GUÍA DE BORRADO SEGURO DE LOS DATOS PERSONALES

COMITÉ DE TRANSPARENCIA
OFICIAL DE PROTECCIÓN DE DATOS PERSONALES
enero de 2023

GUÍA DE BORRADO SEGURO DE LOS DATOS PERSONALES

PRESENTACIÓN

El presente documento tiene como finalidad orientar a las personas que colaboran con el Partido del Trabajo, y que tienen bajo su resguardo datos personales, sobre la importancia de eliminarlos de manera segura cuando éstos hayan dejado de ser necesarios para el cumplimiento de las finalidades para los cuales fueron recabados, acorde a lo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados -LGPDPPSO- y con base en la Guía de Borrado Seguro publicada en

http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf

IMPORTANCIA DE LA DESTRUCCIÓN SEGURA

Una vez que los datos personales tratados han llegado al final de su vida útil, deben ser eliminados o destruidos bajo técnicas seguras de borrado que garanticen que los datos fueron borrados o eliminados de los sistemas de datos personales en su totalidad y que los mismos no pueden ser recuperados ni utilizados de manera indebida.

Se deben considerar los plazos de conservación, los cuales se fijan a partir de las disposiciones legales aplicables en la materia de que se trate; los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información, y el periodo de bloqueo.

Plazo de conservación

= Tiempo requerido para llevar a cabo las finalidades del tratamiento
+ Plazos legales, administrativos, contables, fiscales, jurídicos e históricos aplicables, de conformidad con el Catálogo de Disposición Documental del Partido del Trabajo (CADIDO).
+ Periodo de bloqueo

Es importante mencionar que existen métodos de borrado no seguro, ya que es posible invertir el proceso para recuperar de manera parcial o total los datos personales, por ejemplo:

- Romper archivos y documentos a mano, con tijeras o rasgarlos, permite que una persona pueda recuperarlos y extraer información importante.
- Utilizarlos como papel de reciclaje o arrojarlos íntegros a la basura es una conducta aún más riesgosa.
- Utilizar comandos como “borrar”, “eliminar” o “formatear”, permite que los archivos puedan ser recuperados con la utilización de *software* que en su mayoría puede ser gratuito.

MEDIOS DE ALMACENAMIENTO

Los datos personales tratados[1] pueden almacenarse de forma física o electrónica en función de su ciclo de vida y de su valor, tomando en consideración que no todos puede ser tratada de la misma manera, además, los medios donde se almacenan deben contar con medidas de seguridad que garanticen su confidencialidad, disponibilidad e integridad durante el periodo que sea necesario, por lo que los dispositivos de almacenamiento constituyen una parte vital de cualquier sistema de protección de datos personales.

MEDIOS DE ALMACENAMIENTO FÍSICO

Es todo recurso con el que se puede interactuar a simple vista, sin la necesidad de ningún aparato que procese su contenido para examinar, modificar o almacenar datos personales, por ejemplo: archiveros, gavetas, cajones, bodegas, estantes, oficinas, carpetas, entre otros. En este caso, la técnica de destrucción a utilizar debe estar enfocada a la destrucción del documento y no al medio de almacenamiento.

MEDIOS DE ALMACENAMIENTO ELECTRÓNICO

Es todo recurso al que se puede acceder sólo mediante el uso de un equipo de cómputo que procese su contenido para examinar, modificar o almacenar los datos personales, por ejemplo: discos duros, *USB, CD, Blu-Ray*, tarjetas de memoria, servicios de almacenamiento en la nube, entre otros.

Medio magnético: Los métodos de destrucción de este tipo de dispositivos se enfocarán en la posibilidad de sobrescribir información o en la destrucción total del dispositivo.

- Disco Duro conector USB o *FireWire*

Medio óptico: Las ralladuras pueden ocasionar la pérdida de los datos y la información ya no puede leerse, por lo que pueden aplicarse métodos de destrucción como la trituración para eliminar la información.

- **CD-ROM / DVD-R / Blu-Ray (BD-R)**
- **CD-RW / DVD-RW / Blu-Ray re-grabable (BD-RE)**

Medio magneto-óptico: Los métodos de destrucción de este tipo de dispositivos se enfocarán en la destrucción total del dispositivo.

- **Disco magneto-óptico.**
- **Mini Disc.**
- **HI-MD.**

[1] Cualquier operación o conjunto de operaciones efectuadas mediante procedimiento manuales o automatizados aplicados a los datos personales, relacionados con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación transferencia o disposición de datos personales.

Medios de estado sólido: Se pueden utilizar tecnologías de borrado seguro para sobrescribir el contenido del medio.

- Unidad de estado sólido o SSD (*Solid State Drive*)
- **USB** o pendrive.
- **Tarjetas de memoria (Flash drive).**

Cómputo en la nube: Servicio que se accede a través de Internet, para almacenar la información en espacios virtuales. Se debe considerar que la información no se encuentra del todo bajo el control del responsable debido a que ésta es almacenada en la infraestructura del proveedor.

TÉCNICAS DE DESTRUCCIÓN Y BORRADO SEGURO

Debemos siempre buscar la mejor técnica de borrado seguro que permita evitar el acceso de personas no autorizadas, garantizando la no recuperación de la información, tanto física como electrónica acorde a estándares internacionales en la materia, cuyas características a considerar son:

- **Irreversibilidad.** Se debe garantizar que no existe un proceso que permita recuperar la información.
- **Seguridad y confidencialidad.** Los medios de almacenamiento se deben tratar durante el borrado con la misma seguridad con que se han mantenido durante su existencia.
- **Favorable al medio ambiente.** El método de borrado debe producir el mínimo de emisiones y desperdicios que afecten el medio ambiente.

MÉTODOS FÍSICOS DE BORRADO

Destrucción de los medios de almacenamiento físico

1) **Trituración:** *S*e debe considerar el tipo y tamaño del corte o "partícula", así como la capacidad de la trituradora, considerando el tipo de corte, existen dos tipos principales de trituradoras:

   - **Trituradora de línea recta o tiras:** Cortan el documento en tiras delgadas. Se recomienda usar el corte en tiras de 2 mm de ancho o menos. No es muy segura debido a que la información puede ser recuperada rearmando los fragmentos, por lo que se recomienda utilizar para eliminar información con riesgo bajo o clasificada con nivel estándar.

   - **Trituradora de corte cruzado o en partículas:** Corta el documento de forma vertical y horizontal generando fragmentos diminutos, denominados "partículas". Se recomienda utilizar para eliminar datos con riesgo medio y alto, o aquellos clasificados con nivel especial.

2) **Incineración:** Consiste en la destrucción a través del uso del fuego, es una opción segura para la destrucción de los datos personales, siempre y cuando se valide que el activo se redujo a cenizas, sin embargo, no es muy recomendable por cuestiones relacionadas con el cuidado del medio ambiente**.**

3) **Químicos:** Consiste en destruir documentos por medio de químicos, sin embargo, tampoco es muy recomendable por temas ecológicos.

Destrucción de los medios de almacenamiento electrónicos

1) **Desintegración:** En este proceso se rompe el dispositivo en trozos lo suficientemente pequeños para asegurar que las placas de los circuitos impresos, así como los chips integrados se destruyan de forma adecuada

2) **Pulverización:** Procedimiento mediante el cual un cuerpo sólido se convierte en pequeñas partículas de polvo.

3) **Fusión:** Paso de un cuerpo del estado sólido al líquido por la acción del calor.

4) **Incineración**: Los procesos de incineración derriten el plástico que protege el dispositivo y los circuitos internos que componen el soporte.

5) **Abrasión**: Acción de arrancar, desgastar o pulir algo por rozamiento o fricción

6) **Trituración: Las** trituradoras de papel se pueden utilizar para destruir los medios de almacenamiento flexibles. El tamaño del fragmento 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. Se recomienda generar fragmentos de un ancho máximo de 2mm.

IMPORTANTE: Los medios ópticos de almacenamiento como CD, DVD, magneto-ópticos, deben ser destruidos por pulverización, trituración de corte transversal o incineración, en el caso de los discos duros se deberá asegurar que los platos internos del disco han sido destruidos eficazmente.

MÉTODOS LÓGICOS DE BORRADO

a) Desmagnetización: Consiste en la exposición de los soportes de almacenamiento a un potente campo magnético a través de un dispositivo denominado desmagnetizador que elimina los datos almacenados en el dispositivo. Sólo se recomienda si no se piensa volver a utilizar el medio de almacenamiento.

b) Sobre-escritura: Se trata de escribir información nueva en el mismo lugar que los datos existentes utilizando herramientas de *software*, puede ser utilizado para todos los dispositivos regrabables, permitiendo su reutilización, debido a que la sobre- escritura se realiza accediendo al

contenido de los dispositivos y modificando sus valores almacenados.

c) 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. Este proceso elimina el lugar donde se almacena la llave con la que se protege la información, lo que ocasiona que también se destruya toda la información almacenada.

d) Cómputo en la nube: Servicio proporcionado por un proveedor, por lo que se debe considerar que la información no se encuentra del todo bajo el control del responsable debido a que ésta es almacenada en la infraestructura de dicho proveedor.

IMPORTANTE: Se recomienda incluir en el contrato de servicio, cláusulas de borrado seguro de datos personales, políticas del proveedor respecto a las copias de seguridad, respaldos que realiza de la información y definición de multas por incumplimiento.

MÉTODO DE BORRADO SEGURO MÁS CONVENIENTE

Para elegir el método de borrado adecuado se debe considerar factores como el volumen, tipo de datos personales y el presupuesto con el que se cuenta:

COMPARACIÓN ENTRE LOS MÉTODOS FÍSICOS[2]

Técnica	Ventajas	Desventajas
Medios de almacenamiento físico		
Trituración	Hay trituradoras de oficina a bajo costo, por lo que la destrucción puede hacerse en las instalaciones.	Es necesario generar evidencia de la Destrucción con certificados, actas, fotografías y bitácoras de la destrucción.
	No siempre se requiere proveedor.	Si no se tritura la información de forma adecuada, ésta puede ser recuperada.
Incineración	Los datos son totalmente Irrecuperables.	Es necesario generar evidencia de la Destrucción, con certificados, actas, fotografías y bitácoras de la destrucción. Daña el medio ambiente y Puede resultar

[2] INAI. (junio, 2016). Guia_Borrado_Seguro_DP. junio, 2018, de INAI Sitio web: *http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf*

		peligroso.
Uso de químicos	Los datos son totalmente Irrecuperables.	Es necesario generar evidencia de la destrucción, con certificados, actas, fotografías y bitácoras de la destrucción Daña el medio ambiente y Puede resultar peligroso.
Destrucción (Trituración, desintegración, incineración, abrasión, pulverización, fusión)	Proporciona la máxima seguridad de destrucción absoluta de los datos.	Implica métodos industriales de destrucción y costos de transportación de los dispositivos. Al ser generalmente una subcontratación, se debe gestionar la entrega de evidencia de la destrucción.

COMPARACIÓN ENTRE LOS MÉTODOS LÓGICOS		
Técnica	**Ventajas**	**Desventajas**
Desmagnetización	Los datos son irrecuperables. Método rápido.	Se requiere un desmagnetizador e implica transportar el dispositivo a donde se encuentre. El dispositivo deja de ser utilizable. Dificultad para verificar borrado de datos. Dificultad para calcular la potencia requerida para borrar cada dispositivo. Por cada tipo de soporte. Personas con ciertas condiciones médicas o que tienen marcapasos deben permanecer alejados. Se debe gestionar la entrega de evidencia de la destrucción.
Sobre-excritura	Facilidad para comprobar la eliminación de la información. Se puede hacer en las instalaciones. Permite reutilizar dispositivos. Bajo costo.	No se puede utilizar en dispositivos que no sean degradables

En caso de que la destrucción lógica no sea correctamente ejecutada, debe utilizarse métodos de destrucción física del soporte, el cual debe quedar claramente documentado.

Importante: Se debe comprobar y documentar cuándo y cómo el proceso de borrado seguro se ha realizado a fin de demostrar que los datos personales en el medio de almacenamiento fueron eliminados. (Actas, fotografías y bitácoras de destrucción). Véase **"Formato reporte de operación de borrado". Esto incluye a los prestadores de servicio.**

TRANSITORIO. La presente Guía surtirá efectos legales internos inmediatamente después de ser aprobado por el Comité de Transparencia del Partido del Trabajo.

Formato Reporte de Operación de Borrado

Lugar y fecha de ejecución

Fabricante del dispositivo	
Modelo:	**Número de serie:**

Tipo de medio -tache el de su elección-			
Archivero	Gaveta	Estante	Disco Duro
USB	CD	DVD	Blu-Ray
Mini Disc	Memoria flash	Otro:_____	

Método de borrado seguro aplicado -tache el de su elección-	
Trituración	Incineración
Sobre-escritura	Uso de químicos
Desmagnetización	Tercero especializado
Destrucción física	Otro: _____

Personas involucradas en el proceso de borrado	
Nombre:	**firma**
Cargo:	
Nombre:	**firma**
Cargo:	

Herramienta utilizada

Método de revisión utilizado

Personas involucradas en el proceso de revisión	
Nombre: Cargo:	firma
Nombre: Cargo:	firma
Nombre: Cargo:	firma
Observaciones	
Firma	

Nombre y firma de la persona responsable del
Sistema de datos personales