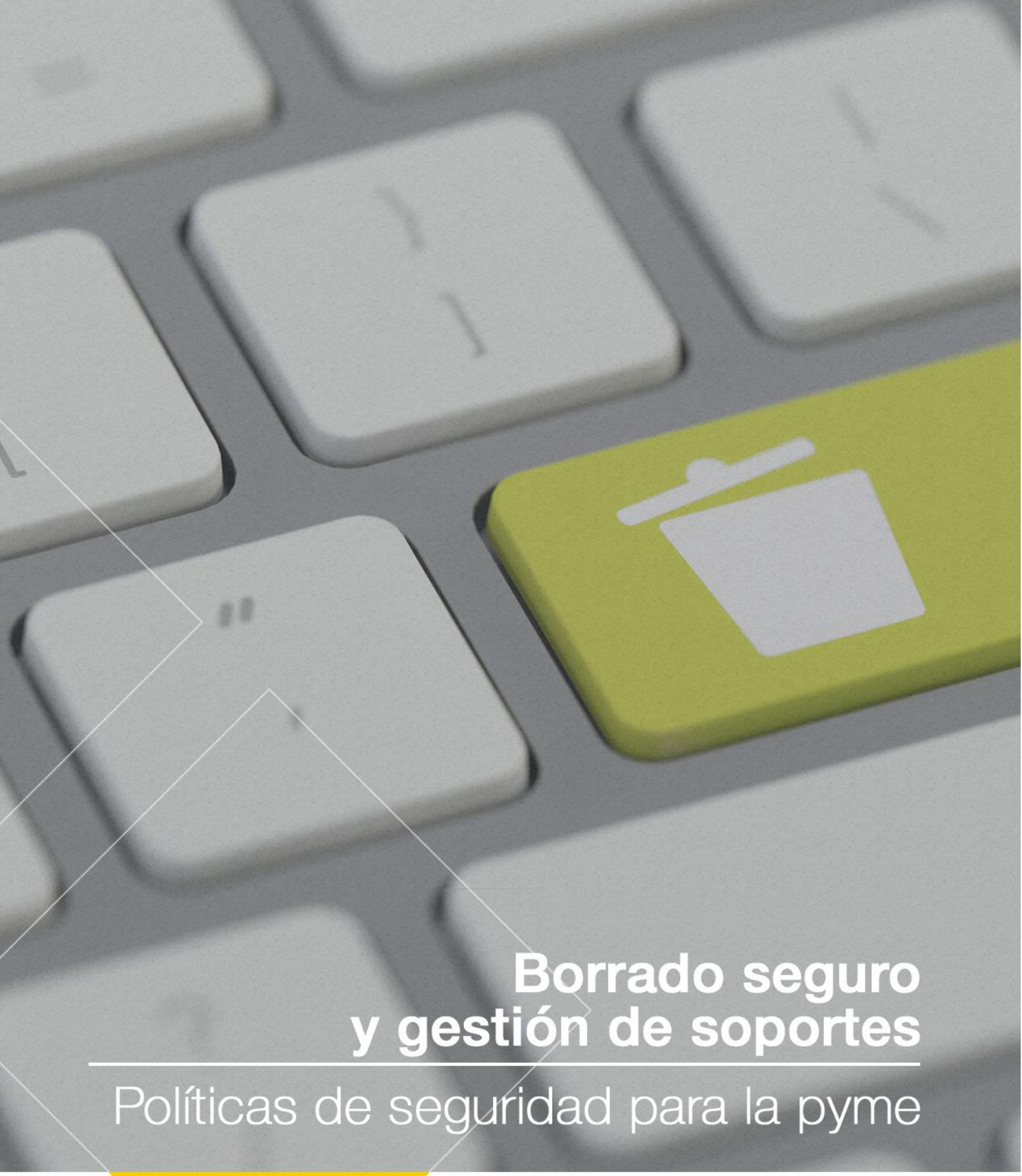

Borrado seguro y gestión de soportes

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. Borrado seguro y gestión de soportes 3

1.1. Antecedentes 3
1.2. Objetivos 3
1.3. Checklist 4
1.4. Puntos clave 6

2. Referencias 8

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 Ley de Protección de Datos [1], cuando contenga datos de carácter personal.

También debemos utilizar el borrado seguro cuando queremos:

- reutilizar un soporte:
  - que ya contiene datos corporativos;
  - que no funciona correctamente;
- o 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.

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.	☐
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.	☐

NIVEL	ALCANCE	CONTROL	
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 el RGPD.	☐

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, Flash 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.
- **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.
- **Eliminación de la información:**
  - 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, cintas magnéticas, radiografías, etc.) debemos utilizar la opción de triturado 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. La sobrescritura se puede utilizar en todos los dispositivos regrabables (discos duros, pendrives o pinchos USB, etc.) siempre que el dispositivo no esté dañado.
  - Antes de deshacernos del soportes electrónicos:
    - Cuando queremos 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.
- **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.
- **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 normativa del RGPD) y en el caso de que nos viéramos obligados a ello por un contrato o acuerdo con otra empresa.

2. REFERENCIAS

[1]. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo · https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=es

[2]. Incibe – Protege tu empresa – Blog – Borrado seguro de la información: una guía de aproximación para el empresario · https://www.incibe.es/protege-tu-empresa/guias/borrado-seguro-informacion-aproximacion-el-empresario

[3]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Copias de seguridad https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[4]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Protección del puesto de trabajo https://www.incibe.es/protege-tu-empresa/herramientas/politicas

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

[6]. Incibe – Protege tu empresa – Blog – Borrado y destrucción segura de soportes de información · https://www.incibe.es/protege-tu-empresa/blog/borrado-destruccion-segura-soportes

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD