Guía sobre **borrado seguro** de la información

Una aproximación para el empresario

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

10 incibe_ 2006-2016

TRABAJANDO POR LA CONFIANZA DIGITAL

Guía sobre **borrado seguro** de la información

Una aproximación para el empresario

INCIBE_PTE_AproxEmpresario_006_BorradoSeguro-2016-v1

índice

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 Introducción

Las empresas, sin importar su tamaño o su sector, basan su actividad en la información: bases de datos, documentos de texto, archivos, imágenes, etc. El ciclo de vida de la información, de forma simplificada, consta de tres fases: generación, transformación y destrucción.

Toda información tiene una vida útil tanto si está formato digital (CD, DVD, Flash USB, discos magnéticos, tarjetas de memoria…) como en formatos tradicionales (papel, microfichas, películas,…). Cuando la vida de los documentos llega a su fin, se deben emplear mecanismos de destrucción y borrado para evitar que queden al alcance de terceros. En esta guía veremos cómo tratar la información digital, y sus soportes, al final de su ciclo de vida.

Ilustración 1: Ciclo de vida de la información

Además entre la información que manejan las empresas hay información crítica que de verse comprometida, destruida o divulgada puede hacer tambalearse o incluso interrumpir el quehacer de la empresa. Son ejemplos de esta información crítica todos los documentos confidenciales y los datos de carácter personal.

Con el borrado y destrucción de soportes de información (discos duros, memorias flash, papel…), no solo se busca proteger la difusión de información confidencial de una organización. También se busca proteger la difusión de datos personales que puedan contener los soportes.

La legislación y normativa actuales [1] hacen que la destrucción segura de información confidencial constituya un acto igual de importante que su correcto almacenamiento o la restricción del acceso a ésta, ya que de lo contrario esos datos confidenciales que han dejado de ser útiles pueden llegar a manos malintencionadas.

Son muchos los casos de sanciones interpuestas por la AEPD por la falta de diligencia en la destrucción de datos personales, que por ejemplo son tirados en lugares públicos (papeleras, contenedores, etc.), que no habían sido debidamente destruidos (triturados, desmagnetizados, sobrescritos, etc.), en la mayoría de los casos documentos impresos, por lo evidentemente llamativo que resulta encontrarse con datos bancarios, médicos, de menores, etc., en una papelera.

En esta guía se resalta la importancia de la gestión de recursos que ya no van a ser utilizados, no sólo buscando el interés propio o no perjudicar a terceros, si no debido también al imperativo legal que así lo ordena. Además se mostrarán los diferentes tratamientos posibles según los soportes de almacenamiento.

«Datos de carácter personal son cualquier información concerniente a personas físicas identificadas o identificables»

En resumen estas son algunas de las situaciones que una correcta destrucción de la información quiere evitar:

- Las **sanciones legales** por incumplimiento de la legislación que regula el tratamiento de la información de carácter personal.
- Los **daños de imagen** derivados de la divulgación de información que debería haberse borrado o de soportes y equipos, con información confidencial, que deberían haberse destruido.
- **Costes de conservación y custodia** más allá del tiempo necesario.
- **Riesgos por robo o uso indebido** de información confidencial.

1.1 La destrucción de los datos de carácter personal

Según la LOPD [1], datos de carácter personal son «cualquier información concerniente a personas físicas identificadas o identificables». Son datos de carácter personal por ejemplo: nombres de usuarios, nombres y apellidos, direcciones postales, números de teléfono, DNI, formación, profesión, números seguridad social, correos electrónicos, firma electrónica, pruebas, diagnósticos y tratamientos médicos, rendimiento deportivo, edad, raza, afiliación política, cuentas en bancos, compras, suscripciones, visitas a páginas web, direcciones IP, uso de los servicios contratados, fotos, grabaciones de audio o videos de cámaras de seguridad, etc.

Son también datos personales la información de identificación personal o PII (*Personally Identifiable Information*) como intereses, gustos, geo-localización, ADN o información biométrica, es decir, toda información que pueda servir para averiguar la identidad, localizar o contactar a una persona o a un individuo a través del contexto.

La Agencia Española de Protección de Datos (AEPD) es la encargada de la protección de los datos de carácter personal. En cuanto a destrucción de información, el Reglamento de Protección de datos de carácter personal [1] menciona:

> *«Art. 92.4 Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.»*

Y más adelante, sobre las copias:

> *«112.2 Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.»*

«Hay empresas que realizan la destrucción del material confidencial según la norma ISO 15713 y emiten un certificado»

1.2 Destrucción certificada

La norma **ISO 15713: 2010 Destrucción segura del material confidencial, código de buenas prácticas** sirve de complemento a la LOPD para la destrucción de documentos que contienen datos personales en cualquier tipo de soporte. También es útil si queremos garantizar la destrucción de datos confidenciales, en el caso de que nos obligáramos a ello por un contrato o acuerdo con otra empresa.

La norma define los requisitos para la gestión y control de recogida, transporte y destrucción del material confidencial. Indica los niveles de destrucción (nivel de triturado) según el tipo de información a eliminar y el soporte (papel, tarjetas SIM y negativos, cintas de audio y video, ordenadores, CD, DVD, microfichas…). Los niveles más altos hacen que la recuperación de la información sea más difícil. Hay empresas (como comentaremos en el apartado de Soluciones del Catálogo [3]) que realizan la destrucción según esta norma y emiten un certificado.

2 Borrado seguro y destrucción de la información

Para finalizar el ciclo de vida de la información desde el enfoque de la seguridad, es indispensable cubrir un aspecto de suma importancia: la destrucción de la información.

Las empresas pueden encontrar diversos motivos para eliminar la información que guardan. Además, son las encargadas de velar por la adecuada gestión de datos personales, estratégicos, legales o contables, entre otros, y están obligadas a conservar estos datos durante un periodo de tiempo, tras el cual se suelen eliminar.

Por ello se recomienda un primer proceso de reflexión interna para analizar la forma en la que eliminan los datos o entregan los dispositivos a terceros (y por tanto, ceden el control de la información).

En el presente capítulo se aborda el planteamiento que debe realizar la empresa en cuanto a la destrucción de información y los métodos de borrado seguro que garantizan la adecuada gestión del ciclo de vida desde el punto de vista de la seguridad de la información.

2.1 Métodos que no destruyen la información de forma segura

Cuando se utilizan métodos de borrado [2] dispuestos por el propio sistema operativo como con la opción «eliminar» o la tecla «Supr» o «Delete», se realiza el borrado exclusivamente en la «lista de archivos»[1] sin que se elimine realmente el contenido del archivo, que permanece en la zona de almacenamiento hasta que se reutilice este espacio con un nuevo archivo.

Por tanto toda aquella acción que no conlleve la eliminación, tanto de la información de la «lista de archivos» como del contenido del mismo, no consigue destruir eficazmente dicha información. De forma específica, no son métodos de destrucción segura:

- Los comandos de borrado del sistema operativo, acceden a la «lista de archivos» y marcan el archivo como suprimido, pero su contenido permanece intacto.

- Al formatear un dispositivo normalmente se sobre-escribe el área destinada a la «lista de archivos» sin que el área de datos donde se encuentra el contenido de los archivos haya sido alterada.

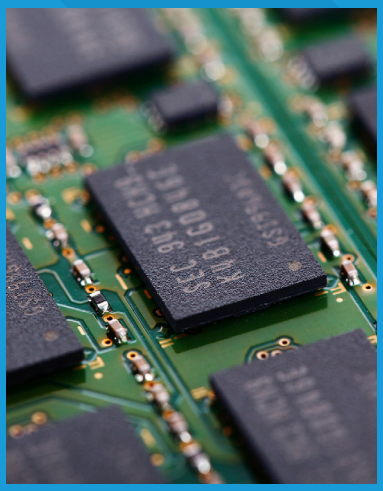
2.2 Métodos de destrucción de la información

Los medios eficaces que evitan completamente la recuperación de los datos contenidos en los dispositivos de almacenamiento son: la desmagnetización, la destrucción y la sobre-escritura en la totalidad del área de almacenamiento de la información.

2.2.1 Desmagnetización

La desmagnetización consiste en la exposición de los soportes de almacenamiento a un potente campo magnético, proceso que elimina los datos almacenados en el dispositivo.

1 La «lista de archivos» es un término genérico que referencia al conjunto de elementos que cada sistema de archivos utiliza para guardar, tanto la información que identifica los archivos (nombre, tipo, fecha de creación, etc.), como un índice que recoge la ubicación física del contenido del mismo.



«La destrucción física es la inutilización del soporte que almacena la información para evitar la recuperación posterior de los datos almacenados»

Este método es válido para la destrucción de datos de los dispositivos magnéticos, como por ejemplo, los discos duros, disquetes, cintas magnéticas de *backup*, etc.

Cada dispositivo, según su tamaño, forma y el tipo de soporte magnético de que se trate, necesita de una potencia específica para asegurar la completa polarización de todas las partículas.

2.2.2 Destrucción física

El objetivo de la destrucción física es la inutilización del soporte que almacena la información en el dispositivo para evitar la recuperación posterior de los datos que almacena. Existen diferentes tipos de técnicas y procedimientos para la destrucción de medios de almacenamiento:

Desintegración, pulverización, fusión e incineración: son métodos diseñados para destruir por completo los medios de almacenamiento. Estos métodos suelen llevarse a cabo en una destructora de metal o en una planta de incineración autorizada, con las capacidades específicas para realizar estas actividades de manera eficaz, segura y sin peligro.

Trituración: las trituradoras de papel se pueden utilizar para destruir los medios de almacenamiento flexibles. El tamaño del fragmento[2] de la basura debe ser lo suficientemente pequeño para que haya una seguridad razonable en proporción a la confidencialidad de los datos que no pueden ser reconstruidos. Los medios ópticos de almacenamiento (CD, DVD, magneto-ópticos) deben ser destruidos por pulverización, trituración de corte transversal o incineración. Cuando el material se desintegra o desmenuza, todos los residuos se reducen a cuadrados de cinco milímetros (5mm) de lado.

Como todo proceso de destrucción física, su correcta realización implica la imposibilidad de recuperación posterior por ningún medio conocido. En el caso de los discos duros se deberá asegurar que los platos internos del disco han sido destruidos eficazmente, no sólo la cubierta externa.

2.2.3 Sobre-escritura

La sobre-escritura consiste en la escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento. Para asegurar la completa destrucción de los datos se debe escribir la totalidad de la superficie de almacenamiento.

La sobre-escritura se realiza accediendo al contenido de los dispositivos y modificando los valores almacenados, por lo que no se puede utilizar en aquellos que están dañados ni en los que no son regrabables, como los CD y DVD.

2.2.4 Ventajas e inconvenientes de los métodos de borrado seguro

Una vez vistos los principales métodos de borrado de información, se aprecia que no ofrecen los mismos resultados. A continuación se

2 La destrucción certificada, es decir con garantías de seguridad y confidencialidad, está normalizada según las normas UNE-EN 15713: 2010 Destrucción segura del material confidencial, código de buenas prácticas y DIN 66399. Se tipifican soportes, métodos de destrucción y niveles de protección y de seguridad. http://solucionestecnologicasparaempresas.com/gestion-de-documentos/la-normativa-vigente-para-la-destruccion-de-documentos/

ofrece un resumen de las principales características observadas en cada uno de estos métodos y los métodos de borrado aplicables en cada dispositivo.

DESTRUCCIÓN FÍSICA	DESMAGNETIZACIÓN	SOBRE-ESCRITURA
✓ Eliminación de forma segura de la información	✓ Eliminación de forma segura de la información	✓ Eliminación de forma segura de la información
✗ Un sistema de destrucción para cada soporte	✗ Una configuración del sistema para cada soporte	✓ Una única solución para todos los dispositivos
✗ Dificultad de certificación del proceso	✗ Dificultad de certificación del proceso	✓ Garantía documental de la operación
✗ Necesidad de transportar los equipos a una ubicación externa	✗ Necesidad de transportar los equipos a una ubicación externa	✓ Posibilidad de eliminación en las propias oficinas
✗ Medidas extraordinarias para garantizar la cadena de custodia	✗ Medidas extraordinarias para garantizar la cadena de custodia	✓ Garantía de la cadena de custodia
✓ Destrucción de dispositivos, no regrabables, ópticos	✗ Sólo válido para dispositivos de almacenamiento magnético	✗ No válido para dispositivos no regrabables ni ópticos
✗ Destrucción definitiva y dificultad de reciclaje de materiales	✗ Tras el proceso el dispositivo deja de funcionar correctamente	✓ Reutilización de los dispositivos con garantías de funcionamiento.

Tabla 1: Comparativa de los métodos de borrado seguro

A continuación se ofrece un resumen del tipo de destrucción más adecuado dependiendo del tipo de soporte.

SOPORTE	TIPO	DESTRUCCIÓN FÍSICA	DESMAGNETIZACIÓN	SOBRE ESCRITURA
Discos Duros	Magnético	✓	✓	✓
Discos Flexibles	Magnético	✓	✓	✓
Cintas de *Backup*	Magnético	✓	✓	✓
CD	Óptico	✓	✗	✗
DVD	Óptico	✓	✗	✗
Blu-ray Disc	Óptico	✓	✗	✗
Pen Drive	Electrónico	✓	✗	✓ [3]
Discos Duros SSD	Electrónico	✓	✗	✓ [3]

