



G05/D03/O

# Directrices – Eliminación de documentos

Modelo de Gestión de Documentos y  
Administración de Archivos (MGD) para  
la Red de Transparencia y Acceso a la  
Información (RTA)

**Versión: 1.0**

**Fecha: diciembre de 2014**

---

### **Coordinadores**

Beatriz Franco Espiño  
Ricard Pérez Alcázar

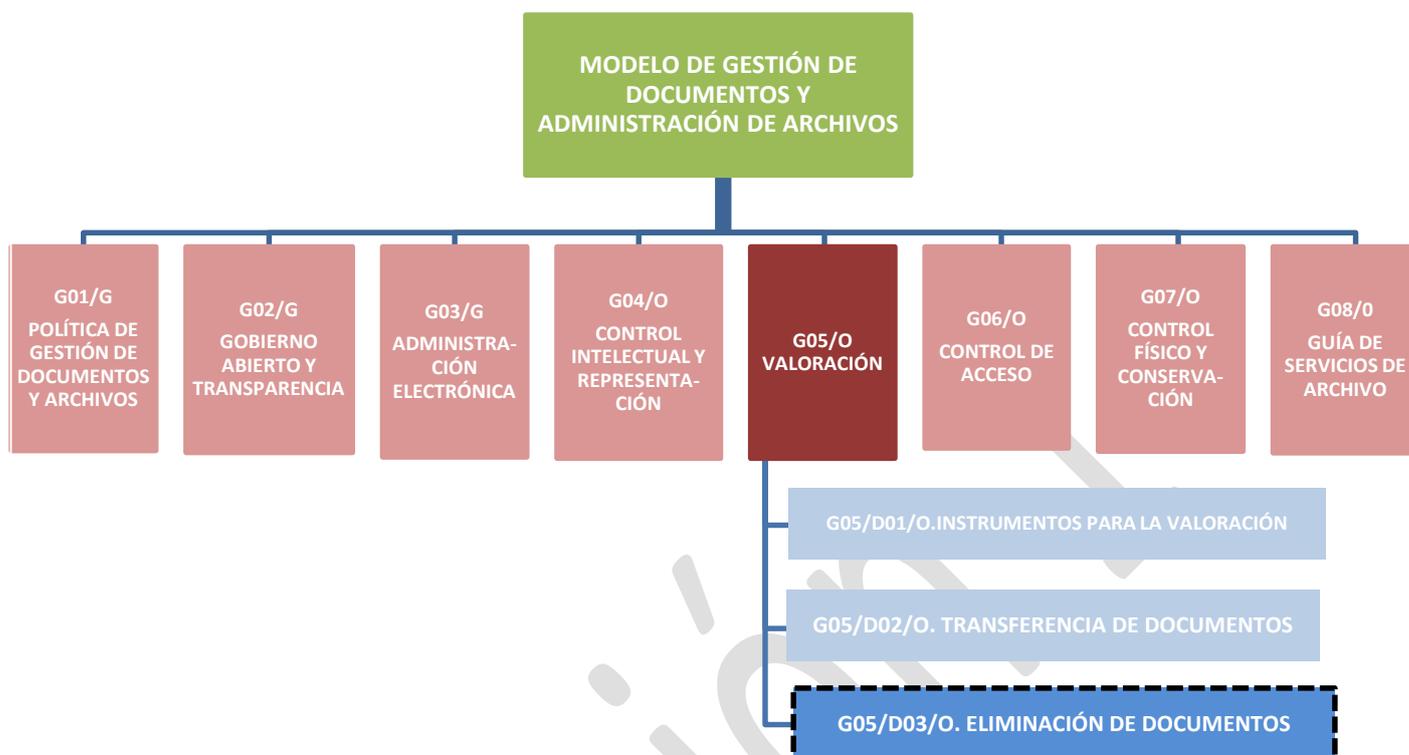
### **Equipo**

Blanca Desantes Fernández  
Francisco Fernández Cuesta  
Javier Requejo Zalama

© De los textos: sus autores

Este documento se encuentra en fase borrador. Ni la RTA ni los autores se hacen responsables de un mal uso de esta información

Estas Directrices se integran en el MGD según se especifica en el siguiente Diagrama de relaciones:





1. Presentación y objetivos
  - 1.1. Finalidad
  - 1.2. Alcance y contenido
  - 1.3. Documentos relacionados
2. Principios de la eliminación
  - 2.1. Autorizada / Legal
  - 2.2. Apropiaada e irreversible
  - 2.3. Segura / confidencial
  - 2.4. En tiempo
  - 2.5. Documentada
3. Métodos de destrucción
  - 3.1. Documentación en papel
  - 3.2. Documentación electrónica
4. Contratación externa
5. Cuadro de compromisos de cumplimiento
6. Términos y referencias
  - 6.1. Glosario
  - 6.2. Referencias
  - 6.3. Bibliografía

## 1. Presentación y objetivos

### 1.1. Finalidad

La finalidad de estas Directrices es proporcionar recomendaciones técnicas para la eliminación reglada de documentos, una vez hayan sido valorados y se haya dictaminado su destrucción, en el marco del Modelo de Gestión de Documentos y administración de archivos de la Red de Transparencia y Acceso a la información (RTA).

### 1.2. Alcance y contenido



La eliminación de unidades y series documentales tiene que realizarse en el marco del procedimiento archivístico que identifica aquellos documentos que se van a destruir conforme a los plazos establecidos en la fase de valoración.

La destrucción física siempre se hará de aquellas unidades o series documentales que hayan perdido su valor administrativo, probatorio o constitutivo o extintivo de derechos y que no hayan desarrollado ni se prevea que vayan a desarrollar valores históricos o testimoniales significativos.

La eliminación tiene obviamente una connotación física, puesto que lo que se destruye es el soporte y con él la información que contiene. Si se trata de documentos de archivo en papel, soporte e información forman un todo, y destruyendo el primero destruimos también el segundo, pero si nos referimos a documentos electrónicos el resultado no es tan sencillo. En estas directrices se incluirán recomendaciones para la destrucción de todo tipo de documentos, con independencia del soporte.

5

### 1.3. Documentos relacionados

|   |           |                                 |
|---|-----------|---------------------------------|
|  | G05/O     | Valoración                      |
|  | G05/D01/O | Instrumentos para la valoración |

## 2. Principios de la eliminación

La eliminación de documentos debe ser:

- Autorizada / Legal
- Apropiada e irreversible
- Segura/confidencial
- En tiempo
- Documentada

### 2.1. Autorizada / Legal

---

La destrucción física de unidades o series documentales sólo debe realizarse una vez que han perdido completamente su valor y su utilidad administrativa y no presenten valor histórico que justifique su conservación permanente. Siempre se realizará fruto de una eliminación reglada y autorizada.

La eliminación debe hacerse en seguimiento estricto a las normas establecidas por el organismo con capacidad decisoria que establezca los plazos y si la documentación es de conservación permanente o susceptible de ser eliminada.



Los documentos siempre se deben destruir conforme a los plazos establecidos en la fase de valoración.

El proceso de eliminación de documentos forma parte de la política de gestión documental de la organización. En este sentido, es necesario definir los métodos de destrucción específicos según los soportes y en función de una serie de escenarios, como puede ser el tipo de documentación, el nivel de seguridad necesario para la información que contiene, la eventual reutilización del soporte (para documentación electrónica) o el tipo de control de la gestión (si el proceso de destrucción va a ser interno o externo). Todos estos escenarios se van a tratar en estas Directrices.

### 2.2. Apropiada e irreversible

---

La eliminación se llevará a cabo empleando cualquier método que garantice la imposibilidad de reconstrucción de los mismos y su posterior utilización, así como la recuperación de cualquier información contenida en ellos. Es deseable que el método utilizado sea respetuoso con el medio ambiente así como, en la medida de lo posible, el resultado se pueda reciclar.

Se tienen que tomar precauciones extraordinarias para la destrucción de materiales nocivos o tóxicos, por ejemplo, utilizando el reciclado químico. En estos casos, se recomienda buscar un servicio especializado.

Asimismo, los documentos se deben destruir de una manera segura, también para quienes llevan a cabo la misma.

Las Administraciones Públicas deben vigilar que la destrucción de la documentación se efectúe de acuerdo con la normativa de protección medio ambiental, estableciendo un sistema de reciclaje adecuado para el material en el que se soporta la información.

### 2.3. Segura / confidencial

---



Los documentos siempre deben eliminarse de una manera segura, con el mismo nivel de seguridad que han tenido durante todo su ciclo de vida.

Los documentos que incluyan datos de carácter personal o confidencial deben eliminarse de acuerdo con un procedimiento que garantice la preservación de su información hasta el momento de su destrucción y la imposibilidad de recomposición, tanto de la información como de los soportes.

Los documentos que se van a destruir deben estar protegidos frente a posibles intromisiones externas hasta su destrucción. El lugar o los contenedores donde se almacenan los documentos que se van a eliminar requieren medidas de seguridad eficaces frente a posibles intromisiones exteriores. No deben permanecer al descubierto en el exterior de los edificios, ni amontonarse en lugares de paso, ni en locales abiertos. Las instalaciones donde se custodie dicha documentación hasta el momento de su destrucción deben contar con medidas de seguridad adecuadas.

#### **2.4. En tiempo**

---

De la misma forma que ningún documento debe ser eliminado antes de lo establecido, es también importante que no se conserven los documentos más tiempo del necesario. Esto minimizará los costes administrativos y de custodia.

Si hay motivos justificados para conservar una documentación más tiempo de lo establecido según los plazos establecidos tras la valoración, se deben documentar dichos motivos, por si hay que modificar el dictamen recogido en el calendario de conservación / tabla de retención documental.

#### **2.5. Documentada**

---

El proceso de eliminación debe siempre documentarse a través de un acta de eliminación. Debe constar, como mínimo, de la fecha de destrucción, del método utilizado para la misma, de un listado de los documentos que se han eliminado, de la firma de la persona que ha supervisado la destrucción, así como, la mención del dictamen / resolución / procedimiento reglado al que se acoge para poder realizar dicha destrucción.

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.

Las organizaciones públicas deben llevar un registro de la destrucción (Registro de Salida de Documentos). En algunos casos, por ejemplo en los procesos judiciales, se puede solicitar una prueba de destrucción de la documentación, por lo que es sumamente importante dejar constancia documental de la misma.

### **3. Métodos de destrucción**

---

En la selección del método de destrucción se debe tener en cuenta, además del nivel de confidencialidad de la información contenida en la documentación a eliminar, el tipo de soporte que la contiene.

#### **3.1. Documentación en papel**

---



El método más adecuado de eliminación de la documentación en papel es la trituración mediante corte en tiras o cruzado. El papel se hace tiras o partículas, cuyo tamaño se elegirá en función del nivel de protección requerido por la información contenida en los documentos a destruir.

Es recomendable que la documentación triturada se entregue o venda para su reciclaje. Lo que no es un método seguro es entregar o vender la documentación a eliminar como papel usado para su reciclaje sin destrucción previa. El receptor o comprador de papel usado normalmente realizará una selección, descartando lo que considere inútil, sin que el responsable de los documentos sepa cuál será el destino del papel que no se considere apto para el reciclaje. Por otra parte, puede almacenar intacta, durante un tiempo indeterminado y sin ninguna medida de seguridad, la documentación a eliminar en espera de reunir una cantidad suficiente de papel de un mismo tipo o color para reciclar, lo que no se puede asumir por parte del responsable de dicha documentación.

Otro método que se ha utilizado es el enterramiento de los documentos. No es un método recomendable porque no supone la desaparición inmediata de la información, e incluso se ha comprobado que el papel se conserva más tiempo enterrado que si se dejase al aire libre. Además, no se puede garantizar la confidencialidad de la información ni la imposibilidad de reconstrucción, ya que realmente no se está destruyendo la documentación.

La incineración es otro método ampliamente utilizado. En este caso sí se acaba con la información e imposibilita la reconstrucción, pero resulta peligroso para el entorno, puede perjudicar al medio ambiente e impide el reciclaje.

Hay varias normas del ámbito de ISO o de otras agencias nacionales de normalización basadas en la destrucción de documentación. Una de ellas es la Norma UNE – EN 15713:2010 *Destrucción segura del material confidencial. Código de buenas prácticas*, versión de la agencia normalizadora española (AENOR) de la aprobada por el Comité Europeo de Normalización (CEN) EN 15713:2009, que proporciona recomendaciones para la gestión y control de la destrucción de material de carácter confidencial, asegurando que dicho material se destruye de forma segura. Establece ocho niveles de triturado o desintegración (aplicables o no según la clase de material) y determina el tamaño máximo de corte y el método de destrucción en función de ese nivel.

Para documentos en papel establece el triturado o desintegración de la documentación según los siguientes niveles de seguridad:



Documentos de carácter general para que sean ilegibles o anulados.  
Partículas de material con una superficie < 5000 mm<sup>2</sup> o tira de longitud indeterminada con un corte máximo de ancho de < 25 mm



Documentos internos que pasarán a ser ilegibles o anulados.  
Partículas de material con una superficie < 3600 mm<sup>2</sup> o tira de longitud indeterminada con un corte máximo de ancho de < 16 mm.



Datos sensibles y confidenciales, así como datos personales sujetos a requisitos de protección. Partículas de material con una superficie  $< 2000 \text{ mm}^2$  o tira de longitud indeterminada de ancho  $< 12 \text{ mm}$

---



Datos altamente sensibles y confidenciales, así como los datos personales que sean objeto de altos requisitos de protección. Partículas de material con una superficie  $< 800 \text{ mm}^2$  y regulares con ancho máximo de corte de  $< 6 \text{ mm}$

---



Datos con información confidencial de importancia fundamental para una persona, empresa o institución. Partículas de material con una superficie  $< 320 \text{ mm}^2$  y regulares con ancho máximo de corte de  $< 4 \text{ mm}$

---



Datos confidenciales con medidas de seguridad extraordinarias. Partículas de material con una superficie  $< 30 \text{ mm}^2$  y regulares con ancho de tira  $< 2 \text{ mm}$

---



Datos estrictamente confidenciales con las más elevadas precauciones de seguridad. Partículas de material con una superficie  $< 10 \text{ mm}^2$  y regulares con ancho de tira  $< 0.8 \text{ mm}$

---

### 3.2. Documentación electrónica

---

Los documentos electrónicos poseen unas características específicas que deben tenerse en cuenta de cara a su eliminación:

- se almacenan en soportes de almacenamiento con un formato específico
- el contenido informativo es independiente del soporte y el formato
- los soportes son generalmente reutilizables
- su vida útil es corta comparada con la de un soporte en papel
- todo soporte o formato se hará obsoleto en un plazo más o menos largo de tiempo, lo que implicará necesariamente un cambio de soporte o formato (excepto algunos formatos longevos como PDF/A).
- los procedimientos de destrucción deberán tener en cuenta las características de los soportes más adecuados para la conservación de los documentos electrónicos
- pueden existir múltiples copias, no siempre controladas, de los documentos.

Atendiendo a estas características de la documentación electrónica se propone emplear los términos *borrado*, entendido como el procedimiento de eliminación de los datos o ficheros de un soporte o conjunto de soportes, permitiendo su reutilización, y *destrucción*, entendido como el proceso de destrucción física de soportes de almacenamiento que contengan documentos electrónicos.

Se deben identificar las técnicas de borrado apropiadas para cada soporte (si es óptico, magnético, memorias externas...) y tipo de información que contiene. Como en cualquier otro proceso de destrucción, es necesario dejar constancia de los procedimientos de borrado realizados.

Los soportes y sistemas de almacenamiento más utilizados son:



Información en soportes de datos ópticos, por ejemplo CDs / DVDs. Actualmente su uso está en retroceso ya que no pueden competir con la capacidad que proporcionan los soportes de tipo magnético.



Información en soportes de datos magnéticos, por ejemplo, tarjetas de identificación, disquetes, etc. Uso en retroceso por su escasa capacidad.



Información en unidades de discos duros magnéticos.



La información en soportes de datos electrónicos, por ejemplo, en memorias USB o en tarjetas de chip.

Sin entrar en mucho detalle debido en parte a la gran cantidad de datos técnicos, las técnicas específicas de borrado seguro de documentos y destrucción de soportes más utilizadas actualmente son:

- La **sobrescritura**: consiste en reemplazar los datos almacenados por un patrón binario de información sin sentido. La eficacia de este método depende del número de ciclos de sobrescritura. Existen procedimientos avanzados que permiten saber, con bastante precisión, la información que existía originalmente, por eso la información que se debe sobrescribir debe generar tal desorden en el soporte magnético que la recuperación de los datos originales sea prácticamente imposible. No se puede utilizar en soportes dañados ni en aquellos que no sean regrabables, como CDs y DVDs de solo escritura.
- La **desmagnetización**: consiste en la exposición de los soportes de almacenamiento a un campo magnético suficientemente potente para modificar la polaridad de las partículas magnéticas y, por tanto, eliminar los datos almacenados, impidiendo la recuperación de los mismos. Válido para dispositivos magnéticos, como por ejemplo los discos duros o cartuchos de cinta. Tiene varios inconvenientes, como que se debe

analizar qué campo electromagnético se tiene que utilizar para cada dispositivo, se tienen que trasladar los dispositivos al lugar donde se encuentre el desmagnetizador y en algunos medios de grabación magnética (aquellos con caché de memoria Flash) no se elimina toda la información almacenada.

- La **destrucción física**: consiste en la inutilización del soporte. Se puede hacer mediante:
  - la **desintegración**: mecanismo de corte o triturado no uniforme que reduce el dispositivo a pedazos de tamaño y forma aleatorios
  - la **pulverización**: proceso que consiste en machacar el material y que se utiliza para la destrucción de discos duros
  - la **fusión**: proceso mediante el cual el material se calienta a una temperatura que es menor que el punto de encendido pero suficientemente alta para derretirlo, puede ser un medio efectivo de destrucción para los discos duros
  - la **incineración**: puede destruir completamente todos los dispositivos y para todos los niveles de seguridad. Debe llevarse a cabo en incineradoras que hayan sido aprobadas en cuanto a impacto medioambiental, para plásticos y otros materiales
  - el **triturado**: consiste en reducir el soporte a pedazos minúsculos de tamaño y forma uniformes. El uso de trituradoras está normalmente limitado a soportes de grosor fino, como los soportes de datos ópticos (DVDs o CDs)

Los métodos de destrucción física pueden ser completamente seguros en cuanto a la destrucción real de los datos pero tienen algunos inconvenientes como que los residuos generados deben ser tratados adecuadamente, que implican la utilización de distintos métodos industriales de destrucción según el soporte o que obligan a un transporte de los dispositivos a un centro de reciclaje adecuado, lo que hay que hacer con las medidas de custodia adecuadas para asegurar el control de los dispositivos.

- La **criptografía y borrado criptográfico**. En los últimos años se han sacado al mercado dispositivos con cifrado integrado, también conocidos como Dispositivos de AutoCifrado (SED “self encrypting devices”). Disponen de un cifrado permanente que reduce la probabilidad de que datos sin cifrar se conserven en el dispositivo. El borrado criptográfico consiste en aprovechar el cifrado para implementar el borrado de los datos mediante la eliminación de la clave de cifrado del dispositivo. Ello implica que en el soporte de almacenamiento sólo se conservan los datos cifrados, impidiendo su recuperación sin la clave, efectuando de esta manera un borrado seguro. Su mayor ventaja es que permite realizar una limpieza de alta seguridad de una manera mucho más rápida. Un inconveniente es que hay que ser muy cuidadoso y asegurarse que todas las copias de las claves de cifrado se eliminan. También es complicada la verificación de la eliminación porque los proveedores no suelen proporcionar información sobre la tecnología utilizada para fabricar el controlador que es necesaria para comprender las cuestiones de permanencia en memoria de residuos de datos.

Se deben destruir todas las copias de los documentos cuya eliminación esté autorizada, incluidas las copias de seguridad, las copias de conservación y las copias de seguridad electrónica.

#### **4. Contratación externa**

---

La contratación de una empresa especializada en servicios de destrucción de documentos puede resultar, en función del volumen de documentación y de los medios técnicos exigidos, una opción aconsejable. Si se escoge esta opción, hay que tener en cuenta que se está cediendo el control de la información a un tercero, por lo que se deben solicitar las máximas garantías al proveedor.

El cumplimiento de los siguientes requisitos da garantías a los responsables de la documentación de la seguridad y confidencialidad en los procesos realizados hasta la destrucción física y eliminación de la información:

- Debe suscribirse un contrato por escrito entre la empresa de destrucción y el cliente, en el que se regulen todas las transacciones. En él se debe dar información sobre las actividades, los medios de transporte, de custodia, de destrucción, así como de los compromisos asumidos y la entrega de los correspondientes certificados de destrucción.
- Se debe exigir que un representante del responsable de los documentos presencie la destrucción de los documentos y compruebe las condiciones en que se realiza y los resultados.
- Se debe garantizar la destrucción de los documentos en sus instalaciones y con medios propios, sin subcontratos que conlleven el manejo de los documentos por parte de otras empresas sin conocimiento del responsable de los documentos.
- La destrucción debe realizarse al nivel adecuado conforme a la confidencialidad de los documentos y del material que se tiene que destruir.
- El personal que lleva a cabo la recogida, transporte y destrucción debe contar con la formación adecuada, así como suscribir un compromiso de confidencialidad.
- Resulta evidente que a las empresas de destrucción se les debe exigir que cumplan con la legislación que les aplica por su actividad, por el tratamiento de los datos que realizan y por el potencial impacto medioambiental.

Todas las operaciones de manejo y transporte de los documentos durante el traslado y hasta el momento de la destrucción deben estar realizadas por personal autorizado e identificable. El medio de transporte debe utilizarse exclusivamente para aquellos documentos que se van a eliminar y contar con sistemas de seguridad (vehículos cerrados, con sistemas de alarma e inmovilización, por ejemplo).

A la empresa se le debe exigir un certificado de destrucción de los documentos donde conste que la información ya no existe, y dónde, cuándo y cómo ha sido destruida. Es imprescindible dejar constancia de las actividades realizadas, y sirve para la auditoría y evaluación del cumplimiento de los requisitos acordados entre la empresa y el archivo.

Version 1

## 5. Cuadro de compromisos de cumplimiento

Este cuadro identifica aquellos compromisos establecidos en las líneas de actuación de la Guía de Implementación de Valoración y unas recomendaciones sobre cómo cumplir con los mismos.

El número representado es el mismo con el que se identifica dicho compromiso en la Guía de Implementación.

| Nº  | Compromisos  | Cómo cumplir con los compromisos  |
|-----|--|---|
| 8.1 | Establecer y documentar la identidad de la/s persona/s autorizada/s para llevar a cabo las decisiones tomadas en relación con la eliminación y de la autoridad competente que lo ha autorizado | <p>Incluir definiciones de las responsabilidades del personal del organismo para llevar a cabo estas actuaciones</p> <p>Incluir en el expediente de eliminación de la serie las autorizaciones que aprueban dichas decisiones</p> <p>Ponerse en contacto siempre con el órgano responsable de las decisiones de valoración</p> <p>Delegar y asignar la responsabilidad de llevar a cabo la eliminación de los documentos al empleado/s apropiado/s. Necesitará una autorización para realizar los procedimientos de eliminación</p> <p>Asegurarse que el personal que lleva a cabo los procesos de eliminación entiende:</p> <ul style="list-style-type: none"> <li>- Las normas de cumplimiento para la valoración de documentos</li> <li>- Cómo se interpretan y se cumplen</li> </ul> <p>Incluir definiciones de las responsabilidades del personal del organismo para llevar a cabo estas actuaciones</p> <p>Identificar quién lleva a cabo la eliminación y es responsable de ella dentro de la organización</p> <p>Capacitar a los responsables mediante cursos específicos</p> |



| Nº  | Compromisos                                       | Cómo cumplir con los compromisos   |
|-----|---|--|
| 8.2 | Realizar eliminaciones autorizadas y legales      | <p>Documentar el análisis y los procedimientos de toma de decisión</p> <p>Incluir la descripción de cómo se han tomado las decisiones de valoración</p> <p>Tener decisiones aprobadas a un nivel directivo dentro de la organización</p> <p>Establecer en las políticas y procedimientos de la organización actuaciones autorizadas para poder realizar actividades de eliminación</p> <p>Constatar que la eliminación se hace de documentos que han perdido completamente su valor y su utilidad administrativa y no presentan valor histórico que justifique su conservación permanente</p>  |
| 8.3 | Realizar eliminaciones apropiadas e irreversibles | <p>Incluir la descripción de cómo se han tomado las decisiones dentro de la política y los procedimientos del organismo público</p> <p>Verificar que el método empleando para la eliminación garantiza la imposibilidad de reconstrucción de los documentos y su posterior utilización, así como la recuperación de cualquier información contenida en ellos</p> <p>Vigilar que la eliminación de los documentos se realiza de acuerdo con la normativa de protección medio ambiental, estableciendo un sistema de reciclaje adecuado para el material en el que se soporta la información</p> |

| Nº  | Compromisos   | Cómo cumplir con los compromisos   |
|-----|---|--|
| 8.4 | Realizar eliminaciones seguras y con los niveles necesarios de confidencialidad | <p>Asegurarse que los documentos se eliminan de una manera segura, con el mismo nivel de seguridad que han tenido durante todo su ciclo de vida</p> <p>Eliminar los documentos que incluyan datos de carácter personal o confidencial de acuerdo con un procedimiento que garantice la preservación de su información hasta el momento de su destrucción y la imposibilidad de recomposición, tanto de la información como de los soportes</p> <p>Proteger a los documentos que se van a destruir frente a posibles intromisiones externas hasta su destrucción.</p>   |
| 8.5 | Eliminar los documentos identificados para ello en los plazos establecidos      | <p>Desarrollar políticas y procedimientos para identificar y documentar las series documentales del organismo que ya están valoradas para su eliminación</p> <p>Identificar aquellos documentos que tienen que eliminarse, siguiendo las decisiones de valoración aprobadas, dentro de la organización</p> <p>Incluir en la aplicación de gestión de documentos la información pertinente para informar qué series documentales están afectadas por un dictamen de eliminación y los plazos para cumplir dicho dictamen</p> <p>Incluir en la aplicación de gestión documental avisadores de tiempo para realizar dichas acciones</p> |

| Nº  | Compromisos  | Cómo cumplir con los compromisos   |
|-----|--|--|
| 8.6 | Documentar la naturaleza y plazos de eliminación   | <p>Documentar todas las acciones, incluyendo información sobre:</p> <ul style="list-style-type: none"><li>- los documentos que van a destruirse/borrarse</li><li>- fecha y lugar en que se lleva a cabo la eliminación</li><li>- la aprobación y autorización, incluyendo los detalles de la persona que lleva a cabo la acción, así como su confirmación de que se ha llevado a cabo</li></ul> <p>Confirmar y documentar:</p> <ul style="list-style-type: none"><li>- que se ha realizado una correcta eliminación de los documentos</li><li>- que las decisiones de eliminación son precisas y se han realizado en tiempo</li></ul> <p>Si se han destruido / borrado documentos, las organizaciones deben ser capaces de demostrar que los documentos se han eliminado físicamente (por ejemplo, con un certificado) o borrados del sistema (por ejemplo, con los metadatos que incluyen la información sobre la eliminación de dichos documentos del sistema)</p> |
| 8.7 | Planificar e integrar la eliminación de documentos en el programa de gestión documental de la organización | <p>Incorporar al sistema de gestión documental de la organización todas las acciones relacionadas con la eliminación de documentos para que se hagan en el tiempo establecido</p> <p>Incorporar al sistema de gestión documental de la organización las fechas en las que se deben llevar a cabo las decisiones relativas a la eliminación de series documentales, una vez aprobadas por el organismo competente</p>   |

| Nº   | Compromisos  | Cómo cumplir con los compromisos  |
|------|--|---|
| 8.8  | Poner a disposición de todos los miembros de la organización las decisiones tomadas en cuanto a eliminación de series documentales | <p>Desarrollar procedimientos dentro de la organización para informar sobre todas las decisiones tomadas en cuanto a la eliminación de series documentales</p> <p>Incluir en la intranet de la organización información sobre plazos y series documentales valoradas para su eliminación</p>  |
| 8.9  | Monitorizar todas las acciones que se llevan a cabo para la implementación de la eliminación de documentos                         | <p>La organización debe proporcionar una supervisión adecuada y un control de los trabajos que asegure la calidad y pertinencia de dichos procesos</p> <p>Debe estar presente en la eliminación de los documentos un responsable de la organización que da fe de dicha actuación</p> <p>Si la eliminación se lleva a cabo por una empresa de contratación externa se debe hacer un seguimiento por parte del organismo de cumplimiento de todos los requisitos de eliminación acordados</p> |
| 8.10 | Incluir la eliminación de documentos dentro de las actuaciones rutinarias y regulares de la organización                           | <p>Realizar peticiones de información a las unidades o archivos remitentes responsables de la eliminación para realizar un informe sobre las eliminaciones realizadas una vez al año</p> <p>Confeccionar un Plan anual con la previsión de los recursos necesarios para la eliminación de documentos para tenerse en cuenta en la planificación del presupuesto del archivo</p>   |



| Nº   | Compromisos  | Cómo cumplir con los compromisos   |
|------|--|--|
| 8.11 | Revisar regularmente las decisiones tomadas en relación con la eliminación de series documentales por parte del organización | Establecer una fecha cíclica para la revisión de las decisiones, por ejemplo, cada 5 años si no ha habido cambios administrativos o procedimentales que obliguen a una revisión en menos tiempo<br><br>Incluir las revisiones dentro de la planificación del Programa de gestión documental de la organización |

## 6. Términos y referencias

---

### 6.1. Glosario

---

**Borrado:** referido a documentos electrónicos, procedimiento de eliminación de los datos o ficheros de un soporte o conjunto de soportes, permitiendo su reutilización. El borrado criptográfico consiste en aprovechar el cifrado para implementar el borrado de los datos mediante la eliminación de la clave de cifrado del dispositivo.

**Desmagnetización:** exposición de los soportes de almacenamiento a un campo magnético suficientemente potente para modificar la polaridad de las partículas magnéticas y, por tanto, eliminar los datos almacenados, impidiendo la recuperación de los mismos.

**Destrucción:** referido a un soporte de almacenamiento que contenga documentos electrónicos, proceso de destrucción física del mismo, ya sea por obsolescencia del soporte, por sustitución completa del sistema de almacenamiento o porque las características de la información de los documentos aconsejen esta destrucción (por ejemplo, por su elevado grado de confidencialidad).

**Eliminación:** proceso consistente en la destrucción de documentos o en la baja o borrado de un sistema informático, una vez analizados sus valores (administrativo, jurídico, informativo, histórico, testimonial) que permitan constatar su inutilidad a todos los efectos y tras un procedimiento reglado de valoración.

**Selección:** operación intelectual y material de localización de las fracciones de series documentales que han de ser objeto de valoración.

**Sobrescritura:** efecto de reemplazar los datos almacenados por un patrón binario de información sin sentido.

### 6.2. Referencias

---

AENOR. 2010. *UNE-EN 15713: 2010. Destrucción segura del material confidencial. Código de buenas prácticas*. Madrid: AENOR.

AUSTRALIA. NORTHERN TERRITORY GOVERNMENT. 2010. *Guidelines for the destruction of a public sector organisation's temporary value records (Issued November 2010)* [en línea]. [Consulta: 15 diciembre 2014]. Disponible en: [http://www.nt.gov.au/dcis/info\\_tech/records\\_policy\\_standards/tempo\\_value\\_records\\_disposal.shtml](http://www.nt.gov.au/dcis/info_tech/records_policy_standards/tempo_value_records_disposal.shtml)

AUSTRALIA. STATE RECORDS AUTHORITY OF NEW SOUTH WALES. 2010a. *Guideline 3: Destruction of Records* [en línea]. [Consulta: 15 diciembre 2014]. Disponible en: <http://www.records.nsw.gov.au/recordkeeping/advice/retention-and-disposal/destruction-of-records>

AUSTRALIA. STATE RECORDS AUTHORITY OF NEW SOUTH WALES. 2010b. *Recordkeeping In Brief 51 - Destroying digital records: When pressing delete is not enough. Guideline 3: Destruction of Records* [en línea]. Sydney. [Consulta: 15 diciembre 2014]. Disponible en: [http://www.archives.qld.gov.au/Recordkeeping/GRKDownloads/Documents/Destruction\\_of\\_digital\\_records.pdf](http://www.archives.qld.gov.au/Recordkeeping/GRKDownloads/Documents/Destruction_of_digital_records.pdf)

COLOMBIA. ALCALDÍA MAYOR DE BOGOTÁ. *Protocolo para la eliminación de documentos de archivo* [en línea]. Bogotá: Alcaldía Mayor. [Consulta: 15 diciembre 2014]. Disponible en: [http://intranetsdis.integracionsocial.gov.co/anexos/documentos/3.4\\_proc\\_adminis\\_gestion\\_bienes\\_servicios/3.%20DOC\\_EliminacionDocumentosArchivo.pdf](http://intranetsdis.integracionsocial.gov.co/anexos/documentos/3.4_proc_adminis_gestion_bienes_servicios/3.%20DOC_EliminacionDocumentosArchivo.pdf)

ESPAÑA. COMISIÓN SUPERIOR CALIFICADORA DE DOCUMENTOS ADMINISTRATIVOS. 2003. *Recomendaciones para la destrucción física de documentos de archivo en papel de la Administración General del Estado* [en línea]. Madrid: Ministerio de Educación, Cultura y Deporte. [Consulta: 15 diciembre 2014]. Disponible en: <http://www.mcu.es/archivos/docs/MetodologiaComSup.pdf>

ESPAÑA. INTECO. 2011. *Guía sobre almacenamiento y borrado seguro de información* [en línea]. Madrid: Ministerio de Industria, Comercio y Turismo. [Consulta: 15 diciembre 2014]. Disponible en: [http://www.inteco.es/guias\\_estudios/guias/guia\\_borrado\\_seguro](http://www.inteco.es/guias_estudios/guias/guia_borrado_seguro)

### 6.3. Bibliografía

---

CERMENO, L.; RIVAS, E. 2011. Valoración, selección y eliminación. En: CRUZ MUNDET, J. R. (dir.). *Administración de documentos y archivos. Textos fundamentales* [en línea]. Madrid: Coordinadora de Asociaciones de Archiveros y Gestores de Documentos, pp. 215-272. [Consulta: 15 diciembre 2014]. Disponible en: <http://www.archiveros.net/LIBRO.ARCHIVOS.IBEROAMERICANOS.pdf>

MILLARUELO, A.; PÉREZ DE LEMA, A. 2014. Destrucción o eliminación segura de documentación electrónica y soportes informáticos. En: *Política de gestión de documentos electrónicos. Ponencias complementarias* [en línea]. Madrid: Ministerio de Hacienda y Administraciones Públicas. [Consulta: 15 diciembre 2014]. Disponible en: <http://www.minhap.gob.es/Documentacion/Publico/SGT/POLITICA%20DE%20GESTION%20DE%20DOCUMENTOS%20MINHAP/politica%20de%20gestion%20de%20documentos%20electronicos%20MINHAP-ponencias%20complementarias%20al%20documento.pdf>

RAMÍREZ DELEÓN, J. A. (Coord.). 2011. *Metodología para la valoración y disposición documental: aspectos teóricos e instrumentales* [en línea]. México: Instituto Federal de Acceso a la Información y Protección de Datos (IFAI). [Consulta: 15 diciembre 2014]. Cuadernos de la serie Gestión de Documentos y Administración de Archivos. Nº 5. Disponible en: <http://inicio.ifai.org.mx/Publicaciones/cuaderno5.pdf>

TORREBLANCA, A.; CONDE, M. L. 2003. *Sistemas de eliminación de documentos administrativos*. Murcia: Dirección General de Cultura