

Guía para el Borrado Seguro de Datos Personales

Para la protección de los datos personales a lo largo de su ciclo de vida, así como en general de cualquier información que represente un activo para CONSAR, es importante contar con una medida de seguridad que permita minimizar el efecto de cualquier tipo de recuperación no autorizada.

Por lo tanto:

**Borrado
Seguro**



Es la medida de seguridad mediante la cual se establecen métodos y técnicas para la eliminación definitiva de los datos personales.

Finalidad

La probabilidad de recuperarlos sea mínima.

Es de cumplimiento legal: principio de Calidad y el deber de Seguridad.

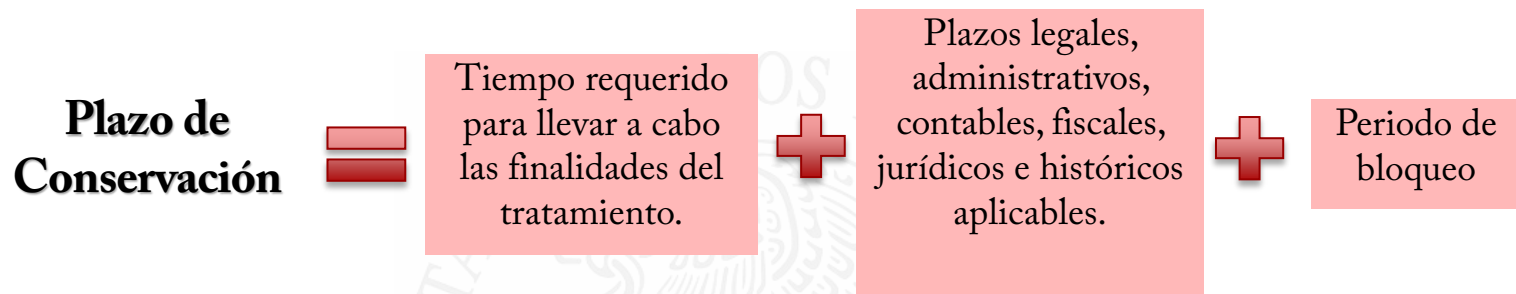


Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Con independencia de que el titular ejerza su derecho de cancelación, CONSAR está obligado a eliminar, de oficio, los datos personales cuando hayan dejado de ser necesarios para la finalidad para la cual se obtuvieron.



El momento indicado para eliminar los datos personales depende del plazo de conservación de los mismos, de acuerdo a las disposiciones legales que correspondan.



*Puede coincidir los tres plazos

Bloqueo:

“La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponde.” *Fracción IV, Art.3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*


A falta del Borrado Seguro de los medios de almacenamiento el escenario de riesgo implica:

Una alta probabilidad de que se materialice el riesgo, es decir, que una persona utilice técnicas de recuperación de información, para obtener datos personales de los medios de almacenamiento desechados o reutilizados por CONSAR.


Puede ocasionar daño económico o moral tanto a los titulares de los datos personales como a la organización.

Para mitigar dicho riesgo, se deberán implementar técnicas de borrado seguro.





Representa una medida de seguridad efectiva para minimizar fugas y/o el mal uso de los datos personales por parte de una persona mal intencionada o no autorizada.



Se optimizan los espacios y los procesos, en particular con la eliminación periódica de los denominados “archivos muertos”.



Se previenen las afectaciones económicas y de imagen debido a multas y/o compensación de daños.

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES



Promueve la adopción de un Sistema de Gestión de Seguridad de Datos Personales (SGSDP).*

Su implementación proporciona varias ventajas que permiten un mejor aprovechamiento respecto de la simple ejecución de métodos de borrado seguro.

- Definir alcances, objetivos y políticas, en el tratamiento.
- Tener un inventario de los datos personales en los sistemas de tratamiento.
- Gestionar los medios de almacenamiento.
- Establecer plazos de conservación de los datos personales y de los medios de almacenamiento.
- Visión de las responsabilidades legales y contractuales que se tienen sobre el resguardo y eliminación de los medios de almacenamiento.
- Contar con revisiones y auditorías para validar los procesos de borrado seguro.
- Documentar los procesos que requieran borrado seguro.

*Recomendaciones en materia de seguridad de datos personales publicadas en el DOF, el 30 de octubre de 2013
http://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013

CONSAR 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, y la información contenida en ellos.
- 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, entre otros.
- En los traslados de los dispositivos de almacenamiento a instalaciones externas a CONSAR, asegurar que se cumple la cadena de custodia de los mismos, para evitar fugas de información.

Documentación de las operaciones de borrado



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.

MEDIOS DE ALMACENAMIENTO

Para definir los métodos de borrado, es necesario establecer si los datos personales se almacenan en un medio de almacenamiento:

Físico



Es todo recurso inteligible a simple vista y con el que se puede interactuar sin la necesidad de ningún aparato que procese su contenido para examinar, modificar o almacenar datos personales.



- Archiveros
- Gavetas/cajones
- Bodegas
- Estantes
- Carpetas
- Documentos

Electrónico

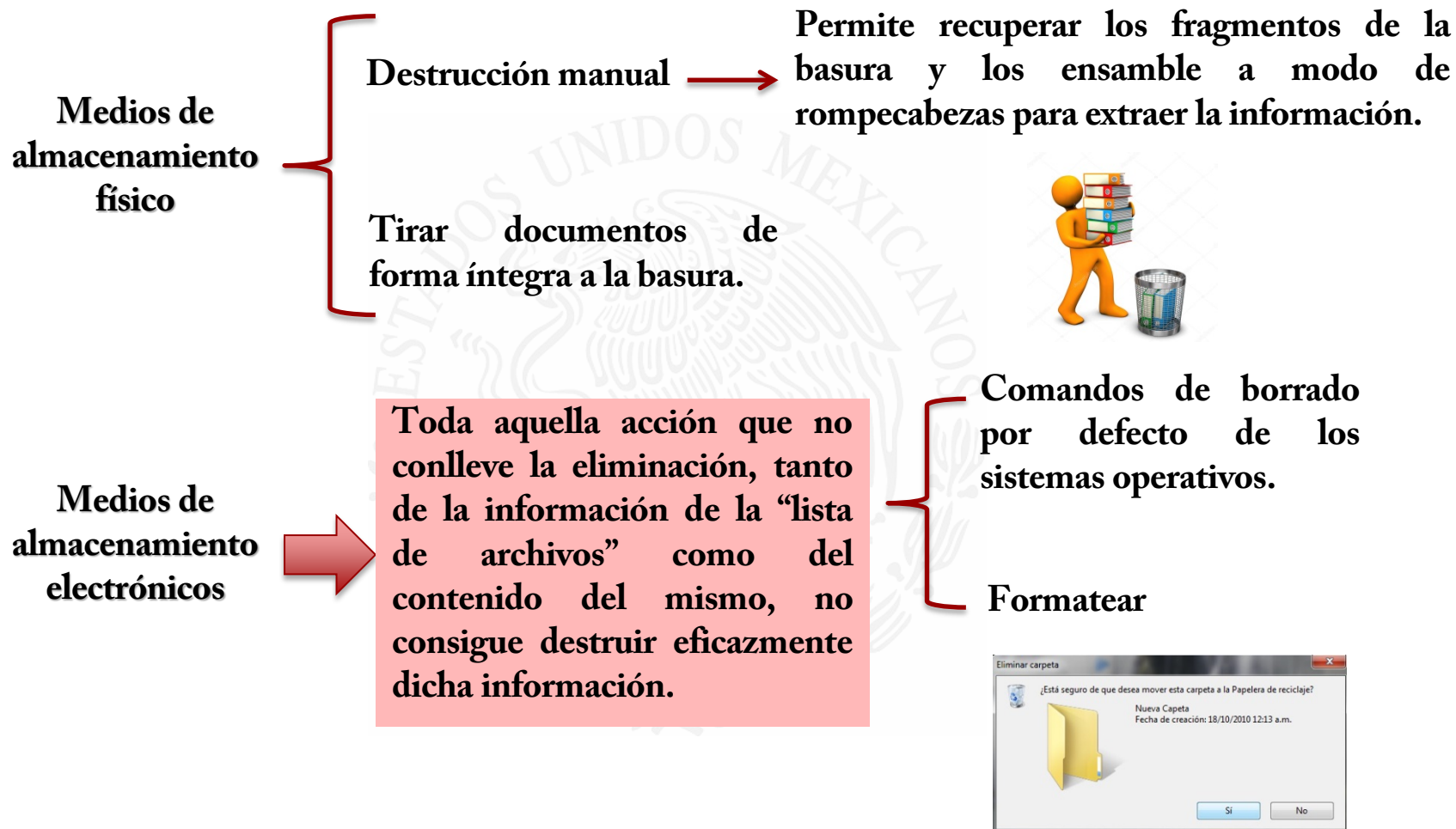


Es todo recurso al que se puede acceder sólo mediante el uso de un equipo de computo que procese su contenido para examinar, modificar o almacenar los datos personales.

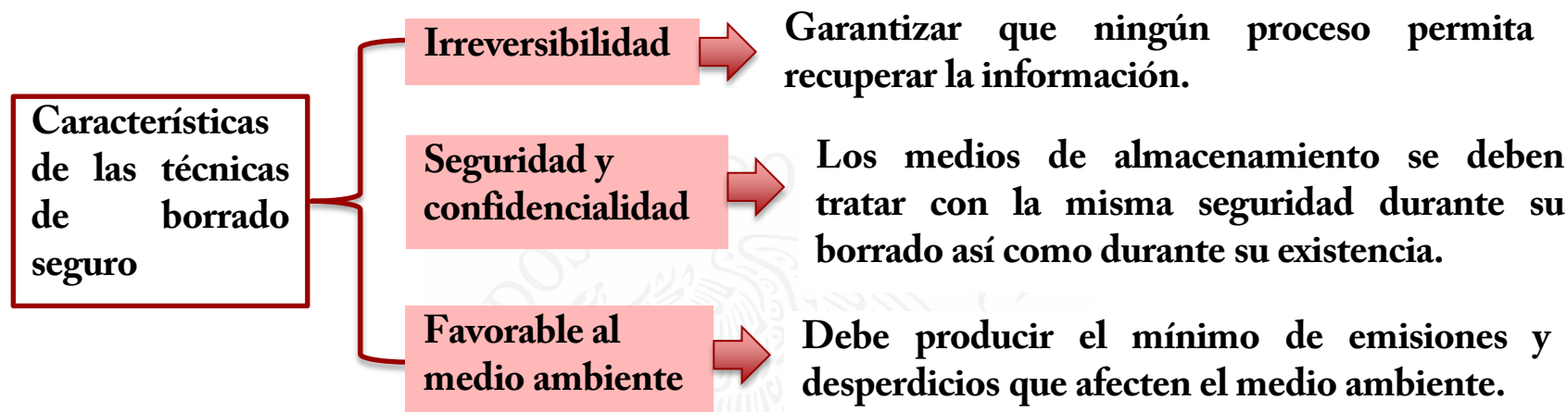


- Medio magnético
- Medio óptico
- Medio magnético-óptico
- Medio en estado sólido
- Medio de almacenamiento en la nube

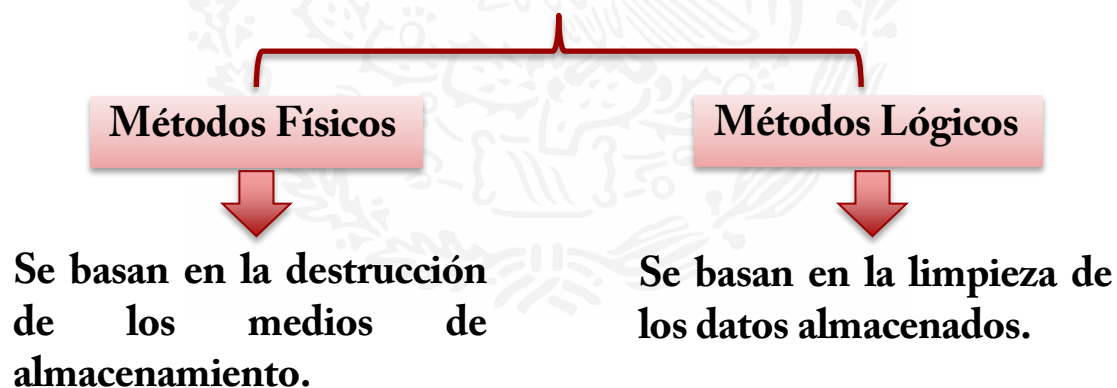
MÉTODOS QUE NO BORRAN DE FORMA SEGURA LOS DATOS PERSONALES



MÉTODOS DE BORRADO SEGURO



Métodos para el Borrado Seguro de los Datos Personales



MÉTODOS FÍSICOS DE BORRADO

Aquellos que implican un daño irreversible o la destrucción total de los medios de almacenamiento.

Destrucción de los medios de almacenamiento físico.

- Trituración
- Incineración
- Químicos

Destrucción de los medios de almacenamiento electrónico.

- Desintegración
- Trituración o pulverización
- Abrasión
- Fundición o fusión

Trituración

Las principales características a considerar de una trituradora son el tipo y tamaño de corte o “partícula”, así como su capacidad.

Considerando el tipo de corte existen dos tipos de trituradoras.

En línea recta o tiras. Se recomienda usar el corte en tiras de 2 mm de ancho o menos.

En corte cruzado o en partículas.

De acuerdo con lo anterior, se sugiere contemplar el riesgo inherente de los datos personales en los sistemas de tratamiento.

Categorías para los sistemas de tratamiento de datos personales según su riesgo inherente.

Nivel estándar

Información de identificación, contacto, datos laborales y académicos.

Nivel Sensible

Datos que permiten conocer la ubicación física de la persona o aquellos que permitan inferir el patrimonio de una persona.

Nivel Especial

Datos cuya naturaleza única, o bien debido a un cambio excepcional en el contexto de las operaciones usuales de CONSAR, puedan causar daño directo a los titulares.

**Las categorías antes descritas son sólo una orientación*

Incineración

No es muy recomendable por cuestiones del medio ambiente, sin embargo, es una opción segura siempre y cuando se valide que el activo se redujo a cenizas.

Químicos

Es posible destruir por medio de químicos, sin embargo, no es recomendable por temas ecológicos.

Desintegración

Separación completa o pérdida de la unión de los elementos que conforman algo, de modo que deje de existir.

Trituración o pulverización

Procedimiento mediante el cual un cuerpo sólido se convierte en pequeñas partículas.

Abrasión

Acción de arrancar, desgastar o pulir algo por rozamiento o fricción.

Fundición o fusión

Paso de un cuerpo del estado sólido al líquido por la acción del calor.

COMPARACIÓN ENTRE LOS MÉTODOS FÍSICOS

Técnica	Ventajas	Desventajas
Medios de almacenamiento físico		
Trituración	<ul style="list-style-type: none"> • Hay trituradoras de oficina a un bajo costo. • La destrucción de documentos puede hacerse en las instalaciones de la organización. • No siempre se requiere contratar a un proveedor externo. • Los documentos triturados pueden ser reciclados. 	<ul style="list-style-type: none"> • No prevé la generación de informes del proceso de borrado necesarios para demostrar el cumplimiento normativo. Es necesario generar evidencia de la destrucción, por ejemplo con certificados, actas, fotografías y bitácoras de la destrucción. • Si no se tritura la información de forma adecuada, ésta puede ser recuperada.
Incineración	<ul style="list-style-type: none"> • Los datos son totalmente irrecuperables. 	<ul style="list-style-type: none"> • Daña el medio ambiente. • No prevé la generación de informes del proceso de borrado necesarios para demostrar el cumplimiento normativo. Es necesario generar evidencia de la destrucción, por ejemplo con certificados, actas, fotografías y bitácoras de la destrucción. Puede resultar peligroso.

Técnica	Ventajas	Desventajas
Medios de almacenamiento físico		
Uso de químicos	<ul style="list-style-type: none"> Los datos son totalmente irrecuperables. 	<ul style="list-style-type: none"> Daña el medio ambiente. No prevé la generación de informes del proceso de borrado necesarios para demostrar el cumplimiento normativo. Es necesario generar evidencia de la destrucción, por ejemplo con certificados, actas, fotografías y bitácoras de la destrucción. Puede resultar peligroso.
Medios de almacenamiento electrónico		
Destrucción	<ul style="list-style-type: none"> Proporciona la máxima seguridad de destrucción absoluta de los datos. 	<ul style="list-style-type: none"> Implica métodos industriales de destrucción. Implica costos de transportación de los dispositivos. El dispositivo deja de ser utilizable. Al ser generalmente una subcontratación, se debe gestionar la entrega de evidencia de la destrucción, por ejemplo con certificados, actas, fotografías y bitácoras de la destrucción.

MÉTODOS LÓGICOS DE BORRADO

Aquellos que implican la sobre-escritura o modificación del contenido del medio de almacenamiento electrónico.

Desmagnetización

Este método expone a los dispositivos de almacenamiento a un campo magnético a través de un dispositivo por lo que el hardware donde se encuentra la información se vuelva inoperable.

Se considera más segura ya que altera directamente el contenido de información.

Sobre-escritura

Consiste en escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.

Cifrado de medios

Cuando un archivo electrónico o medio de almacenamiento se encuentra cifrado, es posible aplicar el denominado “borrado criptográfico” para borrar únicamente las claves que se utilizaron para cifrar el medio de almacenamiento o archivo.

COMPARACIÓN ENTRE LOS MÉTODOS LÓGICOS

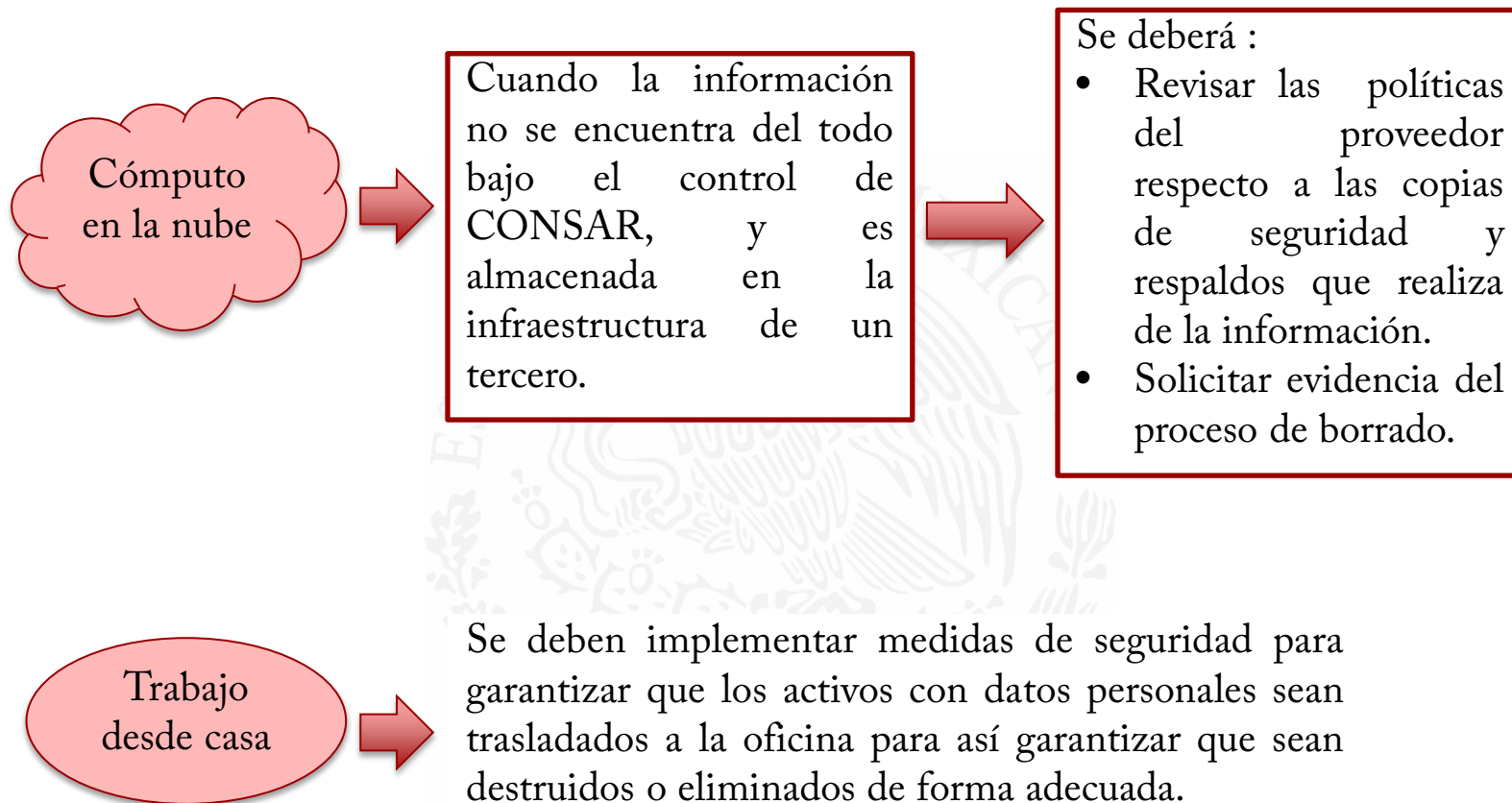
Técnica	Ventajas	Desventajas
Desmagnetización	<ul style="list-style-type: none"> • Hace que los datos sean totalmente irrecuperables. • Es un método rápido. • Permite la eliminación de información aunque el soporte se encuentre dañado. 	<ul style="list-style-type: none"> • Implica costos para transportar dispositivos a donde se encuentre el desmagnetizador. • El dispositivo deja de ser utilizable. • Dificultad para verificar borrado de datos. • Dificultad para calcular la potencia requerida para borrar cada equipo. • No prevé la generación de informes del proceso de borrado necesarios para demostrar el cumplimiento normativo. • Suele requerir un desmagnetizador por cada tipo de soporte. • Se debe tener cuidado para evitar daños a equipos magnéticos cercanos. • Personas con ciertas condiciones médicas o que tienen marcapasos deben permanecer alejados. • Al ser generalmente una subcontratación, se debe gestionar la entrega de evidencia de la destrucción, por ejemplo con certificados, actas, fotografías y bitácoras de la destrucción.

Técnica	Ventajas	Desventajas
Sobre-escritura	<ul style="list-style-type: none"> • Facilidad para comprobar la eliminación de la información. • Se puede hacer en las instalaciones de la organización. • Permite la reutilización de dispositivos. • Bajo costo. • Prevé la generación de informes del proceso de borrado necesarios para demostrar el cumplimiento normativo. 	<ul style="list-style-type: none"> • No se puede utilizar en dispositivos dañados. • No se puede utilizar en dispositivos que no sean regrabables. • No sirve en discos con funciones de gestión de almacenamiento avanzadas.

MEDIOS DE ALMACENAMIENTO Y SUS RESPECTIVOS MÉTODOS

Medio de almacenamiento	Tipo de medio	Método de borrado seguro
Medio de almacenamiento físico	<ul style="list-style-type: none"> • Archiveros • Gavetas • Bodegas • Estantes • Oficinas 	<ul style="list-style-type: none"> • Trituración • Incineración • Uso de químicos
Magnético	<ul style="list-style-type: none"> • Disco duro • Disco duro externo o portátil • Cintas magnéticas 	<ul style="list-style-type: none"> • Sobre-escritura • Desmagnetización • Destrucción física
Óptico (dispositivos regrabables)	<ul style="list-style-type: none"> • CD-RW / DVD-RW • Blu-Ray regrabable (BDRE) 	<ul style="list-style-type: none"> • Sobre-escritura • Destrucción física
Magneto-óptico	<ul style="list-style-type: none"> • Disco magneto-óptico • MiniDisc • HI-MD 	<ul style="list-style-type: none"> • Sobre-escritura • Destrucción física
Estado sólido	<ul style="list-style-type: none"> • Pendrive / USB • Tarjetas de memoria (Flashdrive) • Dispositivo de estado Sólido 	<ul style="list-style-type: none"> • Sobre-escritura • Destrucción física

CONSIDERACIONES ADICIONALES



El método de borrado adecuado dependerá:

Volumen

Tipo de datos personales

Presupuesto

Factores para determinar si el proceso debe realizarse de manera local o a través de la contratación de un tercero.

Volumen de datos personales

Tamaño de la organización

Tomar en cuenta:

Sin importar si el borrado seguro se hace dentro de la organización o través de una subcontratación, se debe administrar la generación de evidencia de dicho proceso, a fin de que ante un procedimiento del INAI se pueda demostrar el cumplimiento.

Guía para el Borrado Seguro de Datos Personales