su destrucción o reciclado. Esto permite evitar la verificación del propio proceso de borrado, por otro lado muy difícil en la práctica porque no es posible el acceso a los soportes desmagnetizados.

5.8.5.Trituración

88. Los denominados “shredders” o trituradoras son máquinas que reducen un soporte a pedazos minúsculos de tamaño y forma uniformes. Es un sistema apto para soportes de tipo óptico.

5.8.6.Desintegración

89. La realizan máquinas especiales denominadas desintegradores o “disintegrators”. Se basan en el uso de cuchillas rotatorias. El soporte queda reducido a partículas muy pequeñas (incluso menores a 2 mm). Es un método válido para SSD, cartuchos magnéticos y soportes ópticos.

5.8.7.Aplastamiento

90. Unas máquinas denominadas “crushers” ejercen una fuerza enorme sobre los soportes, doblándolos y perforándolos. Es un método apto para dispositivos HDD, SSD y memorias flash.

5.8.8.Pulverización

91. Unas máquinas especiales, denominadas “destroyers”, que se asemejan a las que actúan por aplastamiento (“crushers”), funcionan machacando los soportes. Es un sistema válido para discos duros magnéticos.

6. PROCESO DE ELIMINACIÓN

92. En este apartado se resumen los aspectos expuestos en el apartado 5 “Eliminación” de modo que faciliten la elección del método más adecuado para eliminar documentos electrónicos. Se han recopilado en forma de tabla:
    i. Tabla 2 “Proceso de eliminación”
    ii. Tabla 3: “Soportes de almacenamiento y métodos y técnicas de borrado y destrucción seguros”
93. La primera (tabla 2) relaciona los motivos que justifican un proceso de eliminación de documentos electrónicos y los factores que condicionan en buena medida su desarrollo con los métodos y técnicas de borrado y destrucción seguros.
94. La segunda (tabla 3) identifica para cada tipo de soporte los métodos y técnicas de borrado y destrucción seguros más adecuados.
95. La tabla 2 contiene, de izquierda a derecha, la siguiente información:
    i. Motivo de la eliminación: Expediente de eliminación / Transferencia a archivo
    ii. Contexto de los soportes: Sistema de almacenamiento
    iii. Tipo de gestión de los soportes: Gestión interna / Gestión externa
    iv. Afecta a la totalidad del soporte: Sí / No
    v. Reaprovechamiento del soportes: Sí / No
    vi. Nivel de protección de la información
    vii. Acción recomendada: Borrado nivel 0 – Borrado seguro nivel 1 – Borrado seguro nivel 2 – Destrucción segura de soportes

Tabla 2. Proceso de eliminación

PROCESO DE ELIMINACIÓN										
MOTIVO DE LA ELIMINACIÓN	CONTEXTO DE LOS SOPORTES	TIPO DE GESTIÓN	AFECTA A LA TOTALIDAD DEL SOPORTE	REAPROVECHAMIENTO DEL SOPORTE	NIVEL DE PROTECCIÓN DE LA INFORMACIÓN	ACCIONES RECOMENDADAS				NOTAS
EJECUCIÓN DE UN DICTAMEN DE ELIMINACIÓN --- TRANSFERENCIA A ARCHIVO --- CAMBIO DE SOPORTE	SISTEMA DE ALMACENAMIENTO	GESTIÓN INTERNA	SÍ	SÍ	APLICA RGPD NIVEL MEDIO / ALTO ENS		BORRADO SEGURO NIVEL 1	BORRADO SEGURO NIVEL 2		(1)
				NO					DESTRUCCIÓN SEGURA DE SOPORTES	
				SÍ	NO APLICA RGPD NIVEL BAJO ENS		BORRADO SEGURO NIVEL 1			
				NO					DESTRUCCIÓN SEGURA DE SOPORTES	
			NO	SÍ	APLICA RGPD NIVEL MEDIO / ALTO ENS	BORRADO NIVEL 0				(2)
					NO APLICA RGPD NIVEL BAJO ENS	BORRADO NIVEL 0				(2)
		GESTIÓN EXTERNA	SÍ	SÍ	APLICA RGPD NIVEL MEDIO / ALTO ENS			BORRADO SEGURO NIVEL 2		(3)
				NO					DESTRUCCIÓN SEGURA DE SOPORTES	
				SÍ	NO APLICA RGPD NIVEL BAJO ENS		BORRADO SEGURO NIVEL 1	BORRADO SEGURO NIVEL 2		(4)
				NO					DESTRUCCIÓN SEGURA DE SOPORTES	
			NO	SÍ	APLICA RGPD NIVEL MEDIO / ALTO ENS	BORRADO NIVEL 0				(5)
					NO APLICA RGPD NIVEL BAJO ENS	BORRADO NIVEL 0				(5)

96. Notas tabla 2:

    1. Según el nivel de protección de la información podría aplicarse un borrado seguro de nivel 1 o 2.
    2. El borrado de nivel 0 debería combinarse con un control de accesos.
    3. Al ser externa la gestión de los soportes de almacenamiento, lo recomendable sería aplicar un borrado seguro de nivel 2.
    4. Aunque el nivel de protección de la información sea básico, la gestión externa de los soportes haría recomendable escoger entre un borrado seguro de nivel 1 o 2.
    5. El borrado de nivel 0 debería combinarse con un control de accesos y, al tratarse de una gestión externa de los soportes, sería recomendable asimismo añadir alguna otra medida de seguridad, como por ejemplo el cifrado de la información.

97. La tabla 3 detalla los cuatro niveles de borrado y destrucción y los métodos y técnicas asociados a cada uno de ellos, y los tipos de soportes, indicando su compatibilidad:

    i. Borrado de nivel 0 (indicando otras medidas de seguridad como control de accesos o cifrado)
    ii. Borrado seguro de nivel 1
        a. Sobrescritura (de 3 pasadas)
    iii. Borrado de nivel 2
        a. Sobrescritura (de 4 o más pasadas, aunque lo habitual serían 7)
        b. Comandos a nivel de firmware
        c. Borrado criptográfico
        d. Desmagnetización
    iv. Destrucción segura de soportes
        a. Trituración
        b. Desintegración
        c. Aplastamiento
        d. Pulverización
    v. Soportes
        a. HDD
        b. Cinta magnética
        c. Disco óptico WORM
        d. Disco óptico regrabable
        e. SSD

Tabla 3. Soportes de almacenamiento y métodos y técnicas de borrado y destrucción

SOPORTES DE ALMACENAMIENTO Y MÉTODOS Y TÉCNICAS DE BORRADO Y DESTRUCCIÓN

		SOPORTES DE ALMACENAMIENTO				
		HDD	CINTA MAGNÉTICA	DISCO ÓPTICO WORM	DISCO ÓPTICO REGRABABLE	SSD
ELIMINACIÓN	BORRADO (NIVEL 0) + CONTROL DE ACCESOS (+ cifrado)					
	BORRADO (NIVEL 0)	X	X		X	X
	BORRADO SEGURO - NIVEL 1					
	SOBREESCRITURA (=3)	X				X
	BORRADO SEGURO - NIVEL 2					
	SOBREESCRITURA (=>4)	X				X
	COMANDO A NIVEL DE FIRMWARE	X				X
	BORRADO CRIPTOGRÁFICO	X				X
	DESMAGNETIZACIÓN	X	X			
	DESTRUCCIÓN SEGURA DE SOPORTES					
	TRITURACIÓN			X	X	
	DESINTEGRACIÓN		X			X
	APLASTAMIENTO	X				X
	PULVERIZACIÓN	X				

Se indican con una cruz los métodos y técnicas compatibles con cada tipo de soporte

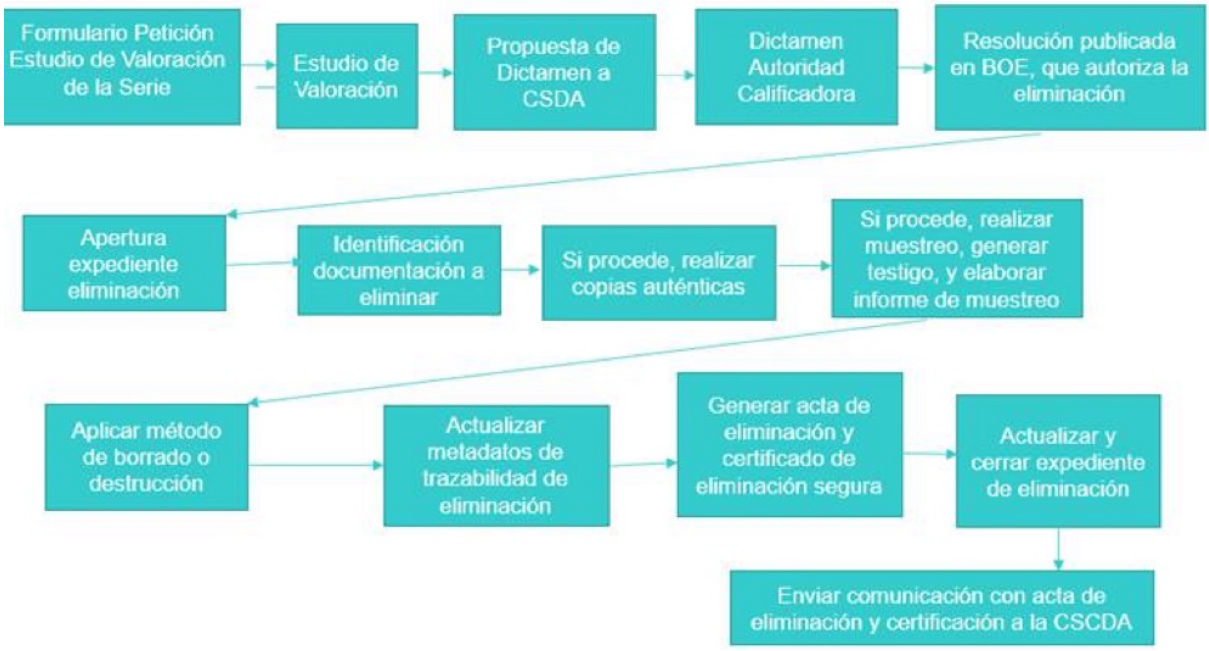
SOPORTES DE ALMACENAMIENTO Y MÉTODOS Y TÉCNICAS DE BORRADO Y DESTRUCCIÓN

ELIMINACIÓN	SOPORTES DE ALMACENAMIENTO				
	HDD	CINTA MAGNÉTICA	DISCO ÓPTICO WORM	DISCO ÓPTICO REGRABABLE	SSD
BORRADO (NIVEL 0) + CONTROL DE ACCESOS (+ cifrado)					
BORRADO (NIVEL 0)	X	X		X	X
BORRADO SEGURO - NIVEL 1					
SOBREESCRITURA (=3)	X				X
BORRADO SEGURO - NIVEL 2					
SOBREESCRITURA (=>4)	X				X
COMANDO A NIVEL DE FIRMWARE	X				X
BORRADO CRIPTOGRÁFICO	X				X
DESMAGNETIZACIÓN	X	X			
DESTRUCCIÓN SEGURA DE SOPORTES					
TRITURACIÓN			X	X	
DESINTEGRACIÓN		X			X
APLASTAMIENTO	X				X
PULVERIZACIÓN	X				

Se indican con una cruz los métodos y técnicas compatibles con cada tipo de soporte

7. ETAPAS DEL PROCESO DE ELIMINACIÓN DE DOCUMENTOS ELECTRÓNICOS

98. La Política de Gestión de Documentos Electrónicos define los elementos fundamentales de un proceso de eliminación de documentos electrónicos, los cuales se detallan en el siguiente diagrama ilustrativo en el caso de ejecución de un dictamen de eliminación.



8. DEFINICIONES Y ACRÓNIMOS

8.1. Definiciones

Calificación: Proceso de gestión de documentos que tiene por finalidad, en base a un análisis de valores de los documentos, establecer los plazos de permanencia de los documentos en el sistema de gestión, de transferencia y eliminación en su caso, así como los plazos de acceso y la eventual calificación como documento esencial de una organización.

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

Dictamen: En el ámbito del proceso de calificación, decisión de la autoridad calificadora que establece, en base al proceso previo de valoración, los plazos de permanencia de los documentos en el sistema de gestión, las transferencias, el acceso y la eliminación o, en su caso, conservación permanente.

Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Organización: Cualquier órgano de la Administración pública o Entidad de Derecho Público vinculada o dependiente de aquélla.

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

Valoración: Proceso de gestión de documentos que tiene como finalidad juzgar los valores de los documentos, estableciendo plazos de conservación y determinando su accesibilidad, decisión sobre su destino al final de su ciclo de vida y eventual calificación como documento esencial de una organización.

8.2. Acrónimos

AGE: Administración General del Estado

CSCDA: Comisión Superior Calificadora de Documentos Administrativos

ENI: Esquema Nacional de Interoperabilidad

ENS: Esquema Nacional de Seguridad

HDD: Hard Disk Drive, disco duro

LTFS: Linear Tape File System

NTI: Norma Técnica de Interoperabilidad

RGPD: Reglamento General de Protección de Datos

SaaS: Storage as a Service o cloud

SSD: Solid State Drive, dispositivo de estado sólido

WORM: Write Once Read Many

9. REFERENCIAS

9.1. Legislación

i. Ley 9/1968, de 5 de abril, sobre secretos oficiales.

BOE-A-1968-444

ii. Ley 16/1985, de 25 de junio, de Patrimonio Histórico Español.

BOE-A-1985-12534

iii. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

BOE-A-2015-10565

iv. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

DOUE-L-00001-00088

v. Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original.

BOE-A-2002-22192

vi. Real Decreto 1401/2007, de 29 de octubre, por el que se regula la composición, funcionamiento y competencias de la Comisión Superior Calificadora de Documentos Administrativos.

BOE-A-2007-19248

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

BOE-A-2010-1330

viii. Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

BOE-A-2010-1331

ix. Resolución de 28 de junio de 2012, 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.

BOE-A-2012-10048

9.2. Otros

x. Política de gestión de documentos electrónicos del MINHAP (2ª edición)

PGD-e MINHAP 2016

xi. Guía de Aplicación de la Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos (2ª edición)

Guia_NTI_Politica_Gestion_DocElect_PDF_2ed_2016

99. El artículo 17 de la Ley 39/2015, Archivo de documentos, además de tratar el archivo electrónico de expedientes finalizados menciona que la eliminación de los documentos electrónicos deberá ser autorizada:

> **Artículo 17. Archivo de documentos**
>
> 1. Cada Administración deberá mantener un archivo electrónico único de los documentos electrónicos que correspondan a procedimientos finalizados, en los términos establecidos en la normativa reguladora aplicable.
>
> 2. Los documentos electrónicos deberán conservarse en un formato que permita garantizar la autenticidad, integridad y conservación del documento, así como su consulta con independencia del tiempo transcurrido desde su emisión. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones. La eliminación de dichos documentos deberá ser autorizada de acuerdo a lo dispuesto en la normativa aplicable.
>
> 3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.

100. El artículo 13 de la Ley 39/2015, Derechos de las personas en sus relaciones con las Administraciones Públicas, establece asimismo la obligación de la Administración de proteger los datos de carácter personal de los ciudadanos que figuren en sus archivos:

> **Artículo 13. Derechos de las personas en sus relaciones con las Administraciones Públicas.**
>
> Quienes de conformidad con el artículo 3, tienen capacidad de obrar ante las Administraciones Públicas, son titulares, en sus relaciones con ellas, de los siguientes derechos:
>
> a) A comunicarse con las Administraciones Públicas a través de un Punto de Acceso General electrónico de la Administración.
>
> b) A ser asistidos en el uso de medios electrónicos en sus relaciones con las Administraciones Públicas.
>
> c) A utilizar las lenguas oficiales en el territorio de su Comunidad Autónoma, de acuerdo con lo previsto en esta Ley y en el resto del ordenamiento jurídico.
>
> d) Al acceso a la información pública, archivos y registros, de acuerdo con lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y el resto del Ordenamiento Jurídico.
>
> e) A ser tratados con respeto y deferencia por las autoridades y empleados públicos, que habrán de facilitarles el ejercicio de sus derechos y el cumplimiento de sus obligaciones.
>
> f) A exigir las responsabilidades de las Administraciones Públicas y autoridades, cuando así corresponda legalmente.
>
> g) A la obtención y utilización de los medios de identificación y firma electrónica contemplados en esta Ley.

h) A la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

i) Cualesquiera otros que les reconozcan la Constitución y las leyes.

Estos derechos se entienden sin perjuicio de los reconocidos en el artículo 53 referidos a los interesados en el procedimiento administrativo.

101. El artículo 49 de la Ley 16/1985, de Patrimonio Histórico Español, establece que forman parte del Patrimonio Documental los documentos "generados, conservados o reunidos en el ejercicio de su función por cualquier organismo o entidad de carácter público":

Artículo 49

1. Se entiende por documento, a los efectos de la presente Ley, La exclusión o eliminación de bienes del Patrimonio Documental y Bibliográfico contemplados en el artículo 49.2 y de los demás de titularidad pública deberá ser autorizada por la Administración competente. 1. Se entiende por documento, a los efectos de la presente Ley, toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos. Se excluyen los ejemplares no originales de ediciones.

2. Forman parte del Patrimonio Documental los documentos de cualquier época generados, conservados o reunidos en el ejercicio de su función por cualquier organismo o entidad de carácter público, por las personas jurídicas en cuyo capital participe mayoritariamente el Estado u otras entidades públicas y por las personas privadas, físicas o jurídicas, gestoras de servicios públicos en lo relacionado con la gestión de dichos servicios.

3. Forman igualmente parte del Patrimonio Documental los documentos con una antigüedad superior a los cuarenta años generados, conservados o reunidos en el ejercicio de sus actividades por las entidades y asociaciones de carácter político, sindical o religioso y por las entidades, fundaciones y asociaciones culturales y educativas de carácter privado.

4. Integran asimismo el Patrimonio Documental los documentos con una antigüedad superior a los cien años generados, conservados o reunidos por cualesquiera otras entidades particulares o personas físicas.

5. La Administración del Estado podrá declarar constitutivos del Patrimonio Documental aquellos documentos que, sin alcanzar la antigüedad indicada en los apartados anteriores, merezcan dicha consideración.

102. El artículo 55 de la Ley 16/1985 determina por otro lado que los documentos que forman parte del Patrimonio Documental no podrán destruirse "en tanto subsista su valor probatorio de derechos y obligaciones de las personas o los entes públicos":

Artículo 55

1. La exclusión o eliminación de bienes del Patrimonio Documental y Bibliográfico contemplados en el artículo 49.2 y de los demás de titularidad pública deberá ser autorizada por la Administración competente.

2. 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.

3. En los demás casos la exclusión o eliminación deberá ser autorizada por la Administración competente a propuesta de sus propietarios o poseedores, mediante el procedimiento que se establecerá por vía reglamentaria.

103. El artículo 58 de la misma ley señala que “el estudio y dictamen de las cuestiones relativas a la calificación y utilización de los documentos de la Administración del Estado” corresponderá a una Comisión Superior Calificadora de Documentos Administrativos:

> **Artículo 58**
>
> El estudio y dictamen de las cuestiones relativas a la calificación y utilización de los documentos de la Administración del Estado y del sector público estatal, así como su integración en los Archivos y el régimen de acceso e inutilidad administrativa de tales documentos, corresponderá a una Comisión Superior Calificadora de Documentos Administrativos, cuya composición, funcionamiento y competencias específicas se establecerán por vía reglamentaria. Asimismo podrán constituirse Comisiones Calificadoras en los Organismos públicos que así se determine.

104. El Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original, define el procedimiento de eliminación de documentos:

> **Artículo 1. Objeto y ámbito de aplicación**
>
> 1. Con objeto de garantizar una adecuada protección del patrimonio documental de la Administración General del Estado y los Organismos públicos vinculados o dependientes de ella, la eliminación de los documentos administrativos y de series de los mismos, así como su conservación en soporte diferente al de su producción original, se regirá por lo dispuesto en este Real Decreto.
>
> 2. El presente Real Decreto es de aplicación a los documentos y series documentales producidos, conservados o reunidos por la Administración General del Estado y los Organismos públicos vinculados o dependientes de ella, cualquiera que sea su soporte.
>
> **Artículo 2. Régimen de la eliminación de documentos y, en su caso, de la conservación de los mismos en soporte distinto al original**
>
> 1. A los efectos de este Real Decreto se entiende por eliminación de documentos la destrucción física de unidades o series documentales por el órgano responsable del archivo u oficina pública en que se encuentren, empleando cualquier método que garantice la imposibilidad de reconstrucción de los mismos y su posterior utilización. La eliminación de documentos sólo podrá llevarse a cabo, tras el correspondiente proceso de valoración documental, según se establece en los artículos siguientes.
>
> 2. Se entiende por valoración documental el estudio y análisis de las características históricas, administrativas, jurídicas, fiscales e informativas de la documentación.
>
> El proceso de valoración establecerá los plazos de transferencia, la posible eliminación o expurgo y el régimen de accesibilidad de la documentación.
>
> (…)
>
> **Artículo 3. Documentos con valor probatorio**
>
> En ningún caso se podrá autorizar la eliminación ni se podrá proceder a la destrucción de documentos de la Administración General del Estado o de sus Organismos públicos en tanto subsista su valor probatorio de derechos y obligaciones de las personas físicas o jurídicas o no hayan transcurrido los plazos que la legislación vigente establezca para su conservación.

Artículo 4. Iniciación del procedimiento

1. A iniciativa propia o de los órganos responsables de los documentos o series documentales concernidos, la Comisión Calificadora de Documentos Administrativos de cada Departamento u Organismo público podrá acordar la iniciación de un procedimiento de eliminación de documentos y, en su caso, de conservación del contenido de los mismos en soporte distinto del original en que fueron producidos.

2. En el Acuerdo de iniciación deberá quedar establecido fundadamente que los documentos originales a que se refiere no poseen valor histórico ni utilidad para la gestión administrativa que exija su conservación.

Asimismo, se expresará en él que los documentos carecen de valor probatorio para los derechos y obligaciones de las personas físicas o jurídicas.

3. En el caso de que se plantee la conservación del contenido de los documentos en soporte distinto al original, deberán observarse los requisitos establecidos en el artículo 2.3 de este Real Decreto, y lo que se dispone en las restantes normas del mismo en cuanto sean aplicables a este supuesto.

4. El acuerdo deberá ir acompañado de la siguiente documentación:

a) Informe del órgano proponente que justifique la necesidad de la eliminación y, en su caso, de la conservación en soporte distinto, acreditando en el mismo la valoración documental efectuada en los términos del artículo 2.2. En este análisis se incluirá la mención de las disposiciones que en su caso hayan regulado hasta el momento de la propuesta el expurgo o la custodia de dicha documentación. Asimismo, deberá concretarse en este análisis si incluye datos referentes a la intimidad de las personas, si contiene datos sanitarios personales, si afecta o afectará a la defensa nacional o la seguridad del Estado y otras características que se consideren especialmente significativas.

b) Memoria relativa a la documentación de que se trate, y que comprenderá básicamente el estudio histórico institucional, cuadro de clasificación en caso de series documentales, órgano productor, signaturas extremas, tipo documental, resumen del contenido, fechas extremas, legislación relativa al origen y desarrollo de la documentación, tipo de muestreo que se propone, en su caso, y archivo u oficina pública en que se encuentra depositada.

5. El acuerdo de iniciación del procedimiento, junto con los documentos antes citados, se remitirá al Presidente de la Comisión Superior Calificadora de Documentos Administrativos, y contendrá la propuesta de eliminación o en su caso de conservación en soporte distinto, de documentos o series documentales determinados, así como la petición del dictamen al que se refiere el artículo 5. Si la citada Comisión considerase precisa más información, la requerirá de la Comisión del Departamento u organismo que hubiese iniciado el procedimiento o, en su caso, de los Departamentos u organismos que estime afectados, que deberán remitirla en plazo no superior a tres meses.

6. Cuando el contenido del documento o documentos a eliminar tenga relación con las competencias atribuidas a otro Departamento u Organismo público, deberá contarse con el informe preceptivo del mismo.

Artículo 5. Dictamen de la Comisión Superior Calificadora de Documentos Administrativos.

1. Sobre el Acuerdo establecido conforme a lo dispuesto en el artículo anterior, emitirá dictamen preceptivo la Comisión Superior Calificadora de Documentos Administrativos regulada por el Real Decreto 139/2000, de 4 de febrero, en el plazo máximo de un año a contar desde que disponga de la documentación completa de que se trate. En el caso de que el órgano proponente solicite por razones de urgencia un plazo inferior al citado, la Comisión Superior Calificadora podrá acordarlo así, notificándolo al órgano proponente.

2. Si el dictamen de la Comisión fuese contrario a la propuesta de eliminación, tendrá carácter vinculante, sin perjuicio de lo que se establece en el apartado siguiente de este artículo.

3. Dictaminada desfavorablemente una propuesta de eliminación, no podrá presentarse otra nueva relativa a la misma documentación hasta que transcurran dos años desde la comunicación de dicho dictamen al órgano proponente. No obstante, si se modificasen los criterios archivísticos aplicados en la primera valoración, la Dirección General del Libro, Archivos y Bibliotecas podrá dirigirse al órgano responsable de la documentación para que, si lo considera pertinente, presente una nueva propuesta, sin necesidad de que transcurra el plazo indicado.

Artículo 6. Resolución administrativa.

1. Si el dictamen fuese favorable a la propuesta, el Subsecretario del Departamento ministerial o el Presidente o Director del Organismo público en el que se encuentren custodiados los documentos adoptará la resolución que considere oportuna. Si la resolución autorizase la eliminación, se dará traslado de ella al órgano que adoptó la iniciativa y deberá publicarse en el «Boletín Oficial del Estado». Igualmente se procederá cuando la resolución disponga la conservación de los documentos en soporte distinto del original en que fueron producidos.

2. La resolución motivada que autorice la eliminación de documentos y, en su caso, disponga la conservación en soporte distinto del original, deberá incluir:

a) Una descripción sumaria de la documentación afectada, con expresión de signaturas, órgano u órganos productores, resumen de contenido, fechas extremas, tipo de muestreo que se realizará en su caso y archivo u oficina pública en que se encuentre depositada.

b) La indicación de que, conforme a lo previsto en el artículo 57.2 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en el presente Real Decreto, la eficacia de la autorización quedará demorada hasta transcurridos tres meses desde su publicación en el «Boletín Oficial del Estado» y condicionada en todo caso a que durante ese plazo no haya constancia de la interposición de recurso de cualquier naturaleza contra la misma. También se hará constar que no podrá procederse a la destrucción de documentos hasta que la resolución, caso de ser impugnada, adquiera firmeza.

c) El señalamiento de los recursos que procedan.

d) La determinación de las medidas precisas para la destrucción de los documentos y, en su caso, para la conservación de su contenido en soporte distinto al original.

Artículo 7. Eliminación de documentos.

1. El órgano responsable de la custodia de la documentación, una vez sea ejecutiva la autorización obtenida, abrirá un expediente de eliminación de los documentos o series documentales de que se trate, el cual comprenderá:

a) La memoria realizada sobre la documentación y cualquier otra información o documentos presentados con la propuesta de eliminación, así como el texto de esta última.

b) El dictamen de la Comisión Superior Calificadora de Documentos Administrativos y el de cualquier otra Comisión que se haya pronunciado previamente.

c) La memoria del muestreo de la documentación a expurgar.

d) La resolución que haya autorizado la eliminación, así como cualquier otro documento administrativo o judicial relacionado con la misma.

e) El acta de eliminación, en la que el órgano responsable de los documentos acreditará que, habiendo transcurrido el plazo de tres meses establecido en el apartado 2, párrafo b), del artículo 6 de este Real Decreto, no tiene constancia de la interposición de recursos de ninguna naturaleza contra la resolución adoptada, o que ésta ha adquirido firmeza, con los demás extremos relativos a la destrucción que se lleva a cabo, fecha de la misma e identificación de los funcionarios y cualquier otro personal que intervenga en ella. En dicha acta se hará constar lugar, fecha y duración de las operaciones de eliminación con o sin sustitución, procedimiento utilizado, personas intervinientes y funcionario fedatario de la operación y del acta.

2. Si se hubiese dispuesto la conservación del contenido de los documentos o series documentales en soporte distinto al original, antes de proceder a la eliminación de dicho original deberán obtenerse copias auténticas en soporte diferente, con los requisitos establecidos en el artículo 46 de la Ley 30/1992, de 26 de diciembre y, en su caso, en el artículo 45 de dicha Ley y en el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas en la Administración General del Estado.

En este mismo supuesto deberá finalmente levantarse un acta complementaria de la reseñada en el párrafo e) del apartado 1 de este mismo artículo, comprensiva de las actuaciones que se sigan para hacer efectiva la conservación del contenido de los documentos en soporte distinto al original. En el acta se hará constar las características técnicas del nuevo soporte de acuerdo con el citado Real Decreto 263/1996, de 16 de febrero.

3. Un duplicado del acta y, en su caso, del acta complementaria se remitirá a la Comisión Superior Calificadora de Documentos Administrativos en el plazo de los diez días siguientes a la fecha de las actuaciones correspondientes.

Artículo 8. Documentos del expediente de eliminación.

El procedimiento de eliminación se documentará en expediente único por el órgano responsable de la custodia de la documentación y en él deben figurar los documentos siguientes, además de los relacionados en el artículo 7 y sin perjuicio de incluir todos aquellos que se hayan generado en la tramitación:

1. Iniciativa para poner en marcha el procedimiento.
2. Informe del órgano proponente.
3. Memoria de la documentación.
4. Acuerdo de iniciación de la Comisión Calificadora Departamental de Documentos Administrativos.
5. Informe preceptivo de la Comisión Superior Calificadora de Documentos Administrativos.
6. Resolución.
7. Notificaciones, en su caso.
8. Publicaciones de la Resolución.
9. Recursos, si se han interpuesto.
10. Resoluciones de los recursos presentados.
11. Acta de eliminación, con o sin sustitución, si procede.

105. El Real Decreto 1401/2007, de 29 de octubre, por el que se regula la composición, funcionamiento y competencias de la Comisión Superior Calificadora de Documentos Administrativos, define su finalidad y funciones:

Artículo 1. Finalidad, funciones y adscripción.

1. La Comisión Superior Calificadora de Documentos Administrativos tiene como finalidad el estudio y dictamen sobre las cuestiones relativas a la calificación y utilización de los documentos de la Administración General del Estado y de los organismos públicos vinculados o dependientes de ella, así como su integración en los archivos y el régimen de acceso e inutilidad administrativa de tales documentos. En concreto, le corresponde el estudio y dictamen sobre las siguientes cuestiones:

a) Los plazos de permanencia de los documentos administrativos en cada uno de los diferentes tipos de archivos de oficina o gestión, central, intermedio e histórico.

b) Las transferencias, una vez cumplidos los plazos de permanencia, entre cada uno de los tipos de archivos.

c) La accesibilidad y utilización de los documentos y series documentales.

d) Las propuestas de eliminación de documentos o series documentales y, en su caso, de conservación de su contenido en soporte distinto al original en que fueron producidos, de acuerdo con los requisitos establecidos reglamentariamente.

e) La correcta aplicación de los dictámenes emitidos por la propia Comisión en relación con los plazos de permanencia de los documentos en cada uno de los diferentes tipos de archivos, las transferencias, el acceso, la inutilidad administrativa y la eliminación o, en su caso, conservación en soporte distinto al original en que fueron producidos, de los documentos.

f) Cualquier otro asunto sobre materia archivística relacionado con las competencias anteriores, que le sea sometido por su Presidente.

106. El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, incluye una medida de protección específica (borrado y destrucción mp.si.5) relativa a los soportes de información: “borrado seguro” para aquellos que se puedan reutilizar y “destrucción de forma segura” cuando las características de un soporte de información impidan su borrado seguro o cuando el tipo de información que contengan así lo requiera.

5.5.5 Borrado y destrucción [mp.si.5].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	+	=

La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

Nivel BAJO

a) Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su contenido.

Nivel MEDIO

b) Se destruirán de forma segura los soportes, en los siguientes casos:

1. Cuando la naturaleza del soporte no permita un borrado seguro.

2. Cuando así lo requiera el procedimiento asociado al tipo de información con tenida.

c) Se emplearán productos certificados conforme a lo establecido en ([op. pl.5]).

107. El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el marco de la Administración Electrónica, contempla la destrucción reglamentaria como la fase final del ciclo de vida de los documentos electrónicos que no han sido seleccionados para su conservación permanente, señalando que "si el resultado del procedimiento de evaluación documental así lo establece, borrado de la información, o en su caso, destrucción física de los soportes, de acuerdo con la legislación que resulte de aplicación, dejando registro de su eliminación."

> **Artículo 21. Condiciones para la recuperación y conservación de documentos.**
>
> 1. Las Administraciones públicas adoptarán las medidas organizativas y técnicas necesarias con el fin de garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida. Tales medidas incluirán:
>
> a) La definición de una política de gestión de documentos en cuanto al tratamiento, de acuerdo con las normas y procedimientos específicos que se hayan de utilizar en la formación y gestión de los documentos y expedientes.
>
> (…)
>
> k) Si el resultado del procedimiento de evaluación documental así lo establece, borrado de la información, o en su caso, destrucción física de los soportes, de acuerdo con la legislación que resulte de aplicación, dejando registro de su eliminación.

108. También el Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso, en su artículo 20, señala la necesidad de que el "borrado de la información" o "la destrucción física de los soportes" sean consecuencia de un "procedimiento regulado".

> **Artículo 20. Condiciones para la recuperación y conservación del documento electrónico.**
>
> 1. (…).
>
> 2. Los Departamentos Ministeriales y las entidades de derecho público vinculadas o dependientes de los mismos, adoptarán las decisiones organizativas y las medidas técnicas necesarias con el fin de garantizar la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida. Entre éstas: (…)
>
> h) El **borrado de la información**, en su caso, o si procede la destrucción física de los soportes, de acuerdo con un procedimiento regulado y dejando registro de su eliminación (…).

109. La NTI de Política de Gestión Documental, aprobada por resolución de 28 de junio de 2012 de la Secretaría de Estado de Administraciones Públicas, incluye entre los procesos de gestión de documentos electrónicos, la calificación de los documentos, la transferencia y la destrucción o eliminación:

> **VI. Procesos de gestión de documentos electrónicos**
>
> Los procesos de gestión de documentos electrónicos de una organización incluirán, al menos, los siguientes:
>
> (…)

6. Calificación de los documentos, que incluirá:

   i. Determinación de los documentos esenciales.

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

   iii. Dictamen de la autoridad calificadora.

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

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

9. Destrucción o eliminación de los documentos, que atenderá a la normativa aplicable en materia de eliminación de Patrimonio Documental y contemplará la aplicación de las medidas de seguridad relacionadas definidas en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica: Borrado y destrucción del capítulo de «Protección de los soportes de información [mp.si]» y Limpieza de documentos del capítulo de «Protección de la información [mp.info]».

110. La Guía de Aplicación de la NTI de Política de Gestión de Documentos Electrónicos, considera que “el proceso de eliminación de documentos electrónicos constituye un proceso clave en la gestión de documentos y tiene como objetivo impedir su restauración y posterior reutilización. Para ello, es necesario aplicar un proceso que incluya tanto el borrado de la información (el propio documento y sus metadatos) como la destrucción física del soporte, en función de las características del formato y las del propio soporte”.

7.9 Destrucción o eliminación de documentos

91. El proceso de eliminación de documentos constituye un proceso clave en la gestión de documentos y tiene como objetivo impedir su restauración y posterior reutilización. Para ello, es necesario aplicar un proceso que incluya tanto el borrado de la información (el propio documento y sus metadatos) como la destrucción física del soporte, en función de las características del formato y las del propio soporte.

92. De forma general, para la selección de los documentos que serán sometidos a un proceso de eliminación es preciso tener en cuenta los siguientes aspectos:

   i. Siempre se ejecuta con autorización expresa de la entidad u organización competente en cuanto a la calificación de los documentos.

   ii. No se eliminan los documentos mientras subsista su valor probatorio de derechos y obligaciones de las personas físicas o jurídicas o cuando no hayan transcurrido los plazos que la legislación vigente establezca para su conservación.

   iii. No se eliminan documentos calificados como de valor histórico o de investigación.

   iv. Se preserva la confidencialidad de cualquier información que contengan los documentos durante todo el proceso de eliminación.

   v. Todas las copias de documentos cuya destrucción esté autorizada (incluidas las copias de seguridad) son eliminadas.

93. Cada organización diseñará su proceso de eliminación de acuerdo con la legislación específica que resulte de aplicación. El proceso a seguir, así como las circunstancias de la ejecución concreta cada vez que se lleve a efecto, será documentado conforme a lo establecido en el apartado VII de la NTI.

94. En cualquier caso, se tendrán en cuenta las medidas de seguridad del ENS relacionadas tal y como indica el apartado.

EQUIPO RESPONSABLE DE LA ELABORACIÓN DE LA POLÍTICA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS (Plan de Acción de Transformación Digital)	
COORDINADOR	
Gerardo Bustos Pretel	Secretaría General Técnica (MINHAC)
EQUIPO DE REDACCIÓN	
José Luis García Martínez	Secretaría General Técnica (MINHAC)
Diego Castro Campano	Secretaría General Técnica (MINHAC)
EQUIPO DE REVISIÓN TÉCNICA	
Miguel Ángel Amutio Gómez	Secretaría General de Administración Digital (MPTyFP)
Laura Flores Iglesias	Secretaría General de Administración Digital (MPTyFP)
EQUIPO DE REVISIÓN JURÍDICA	
Heide Elena Nicolás Martínez	Abogacía del Estado (MPTyFP)
Federico Pastor Ruiz	Abogacía del Estado (MINHAC)
PARTICIPACIÓN EN EL GRUPO DE TRABAJO	
Josefina Otheo de Tejada Barasoain	AEAT
Julián Antonio Prior Cabanillas	Dirección General de Gobernanza Pública
Andoni Pérez de Lema Sáenz de Viguera	IGAE
Alejandro Millaruelo Gómez	IGAE
Sonia María Cascales Sedano	Dirección General del Catastro
Mayte González Sousa	Secretaría General de Administración Digital
Laura Cristina Méndez Medina	Secretaría General de Administración Digital
María del Carmen Barroso González	Dirección General de Función Pública
Juan Antonio Zapardiel López	Inspección General
Carlos Álvarez Martín	INAP
Álvaro Reig González	INAP
Beatriz Bernáldez Méndez	Parque Móvil del Estado
Rosa María Martín Rey	Secretaría General Técnica
María Teresa Villaizán Montoya	Delegación de Economía y Hacienda de Castilla y León
José Luis Esteban Herreros	MUFACE
Celso Rodrigo de Parada Alonso	MUFACE
Ángel Redondo García	Dirección General de Ordenación del Juego
Julio Perales Díaz	Dirección General de Ordenación del Juego
Francisco Javier Garrido Gómez	FNMT
Jesús Pardo Ballenato	FNMT
Víctor Casado Izquierdo	TEAC
Javier Guerra Casanova	SGTIC
Santiago Vélez Fraga	SGTIC
Elsa Pla Colvin	Secretaría General Técnica (MPTyFP)
José Ignacio Gómez Raya	IGAE