Tabla 2: Método de borrado adecuado en función del dispositivo

3 A pesar que actualmente la sobre-escritura es un método seguro de destrucción de datos para dispositivos basados en memorias de estado sólido, diversos trabajos de investigación forense apuntan la posibilidad de recuperación posterior con técnicas de lectura directa de los chips de memoria. Uno de estos estudios es el de la Universidad de California http://nvsl.ucsd.edu/sanitize/.presas.com/gestion-de-documentos/la-normativa-vigente-para-la-destruccion-de-documentos/

3 Política de borrado seguro

Toda empresa debe contar con una política de borrado seguro de la información de los dispositivos de almacenamiento con los que trabaja, que contenga al menos los siguientes elementos:

- Gestión de soportes adecuada:
  - Realizar un seguimiento de los dispositivos que están en funcionamiento, las personas o departamentos responsables, la información contenida en ellos y su clasificación en función del grado de criticidad para el negocio
  - Llevar a cabo la supervisión de los dispositivos que almacenan las copias de seguridad de estos datos
  - Controlar cualquier operación realizada sobre un dispositivo: mantenimiento, reparación, sustitución, etc.
  - En los traslados de los dispositivos de almacenamiento a instalaciones externas a las de la empresa, asegurar que se cumple la cadena de custodia de los mismos, para evitar fugas de información
- Documentación de las operaciones de borrado realizadas:
  - Al seleccionar una herramienta de borrado, elegir aquella que permita la obtención de un documento que identifique claramente que el proceso de borrado se ha realizado, detallando cuándo y cómo ha sido realizado
  - En el caso de que la destrucción lógica no se realice correctamente por fallo del dispositivo, este hecho debe documentarse claramente y utilizar métodos de destrucción física de dicho soporte, asegurando que se realice de forma respetuosa con el medio ambiente

«Toda empresa debe contar con una política de borrado seguro de la información de los dispositivos de almacenamiento con los que trabaja»

4 Soluciones en el Catálogo

El Catálogo de INCIBE [3] recoge las soluciones de seguridad, productos y servicios, que están disponibles en el mercado español. En el caso del **almacenamiento y borrado seguro,** los **productos** están registrados fundamentalmente dentro de las categorías y subcategorías:

- **Cumplimiento legal:**
  - **Herramientas de Cumplimiento legal** (LOPD, LSSI, etc.). Estas herramientas permiten el cumplimiento con la legislación en materia de seguridad de la información. Se encuentra la LOPD (Ley Orgánica de Protección de Datos), LSSI (Ley de Servicios de la Sociedad de la información), LPI (Ley de Propiedad Intelectual), etc.
  - **Borrado seguro.** Son herramientas que permiten realizar la eliminación de archivos, carpetas o unidades lógicas de forma segura.
  - **Destrucción documental.** Son herramientas destinadas a la destrucción de datos confidenciales y documentos.
- **Prevención de fuga de información:**
  - **Gestión del ciclo de vida de la información** *(ILM: Information Life Cicle)*. Son herramientas que permiten gestionar el ciclo completo de vida de la información, implementando políticas y mecanismos para garantizar el nivel de confidencialidad de la información.

En cuanto a los **servicios** registrados para almacenamiento y borrado seguro se encuentran principalmente bajo las categorías de:

- **Contingencia y continuidad:**
  - **Gestión del ciclo de vida de la información.** Son soluciones que permiten gestionar el ciclo completo de vida de la información, implementando políticas y mecanismos para garantizar el nivel de confidencialidad de la información.
- **Cumplimiento legal:**
  - **Adaptación a la legislación** (implantación). Son servicios destinados a llevar a cabo la adecuación de las empresas y organizaciones a la legislación aplicable, llevando a cabo la implantación de las medidas de tipo jurídico, técnico y organizativo.
  - **Auditoría de legislación.** Son servicios destinados a la realización de auditorías de nivel de cumplimiento de la legislación aplicable a una empresa u organización, con el fin de determinar y analizar si la empresa ha adoptado los cambios según la legislación.
  - **Borrado seguro.** Son servicios que permiten realizar la eliminación de archivos, carpetas o unidades lógicas de forma segura según la normativa vigente.
  - **Destrucción documental.** Son servicios destinados a la destrucción de datos confidenciales y documentos, con el fin de evitar sanciones administrativas por incumplimiento con la legislación.

5 Bibliografía

[1] BOE, Normas consolidadas. Protección de datos de carácter personal https://www.boe.es/legislacion/codigos/codigo.php?id=55&modo=1&nota=0&tab=2

[2] Incibe – Blog – Infografía ¿Borrar los datos de manera definitiva? ¡Aprende cómo! https://www.incibe.es/protege-tu-empresa/blog/borrar-informacion-dispositivo-ciberseguridad

[3] Incibe – Empresas – Catálogo https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL