RECOMENDACIONES PARA EL BORRADO LÓGICO DE DOCUMENTACIÓN ELECTRÓNICA Y LA DESTRUCCIÓN FÍSICA DE SOPORTES INFORMÁTICOS QUE FORMEN PARTE DEL PATRIMONIO DOCUMENTAL MADRILEÑO[1]

EL BORRADO LÓGICO DE DOCUMENTACIÓN ELECTRÓNICA Y LA DESTRUCCIÓN FÍSICA DE SOPORTES INFORMÁTICOS SE LLEVARAN A CABO TENIENDO EN CUENTA LA LEY 6/2023, DE 30 DE MARZO, DE ARCHIVOS Y DOCUMENTOS DE LA COMUNIDAD DE MADRID Y SU NORMATIVA DE DESARROLLO Y CONTANDO CON LAS PRECEPTIVAS AUTORIZACIONES

El Consejo de Archivos de la Comunidad de Madrid, de acuerdo con la Ley 6/2023, de 30 de marzo, de Archivos y Documentos de la Comunidad de Madrid, es el órgano colegiado consultivo, multidisciplinar y técnico de asesoramiento, cooperación y participación de la Comunidad de Madrid en las materias relacionadas con el Sistema de Archivos de la Comunidad de Madrid y el Patrimonio Documental Madrileño. En este sentido, y en relación con la valoración y eliminación de documentos, asume una doble responsabilidad: por un lado, es el responsable de informar preceptivamente sobre la inclusión o, en su caso, exclusión del Patrimonio Documental Madrileño de los documentos de titularidad privada a que se hace referencia en los apartados 1 y 2 del artículo 80 de la ley 6/2023, de 30 de marzo; por otro, para los documentos de titularidad pública, en virtud de lo previsto en el apartado 2 de la Disposición Transitoria Tercera de la Ley 6/2023, de 30 de marzo, asume, de forma temporal, la función atribuida a la Comisión de Acceso y Valoración de Documentos de la Comunidad de Madrid de emitir dictamen preceptivo y vinculante tanto sobre la aprobación de las Tablas de Valoración de las series documentales como sobre la autorización de eliminación de aquellos documentos que, extinguido su valor probatorio de derechos y obligaciones, carezcan de interés para la Comunidad de Madrid.

La creciente importancia de los documentos electrónicos y en soportes informáticos impone el diseño y aplicación de unas recomendaciones que faciliten tanto el borrado lógico de documentación electrónica como la destrucción física de los soportes informáticos que formen parte del Patrimonio Documental Madrileño, con vistas a su utilización por todos los interesados.

Para la elaboración de estas recomendaciones, se ha seguido el documento que, en este sentido, aprobó la Comisión Superior Calificadora de Documentos Administrativos del Estado en su reunión de 13 de diciembre de 2017.

1. REQUISITOS LEGALES PREVIOS A LA ELIMINACIÓN DE INFORMACIÓN

Los documentos de titularidad pública y de titularidad privada que forman parte del Patrimonio Documental Madrileño sólo pueden eliminarse mediante los procedimientos establecidos en la Ley 6/2023, de 30 de marzo, de Archivos y Documentos de la Comunidad de Madrid.

La eliminación de documentos de titularidad estatal se producirá de acuerdo con la legislación que le sea de aplicación, con el dictamen de la Comisión Superior Calificadora de Documentos Administrativos del Estado y con lo establecido en el convenio suscrito por la Administración General del Estado y la de la Comunidad de Madrid sobre gestión de archivos de titularidad estatal.

Asimismo, la eliminación de los documentos de la Administración de Justicia de la Comunidad de Madrid se atendrá lo establecido en el Real Decreto 937/2003, de 18 de julio, de modernización de los archivos judiciales y en la Ley 6/2023, de 30 de marzo, de Archivos y Documentos de la Comunidad de Madrid.

[1] Aprobadas por el Pleno del Consejo de Archivos de la Comunidad de Madrid en su sesión ordinaria de 25 de junio de 2018 (modificadas por el Pleno del Consejo de Archivos de la Comunidad de Madrid en: su sesión ordinaria de 14 de diciembre de 2020 y su sesión extraordinaria de 15 de diciembre de 2023).

