# BORRADO SEGURO Y GESTIÓN DE SOPORTES

## POLÍTICAS DE SEGURIDAD PARA LA PYME

Colección

**PROTEGE TU EMPRESA**

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

# ÍNDICE

**1. Borrado seguro y gestión de soportes ..... 03**

1.1. ANTECEDENTES ..... 03

1.2. OBJETIVOS ..... 04

1.3. CHECKLIST ..... 04

1.4. PUNTOS CLAVE ..... 06

**2. REFERENCIAS ..... 08**

# 1. BORRADO SEGURO Y GESTIÓN DE SOPORTES

## 1.1 ANTECEDENTES

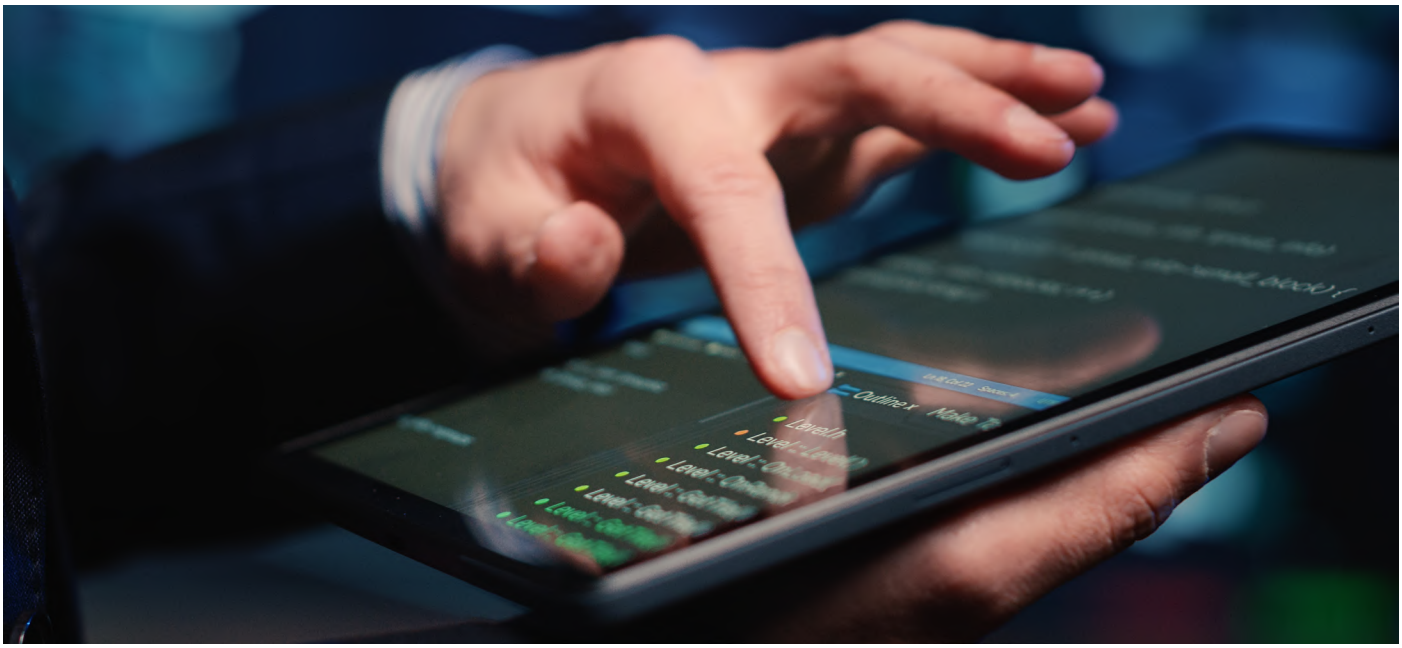
Cuando la información deja de ser necesaria para la organización llega a la última fase de su ciclo de vida y es necesario destruirla de forma segura. Esta opción es indispensable si queremos que la información no vuelva a ser accesible y cumplir con la legislación y normativa actuales **[1]**.

También debemos utilizar el borrado seguro cuando queremos:

- **Reutilizar un soporte:** Que ya contiene datos corporativos y que no funciona correctamente.
- **Deshacernos de un soporte** que se ha quedado obsoleto.

En el caso de que la información esté en soportes no electrónicos (papel, negativos fotográficos, radiografías, cintas magnéticas, etc.) es necesario usar la una trituradora para deshacernos de la información. En caso contrario podría llegar a manos de terceros y utilizarse de forma perjudicial para la empresa.

Por otro lado, si vamos a contratar a terceros la destrucción de nuestros datos o de los soportes, debemos elegir la destrucción certificada si se trata de (o si contienen) datos personales o confidenciales. Esta opción nos asegura la destrucción de la información con las máximas garantías de seguridad y confidencialidad, desde la recogida del material documental hasta su destrucción física y eliminación final.



## 1.2 OBJETIVOS

Establecer normas para el borrado seguro de la información obsoleta y para destrucción de soportes acorde a las necesidades de la empresa [2].

## 1.3 CHECKLIST

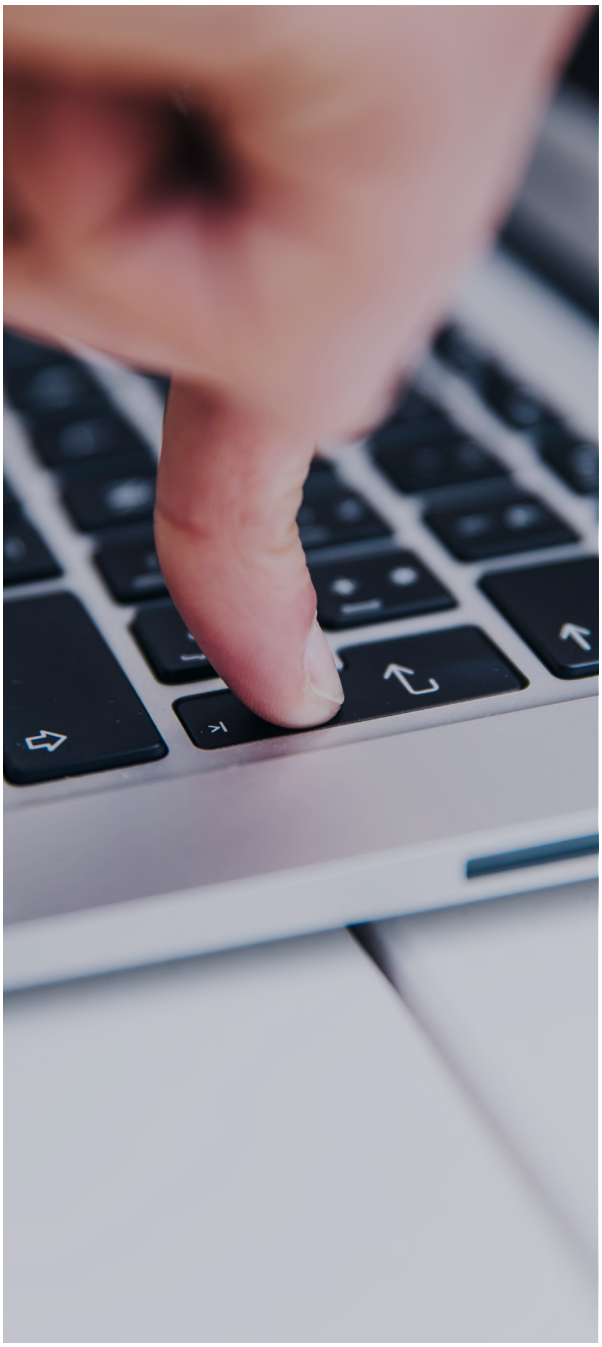
A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a **borrado seguro y gestión de soportes**.

Los controles se clasificarán en dos niveles de **complejidad**:

- **Básico (B):** el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- **Avanzado (A):** el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente **alcance**:

- **Procesos (PRO):** aplica a la dirección o al personal de gestión.
- **Tecnología (TEC):** aplica al personal técnico especializado.
- **Personas (PER):** aplica a todo el personal.



# 1.3 CHECKLIST

| Nivel | Alcance | Control | |
|---|---|---|---|
| B | PRO | **Inventario de activos.** Realizas 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. | ☐ |
| B | PRO/TEC | **Gestión de soportes.** Supervisas los dispositivos que almacenan información corporativa, en particular aquellos que se utilizan para realizar copias de seguridad, documentando cualquier operación realizada sobre los mismos: mantenimiento, reparación, sustitución, etc. | ☐ |
| B | PER | **Cadena de custodia.** Aseguras que se cumple la cadena de custodia en los traslados de los dispositivos de almacenamiento a instalaciones externas a las de la empresa. | ☐ |
| A | PRO/TEC | **Eliminación de la información en soportes no electrónicos.** Utilizas el proceso de triturado para destruir la información de los soportes no electrónicos (papel y soportes magnéticos). | ☐ |
| A | PRO/TEC | **Eliminación de la información para la reutilización de soportes electrónicos.** Optas por el proceso de sobrescritura cuando quieres reutilizar un soporte todavía en buen estado. | ☐ |
| A | PRO/TEC | **Eliminación de la información antes de deshacernos de soportes electrónicos.** Usas el proceso de desmagnetización o de destrucción física antes de desechar el soporte de almacenamiento. | ☐ |
| A | PRO/TEC | **Borrado de información en otros dispositivos.** Eliminas la información en teléfonos móviles, impresoras, GPS, etc. (memoria y tarjetas) antes de deshacernos de ellos. | ☐ |
| A | TEC | **Documentación de las operaciones de borrado realizadas.** Eliges una herramienta de borrado 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. | ☐ |
| A | TEC | **Destrucción certificada.** Utilizas un servicio de destrucción certificada para garantizar la destrucción de datos confidenciales o para cumplir un acuerdo con otra empresa o con la LOPDGDD. | ☐ |

**Revisado por:** _____ **Fecha:** _____

# 1.4 PUNTOS CLAVE

Los puntos clave de esta política son:

- **Inventario de activos.** Tendremos que realizar un seguimiento de los dispositivos que están en funcionamiento (CD, DVD, memorias USB, discos magnéticos, tarjetas de memoria...), las personas o departamentos responsables de esos dispositivos, la información contenida en ellos y su clasificación en función del grado de criticidad para el negocio. También se deberán anotar las veces que el dispositivo ha sufrido un borrado seguro (si es un dispositivo que lo permite), ya que son muy agresivos y el abuso de estos borrados pueden dañar el dispositivo, así como indicar el tipo de borrado que se ha realizado en cada ocasión y el algoritmo de borrado utilizado.
- **Gestión de soportes.** Supervisaremos los dispositivos que almacenan información corporativa, en particular los que se usan para realizar las copias de seguridad, documentando cualquier operación realizada sobre los mismos: mantenimiento, reparación, sustitución, etc.
- **Cadena de custodia.** En los traslados de los dispositivos de almacenamiento a instalaciones externas a las de la empresa se ha de asegurar que se cumple la cadena de custodia de los equipos para evitar la sustracción, pérdida o acceso indebido a la información.
- **Eliminación de la información [3].**
  - **En soportes no electrónicos y soportes magnéticos:**
    - Para eliminar la información que ya no se considera necesaria para la organización en este tipo de soportes (documentos impresos, CD, DVD, memorias USB, cintas magnéticas, radiografías, etc.) debemos utilizar la opción de la destrucción física (desintegración, pulverización, fusión, incineración o trituración) o la desmagnetización como modo seguro de eliminación.
  - **Para la reutilización de soportes electrónicos:**
    - Si queremos **reutilizar un soporte** que ya contiene datos, debemos utilizar la opción de sobrescritura para garantizar un borrado total de la información. Para asegurar la completa destrucción de los datos, se deberá sobrescribir la totalidad de la superficie de almacenamiento. La sobrescritura se puede utilizar en todos los dispositivos regrabables (discos duros, pendrives o memorias USB, etc.) siempre que el dispositivo no esté dañado.
    - Si queremos **reutilizar un dispositivo**, pero no va a ser asignado por el momento, podemos realizar un borrado criptográfico. Consiste en cifrar la información con una clave muy compleja que nadie va a memorizar, por lo que la información se da por perdida. Cuando el dispositivo vaya a ser utilizado de nuevo se realizará un borrado simple, ya que, aunque se lograse recuperar esa información, no se podría descifrar sin la clave.

# 1.4 PUNTOS CLAVE

- **Antes de deshacernos de los soportes electrónicos:**

  • Cuando queramos desechar algún soporte de almacenamiento porque ya no funcione o porque se haya quedado obsoleto, debemos utilizar los métodos de desmagnetización o destrucción física. Cualquiera de estos dos métodos imposibilita la reutilización del dispositivo.

- **Prestar una especial atención** cuando queramos deshacernos de dispositivos móviles (smartphones, tabletas, etc.) y dispositivos que almacenan información de uso (impresoras, GPS, etc.) ya que también pueden contener información empresarial confidencial **[4]**.

- **Documentación de las operaciones de borrado realizadas.** Al seleccionar una herramienta de borrado, elegiremos 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. Para ello, hay que basarse en la ISO 15713:2010, que indica cómo proceder a la hora de emitir un certificado de borrado para justificar una destrucción certificada.

- **Destrucción certificada**. Existe la opción de contratar una empresa que realice una destrucción certificada. Esta empresa se encargará de llevar a cabo el proceso de eliminación de la información garantizando la gestión y control de recogida, transporte y destrucción del material confidencial. Después de llevar a cabo la destrucción, la empresa emite un certificado que garantiza la validez de todo el proceso.

  Esta alternativa es muy útil si queremos **garantizar la destrucción de datos confidenciales** (cumpliendo la LOPDGDD) y en el caso de que nos viéramos obligados a ello por un contrato o acuerdo con otra empresa.

# 2. REFERENCIAS

**[1] BOE – Ley de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) –** https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

**[2] INCIBE – Empresas – Blog – Si la información ya no es necesaria, bórrala de forma segura–** https://www.incibe.es/empresas/blog/si-informacion-no-necesaria-borrala-forma-segura

**[3] INCIBE – Empresas – Blog – La eliminación de datos forma parte de la protección de la información –** https://www.incibe.es/empresas/blog/eliminacion-datos-forma-parte-proteccion-informacion

**[4] INCIBE – Empresas – Blog – ¿Sabes qué hacer antes de desechar tu dispositivo móvil?–** https://www.incibe.es/empresas/blog/sabes-hacer-desechar-tu-dispositivo-movil


Financiado por
la Unión Europea
NextGenerationEU


GOBIERNO
DE ESPAÑA
MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL


Plan de
Recuperación,
Transformación
y Resiliencia


incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD


protege
tuempresa