En ningún caso se podrá autorizar la eliminación ni se podrá proceder a la destrucción de los documentos que forman parte del Patrimonio Documental Madrileño 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 o su correspondiente tabla de valoración establezcan para su conservación.

2. PROCESO DE DESTRUCCIÓN Y BORRADO

La protección de la intimidad de las personas y la defensa de los intereses de la Administración o de las instituciones privadas exigen que, como recoge la normativa vigente, los documentos que se eliminan sean destruidos de forma que su reconstrucción y la posterior utilización de la información que contienen sea imposible. Para hacerlo así, el proceso de destrucción debe estar sometido a estrictos controles que garanticen la seguridad, eficacia y confidencialidad del mismo.

A efectos de este documento, se emplea el término borrado como el procedimiento de eliminación de los datos o ficheros de un soporte o conjunto de soportes, permitiendo la reutilización de dichos soportes, y el término destrucción como el proceso de inutilización 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 de estado sólido, etc.) y tipo de información que contiene. Como en cualquier otro proceso de destrucción, es necesario dejar constancia documental de los procedimientos de borrado realizados.

3. SOPORTES Y SISTEMAS DE ALMACENAMIENTO

Se pueden distinguir tres tipos genéricos de soportes de almacenamiento ligados a tres tecnologías distintas:

a) Soportes magnéticos. Los soportes de esta naturaleza son:

   - Discos duros.
   - Cartuchos de cinta.

b) Soportes ópticos, por ejemplo: CD / DVD.
c) Soportes basados en memorias de estado sólido (FLASH).

Un aspecto también importante a tener en cuenta, considerando la metodología habitual de trabajo en la Administración, es la distinción entre:

a) Los dispositivos de almacenamiento local: Disco duro del puesto de usuario, dispositivos móviles, dispositivos removibles como discos duros externos, memorias USB, tarjetas de memoria y otros de similar naturaleza.
b) Los soportes de almacenamiento en red: Accesibles mediante protocolos para compartir ficheros (CIFS o NFS), redes SAN, almacenamiento en la nube y otros de similar naturaleza.

4. TÉCNICAS DE BORRADO SEGURO Y DE DESTRUCCIÓN DE SOPORTES

Las técnicas específicas de borrado seguro de documentos son:

a) **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.

b) **La desmagnetización.** Consiste en la exposición de los soportes de almacenamiento a un campo magnético suficientemente potente como para modificar la polaridad de las partículas magnéticas y, por tanto, eliminar los datos almacenados, impidiendo la recuperación de los mismos. Esta técnica sería válida para dispositivos magnéticos, como por ejemplo los discos duros o cartuchos de cinta. Tiene varios inconvenientes, como, por ejemplo:

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

c) **El borrado criptográfico.** Consiste en el cifrado de la información almacenada en el soporte utilizando un algoritmo de cifrado de clave privada, con una longitud de clave suficiente para que el descifrado de la información sea técnicamente inviable con las herramientas informáticas disponibles en ese momento. Seguidamente, la clave de cifrado se elimina con alguna de las técnicas de borrado seguro anteriores[2].

   Esta técnica se puede utilizar en cualquier tipo de soporte, aunque está especialmente recomendada para las memorias de estado sólido[3].

Las técnicas específicas de destrucción física que suponen la inutilización del soporte pueden realizarse mediante:

a) **La desintegración**: mecanismo de corte o triturado no uniforme que reduce el dispositivo a pedazos de tamaño y forma aleatorios.
b) **La pulverización**: proceso que consiste en machacar el material y que se utiliza para la destrucción de discos duros.
c) **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.
d) **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.
e) **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 (DVD o CD).

Los métodos de destrucción física pueden ser completamente seguros en cuanto a la destrucción real de los datos pero tienen algunos inconvenientes como, por ejemplo:

---

[2] Actualmente, el algoritmo de cifrado recomendado por el Centro Criptológico Nacional (CCN) es el AES (*Advanced Encryption Standard*, estándar FIPS 197), con una longitud mínima de clave de 128 bits, aunque el CCN recomienda elevarla a 256 bits para mayor seguridad en la Guía CCN – STIC – 807 *Criptología de empleo en el ENS* (edición mayo 2022).

[3] En la Guía de Seguridad de las TIC CCN – STIC – 305 *Destrucción y sanitización de Soportes Informáticos* (última edición de mayo de 2017), se reproducen los resultados de un trabajo de investigación realizado por la Universidad de San Diego en los que se concluye que *"por cada 1000 MB de datos es posible recuperar unos 100 MB de media, dependiendo del método, en cualquier unidad SSD, incluso habiendo aplicado un método de borrado seguro"*. Por esta razón, se recomienda el método de *"borrado criptográfico"* para estos dispositivos.

- Que los residuos generados deben ser tratados adecuadamente;
- Que implican la utilización de distintos métodos industriales de destrucción según el soporte;
- Que obligan al transporte de los dispositivos a un centro de reciclaje adecuado, con el consiguiente gasto en las medidas de custodia adecuadas para asegurar el control de los dispositivos.

Recomendación 1
Métodos de borrado o destrucción aplicables en cada tipo de soporte

Siempre que sea posible, optar por técnicas de borrado que puedan ser realizadas dentro de la propia organización, tales como: el borrado por *firmware*, la sobrescritura, el cifrado seguro y otras de similar naturaleza. De esta manera, se impedirá la entrega de soportes de información a agentes externos, con el consiguiente peligro de ruptura en la cadena de custodia.

En los dispositivos que cuenten con una función de borrado por *"firmware"*, se recomienda recurrir a la misma, ya que suele proporcionar un borrado seguro de bajo nivel equiparable al nivel 2 mencionado en el apartado 5.

El cuadro siguiente resume los métodos de borrado o destrucción aplicables en cada tipo de soporte:

	Magnético Óptico Electrónico (SSD)	Magnético Óptico Electrónico (SSD)	Magnético Óptico Electrónico (SSD)
Sobrescritura	√	(1)	√
Desmagnetización	√		
Borrado criptográfico	√	(1)	√
Destrucción Física	√	√	√

(1): Sólo en el caso de que se trate de medios regrabables.

5. NIVELES DE BORRADO / DESTRUCCIÓN DE LA INFORMACIÓN

Recomendación 2
Niveles de borrado/destrucción de la información

Se tendrá en cuenta la clasificación establecida por el Centro Criptológico Nacional[4], que distingue los niveles siguientes de borrado /destrucción de la información:

a) **Nivel 0**: Borrado usando comandos/utilidades estándar del sistema operativo. Estas técnicas generalmente marcan el espacio ocupado por los archivos a borrar como disponible, pero no eliminan realmente el contenido almacenado. Por este motivo, no impide la recuperación posterior de la información borrada ni proporciona ninguna garantía frente a la revelación no autorizada de la información.

   Este nivel se menciona aquí con carácter "académico" ya que no puede considerarse un método de borrado admisible.

b) **Nivel 1 (*'clearing'*)**: Borrado usando mecanismos de sobrescritura del espacio ocupado por los archivos a borrar. La recuperación de la información borrada sólo puede realizarse usando técnicas avanzadas.

[4] Guía CCN – STIC – 404. *Control de soportes informáticos* (diciembre 2006). Documento de acceso restringido.

Recomendado cuando el nivel de confidencialidad de la información a borrar sea bajo, usando mecanismos de sobrescritura[5] con un número reducido de pasadas sobre los mismos sectores (entre 2 y 5).

c) **Nivel 2 (*'sanitizing'*)**: Borrado seguro. Impide la recuperación de la información borrada incluso utilizando mecanismos avanzados. Algunas de las técnicas que se pueden utilizar para realizar este borrado son: la desmagnetización del soporte; el borrado seguro mediante *'firmware'* incorporado al soporte físico; la sobrescritura de la información con protocolos que hagan imposible su reconstrucción (generalmente, mediante una serie consecutiva de sobrescrituras); o el cifrado de la información con criptografía fuerte y ofuscación de la clave de cifrado empleada.

   Es el nivel recomendable cuando el grado de confidencialidad de la información a borrar sea medio o alto. Se utilizan funciones de sobrescritura más avanzadas[6], equiparables en seguridad al método Gutmann completo.

d) **Nivel 3**: Destrucción física del soporte (destrucción segura): Se realiza por procesos industriales como: triturado, incineración, pulverización, fusión de los materiales de que constan los soportes y otros de similar naturaleza.

Recomendación 3
Obligaciones respecto al Esquema Nacional de Seguridad

En todo caso, se respetarán las previsiones del Esquema Nacional de Seguridad, en especial para la medida **mp.si.5 (Borrado y destrucción)**.

Recomendación 4
Eliminación autorizada de las copias

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, salvo las copias o ficheros de respaldo (*"back – up"*) contempladas en el apartado 11, y dejar constancia exhaustiva/completa de esta destrucción en el expediente de eliminación.

Recomendación 5
Relación entre métodos de borrado/destrucción y nivel de aplicación

El siguiente cuadro resume la relación entre los métodos de borrado/destrucción y el nivel borrado /destrucción de la información en el que son aplicables:

	Nivel 1	Nivel 2	Nivel 3
Sobrescritura	√	√	
Desmagnetización		√	
Borrado criptográfico		√	
Destrucción Física			√

Recomendación 6
Forma y lugar de realización

Respecto a la forma y lugar de realización, el borrado seguro o criptográfico debería realizarse siempre por personal y con medios propios del organismo y en sus instalaciones. Únicamente en los casos de la

[5] Ejemplos de tales funciones son: el método Gutmann 10, Gutmann parcial con 5 pasadas, etc.
[6] Hay diversas aplicaciones que proporcionan estos algoritmos de borrado, tales como *"Eraser"* (aplicación para Windows con licencia GPL desarrollada por Heidi Computers Ltd.) o *"EraseIT Loop"* (desarrollada por Recovery Labs y certificada por el CCN).

desmagnetización y la destrucción física se puede considerar su externalización a empresas especializadas, previa celebración de un contrato administrativo de servicios.

Se resume la situación en el cuadro siguiente:

	Medios propios	Empresa externa
Sobrescritura	√	
Desmagnetización	√	√
Borrado criptográfico	√	
Destrucción Física	√	√

Recomendación 7
Documentación en "servicios en nube"

Un caso particular, pero de relevancia creciente, es el de la información de la que sea propietaria y responsable un organismo, pero que resida técnicamente en infraestructuras y servicios prestados por otra organización bajo cualquiera de las modalidades de *"servicios en nube"* (*"Software As A Service"*, *"Infraestructure As A Service"* y otros de similar naturaleza). En este caso, la organización que presta el servicio es la que debe ofrecer y asegurar la calidad de los procedimientos de borrado/eliminación segura. Dichos procedimientos deben quedar adecuadamente establecidos en el marco del pliego de prescripciones técnicas del contrato de servicios que se suscriba con la entidad prestadora.

6. ELECCIÓN DEL NIVEL DE BORRADO LÓGICO DE DOCUMENTACIÓN ELECTRÓNICA Y DESTRUCCIÓN FÍSICA DE SOPORTES INFORMÁTICOS

Recomendación 8
Elección de nivel de borrado/destrucción

A fin de determinar el nivel de borrado/destrucción más adecuado para cada caso específico, se recomienda tener en cuenta los siguientes parámetros:

R. 8.1. Nivel de confidencialidad de la información que va a ser borrada o destruida, por lo que hay que tener en cuenta:

a) El 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).
b) La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
c) Los grados de clasificación de seguridad (máximo secreto, secreto, reservado, confidencial, de difusión limitada).

R. 8.2. Quién ejecuta el proceso de borrado/destrucción
Si el proceso de borrado/destrucción va a ser gestionado y realizado por el organismo con sus propios medios internos o, por el contrario, va a ser realizado por una empresa externa en el marco de un contrato de prestación de servicios. En este ámbito, se recomienda:

a) Realizar el borrado/destrucción de la información con los medios internos del organismo con carácter general, evitando los riesgos asociados a su externalización, entre otros el transporte de dispositivos y la pérdida de la cadena de custodia.
b) Realizar previamente un borrado de nivel 2 sobre el contenido cuando excepcionalmente se produzca la externalización, entendiendo por ésta la gestión externa de cualquier procedimiento de borrado que se realice en el contexto de servicios en nube cuya infraestructura no sea de

gestión propia del organismo, y existiendo la previsión de cesión a terceros de la destrucción física de los dispositivos.

R. 8.3. Posible reutilización posterior del soporte
Si se va a reutilizar o no el soporte de información tras el borrado de la misma.

R. 8.4. Alcance de la eliminación
Si es parcial (afecta a una parte del soporte de almacenamiento) o total (afecta a todo el soporte de almacenamiento o sistema de almacenamiento).

Recomendación 9
Destrucción de soportes

En cuanto a la destrucción de soportes, se recogen como Anexo I los requisitos mínimos para los procesos de destrucción de distintos tipos de soportes, basados en la guía *Clearing and Declassifying Electronic Data Storage Systems* del Gobierno de Canadá[7].

R. 9.1. La destrucción de soportes en el marco de un contrato de servicios
En caso de realizar la destrucción a través de la contratación de servicios externos, se recomienda incluir en los pliegos del correspondiente procedimiento de contratación las previsiones siguientes:

- Los soportes que vayan a ser objeto de destrucción se almacenarán en contenedores opacos y precintados hasta el momento en que aquélla se lleve a cabo.
- Durante todo el proceso de recogida, entrega y transporte, los contenedores deberán estar permanentemente custodiados. Su entrega y recogida se hará por personal autorizado y debidamente identificado de la empresa adjudicataria.
- El transporte de los contenedores al lugar de destrucción se realizará en vehículos anónimos dedicados a tal efecto, con al menos dos operadores a su cargo. Las rutas de los vehículos deberán poder rastrearse por GPS.
- Por cada destrucción, el adjudicatario emitirá un Certificado de Destrucción Confidencial de todo el material destruido, declarando que el proceso se ha realizado conforme a lo indicado en el artículo 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y de acuerdo a la normativa medioambiental ISO 14001. El certificado reflejará la fecha, hora y lugar de destrucción, el procedimiento utilizado, el listado del personal que ha intervenido en la eliminación y, en su caso, la firma del empleado público fedatario.
- La empresa adjudicataria deberá permitir que la destrucción sea presenciada por un empleado público designado por la Administración que dé fe de la misma.

Una vez producida la destrucción, se confeccionará un acta de eliminación para su remisión a la Secretaría del Consejo de Archivos de la Comunidad de Madrid firmada por el empleado público fedatario, al que se unirá el certificado de destrucción citado.

R. 9.2. La destrucción de soportes con medios propios del organismo
En caso de realizar la destrucción con medios propios del organismo, y teniendo en cuenta que se ejecutará por una unidad de servicios generales distinta de la responsable, se recomienda comunicar a

[7] Fuente: Política de Gestión de Documentos Electrónicos del Ministerio de Hacienda y Administraciones Públicas (2016), p. 255 (en: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Archivo_electronico/pae_Politica-de-gestion-de-documentos-electronicos.html).

dicha unidad la recomendación 10.1 si tiene externalizado anualmente el servicio de mozos, mudanzas y transportes internos, para que se tenga en cuenta en el contrato anual.

7. ASPECTOS ESPECÍFICOS SOBRE EL BORRADO DE INFORMACIÓN Y ELIMINACIÓN DE SOPORTES

Recomendación 10
Copias de seguridad o respaldo (back – up)

En relación a las copias de seguridad o respaldo *("back – up"*[8]), proponemos que queden fuera del ámbito del documento, debido a la enorme dificultad técnica de controlar y, más aún, de eliminar todas las copias de respaldo que puedan existir de un documento cuya eliminación se ha acordado.

Hay que recordar que una copia de seguridad o respaldo *("back – up"*) no es una copia destinada a una actualización o consulta regular (como ocurre con un archivo de oficina), sino que se confecciona una sola vez y se recupera solamente en caso de incidentes de seguridad o pérdidas de información. En la mayoría de estos incidentes se produce la pérdida de la totalidad o la mayoría de la información del soporte del que se obtuvo la copia, por lo que se necesitará restaurar la totalidad de la información contenida en el soporte.

Desde este punto de vista, el que un documento eliminado pueda contener réplicas en varios archivos de respaldo o *"back – up"* no representa un riesgo importante ya que, como se ha indicado, a estas copias se accederá sólo ocasionalmente (cuando se produzcan incidentes) y sin que se efectúen búsquedas selectivas de un archivo o documento concreto.

Además, hay que tener en cuenta que las copias se van sobrescribiendo a medida que se realizan, eliminando las más antiguas de su tipo. En consecuencia, al finalizar un ciclo completo de copiado (por ejemplo, de un año) no quedará ya ninguna réplica de documentos/archivos que se eliminaron durante el año anterior.

Por estas consideraciones, se estima que la extensión de la eliminación de un documento a todas sus réplicas en los ficheros de respaldo (*back – up*) introduciría una enorme complejidad de gestión que no se ve compensada por el resultado (eliminación de soportes que raramente serán accedidos).

Como alternativa, puede plantearse que, cuando se elimine un documento y sea necesario restaurar alguno de los ficheros de respaldo (*back – up*) donde puede estar contenido dicho documento, en el proceso de restauración no se restituya el documento eliminado. Esta previsión obligará a gestionar una

---

[8] Se resumen a continuación algunos aspectos técnicos de la gestión de copias de seguridad:
Las copias de seguridad forman parte de *"políticas de back – up"* de la organización. De acuerdo con estas políticas, se suelen realizar 3 tipos de copias:

- Copias de seguridad completas de un soporte.
- Copias de seguridad incrementales. En estas copias, se incluyen sólo los ficheros/documentos modificados desde la última copia de seguridad completa o incremental.
- Copias de seguridad diferenciales. En estas copias sólo se incluyen los ficheros/documentos modificados desde la última copia de seguridad completa.

Las políticas de copiado contemplan un calendario de realización de copias con arreglo a un ciclo temporal, habitualmente con una duración de un mes, un año, etc. Por ejemplo, para un ciclo de un mes, podría preverse:

- 1 copia de seguridad completa el primer día del mes.
- 1 copia de seguridad incremental diaria.
- 1 copia de seguridad diferencial semanal.

Las copias se van sobrescribiendo a medida que se realizan, eliminando las más antiguas de su tipo.

"lista negra" de documentos que no han de restaurarse de los correspondientes soportes de *"back – up"*, pero su gestión es sin duda más sencilla[9].

Recomendación 11
Eliminación de documentos referenciados en más de un expediente

Un problema conexo es el relacionado con la eliminación de documentos que estén referenciados en más de un expediente, lo que es un escenario frecuente en el entorno electrónico.

Un Sistema de Gestión de Documentos Electrónicos (SGDE) debe ser capaz de consultar en cualquier momento los expedientes de los que forma parte un documento y, si se intenta eliminar este último, generar las alertas correspondientes, tanto si el documento a eliminar está referenciado en expedientes aún en la oficina como si está ya en el archivo electrónico único.

En este sentido, y a fin de mantener la integridad de estos índices y del documento que pertenece a otro expediente de otra serie documental con un plazo distinto de eliminación o con una valoración de conservación permanente, el SGDE no debería permitir dicha eliminación[10].

Recomendación 12
Eliminación de documentos a partir de los cuales se han generado copias auténticas

Una cuestión relacionada con la anterior es la eliminación de documentos que se han utilizado para la generación de copias auténticas completas o parciales. Como es sabido, en estos casos, la Norma Técnica de Interoperabilidad de Procedimientos de Copiado Auténtico y Conversión entre Documentos Electrónicos prevé que al nuevo documento obtenido se le asocie un metadato *"Identificador de documento origen"* con el identificador ENI del documento electrónico original.

Si este último se elimina, podemos encontrarnos de nuevo con una referencia que apunta a un documento ya no existente.

Hay que recordar que, desde el momento en que la copia electrónica auténtica se genera con los requisitos establecidos en la Norma Técnica, y en particular con una firma digital que garantiza su correspondencia con el documento original, la copia generada tiene por sí misma valor de documento electrónico auténtico, con independencia del original o copia auténtica del que se obtuvo.

Por ello, en el caso de copias auténticas completas la eliminación del documento original no cuestionaría la validez de dichas copias; ahora bien, a fin de no alterar los metadatos de la copia auténtica (que, recordemos, son metadatos obligatorios), será necesario que en el SGDE se mantenga una trazabilidad y evidencia suficiente de la acción de borrado (identidad del documento eliminado, momento de eliminación y motivo de la misma).

En el caso de **copias electrónicas parciales**, que suelen obtenerse para filtrar o censurar información del documento original que no se desea o no debe mostrarse por razones legales al destinatario de la copia, se recomienda mantener en el SGDE dicho documento (o una copia auténtica completa del mismo) para que esta acción de ocultación o censura de la información no sea irreversible. Por ello, en este caso recomendamos que, o bien se realice también una eliminación *"en cascada"* del documento original y sus copias parciales, o bien se impida la eliminación mientras no se eliminen primero dichas copias parciales.

---

[9] La mayoría de los sistemas de gestión de *"back – up"* permiten establecer filtros para excluir de la restauración a los ficheros que cumplan una condición (un patrón en su nombre, la pertenencia a una carpeta, por rangos de fechas de creación o modificación, etc.).

[10] Téngase en cuenta que en este caso debe prevalecer para la conservación el plazo más largo dictaminado por la Consejo de Archivos de la Comunidad de Madrid.

ANEXO

Requisitos mínimos para los procesos de destrucción de distintos tipos de soportes

MEDIOS MAGNÉTICOS

DESTRUCCIÓN (cualquier medio excepto incineración)	
Nivel de confidencialidad BAJO o MEDIO	Disco: al menos 3 pedazos, cada uno con un área máxima de 580 mm^2. Cinta magnética: pedazos con una longitud máxima de 50 mm.
Nivel de confidencialidad ALTO	Disco: al menos 3 pedazos, cada uno con un área máxima de 40 mm^2. Cinta magnética: pedazos con una longitud máxima de 6 mm.
Materias reservadas (información clasificada como SECRETA o RESERVADA)	Disco: al menos 3 pedazos, cada uno con un área máxima de 10 mm^2. Cinta magnética: pedazos con una longitud máxima de 3 mm.
INCINERACIÓN	
Todos los niveles de confidencialidad y grados de clasificación	**Destrucción total**. Se debe realizar en instalaciones con licencia para destrucción de metales o plásticos, con habilitación para realizar estas actividades.

MEDIOS ÓPTICOS

DESTRUCCIÓN (cualquier medio excepto incineración)	
Nivel de confidencialidad BAJO o MEDIO	CD exclusivamente: moler la superficie del disco para suprimir la capa de datos coloreada; o CD o DVD: triturar en pequeños pedazos de área <160 mm^2.
Nivel de confidencialidad ALTO	CD exclusivamente: moler la superficie del disco para suprimir la capa de datos coloreada; o CD o DVD: triturar en pequeños pedazos de área < 36 mm^2.
Materias reservadas (información clasificada como SECRETA o RESERVADA)	CD exclusivamente: moler la superficie del disco para suprimir la capa de datos coloreada; o CD o DVD: triturar en pequeños pedazos de área < 10 mm^2.
INCINERACIÓN	
Todos los niveles de confidencialidad y grados de clasificación	**Destrucción total**. Se debe realizar en instalaciones con licencia para destrucción de metales o plásticos, con habilitación para realizar estas actividades.

MEDIOS BASADOS EN MEMORIAS DE ESTADO SÓLIDO

DESTRUCCIÓN (cualquier medio excepto incineración)	
Nivel de confidencialidad BAJO o MEDIO	Reducir a pedazos el dispositivo, cada uno con un área <160 mm^2.
Nivel de confidencialidad ALTO	Triturar o pulverizar el chip de almacenamiento o el dispositivo de almacenamiento completo, en pedazos de tamaño < 2 mm.
INCINERACIÓN	
Todos los niveles de confidencialidad y grados de clasificación	**Destrucción total**. Se debe realizar en instalaciones con licencia para destrucción de metales o plásticos, con habilitación para realizar estas actividades. Se utilizarán herramientas de alto impacto, mazos, tornillos

	de banco, etc.