



**INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN
EN TECNOLOGÍAS DE LA INFORMACIÓN Y
COMUNICACIÓN**

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

**“GUÍA PARA EL BORRADO SEGURO DE
DATOS PERSONALES”**

PROPUESTA DE SOLUCIÓN EMPRESARIAL
Que para obtener el grado de MAESTRO EN DERECHO DE LAS TECNOLOGÍAS
DE LA INFORMACIÓN Y COMUNICACIÓN

Presenta:

Juan Armando Becerra Gutiérrez

Asesor:

Olivia Andrea Mendoza Enríquez

Ciudad de México, enero de 2017.



AUTORIZACIÓN DE IMPRESIÓN

Ciudad de México, 27 de enero de 2017

La Gerencia de Capital Humano/Gerencia de Investigación hacen constar que el proyecto terminal titulado:

“Guía para el borrado seguro de datos personales”

Desarrollada por el alumno

Nombre: **JUAN ARMANDO**

Apellido paterno: **BECERRA**

Apellido materno: **GUTIERREZ**

Desarrollado bajo la asesoría de la:

Dra. Olivia Andrea Mendoza Enríquez

Ha sido revisada y aprobada por el profesor investigador:

Dr. Federico César Lefranc Weegan

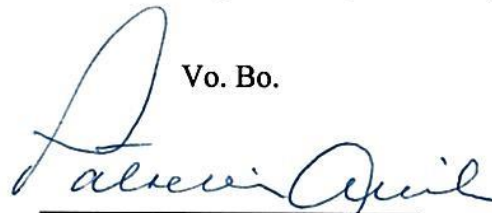
Dr. Alberto Enrique Nava Garcés

Mtra. Evelyn Téllez Carvajal

Quien ha depositado en esta gerencia en su oportunidad sus reflexiones y comentarios que han sido atendidos e integrados en su totalidad por el alumno a la nueva versión escrita del proyecto integrado revisado; siendo corroborados por los mismos revisores, quienes emitieron sus votos aprobatorios por separado que obran en el expediente de investigación correspondiente.

Por lo cual, se expide la presente autorización para la impresión del proyecto terminal al que se ha hecho mención.

Vo. Bo.


Patricia Ávila Muñoz

Gerencia de Capital Humano

* Anexar la presente autorización al inicio de la versión impresa del proyecto integrado que ampara la misma.

C.c.p.: Patricia Ávila Muñoz, Gerencia de Capital Humano, Gilberto Barrios Aldana, Coordinadora de Administración Escolar.

Nota de Contexto

Este documento es una versión modificada, con los comentarios del cuerpo académico de INFOTEC para el proceso de titulación, del borrador final de la *Guía para el Borrado Seguro de Datos Personales*¹ (Guía) presentada por Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) el 14 de julio de 2016².

La Guía se desarrolló en la Dirección General de Prevención y Autorregulación, de la Coordinación de Datos Personales del INAI, área a la cual me encuentro adscrito. Durante el evento de presentación se me reconoció como parte de los autores del presente documento.

Para el desarrollo de la Guía se aplicó un método deductivo directo, ya que se tenía identificada la problemática en particular, y el trabajo consistió en la homologación de los estándares internacionales en materia de eliminación y destrucción de información, al caso mexicano.

Esta Guía tiene por objeto coadyuvar al cumplimiento del principio de calidad mencionado en el artículo 11 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Ley) que entre otras cuestiones indica que cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades de tratamiento y las disposiciones legales aplicables, estos deberán ser borrados o eliminados de manera definitiva.

Este proceso de eliminación debe realizarse bajo procedimientos seguros que garanticen que los datos personales fueron borrados en su totalidad. Por ello el INAI estimó pertinente la emisión de un instrumento que orientara a los sujetos obligados, en el cumplimiento de las disposiciones de la Ley y su Reglamento, con relación al borrado de información como una medida de seguridad para la protección de los datos personales.

¹ Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf

² INAI presenta la guía para el Borrado Seguro de datos personales, vanguardia en América Latina, consultable en: <http://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-199-16.pdf>

Tabla de contenido

Introducción.....	1
Capítulo 1: El Borrado Seguro	4
1.1 Importancia del Borrado Seguro.....	4
1.2 Beneficios del Borrado Seguro.....	8
1.3 Sistema de Gestión de Seguridad de Datos Personales.....	8
Capítulo 2: Medios de almacenamiento.	12
2.1 Medios de almacenamiento físico	12
2.2 Medios de almacenamiento electrónico.....	12
Capítulo 3: Métodos no seguros para el Borrado de datos personales.	15
3.1 Para medios de almacenamiento físico.....	15
3.2 Para medios de almacenamiento electrónico	15
Capítulo 4: Métodos seguros para el Borrado de datos personales.	19
4.1 Métodos Físicos de Borrado	20
4.1.1 Destrucción de los medios de almacenamiento físico	20
4.1.2 Destrucción de los medios de almacenamiento electrónicos	24
4.2 Métodos Lógicos de Borrado.....	25
4.2.1 Desmagnetización	25
4.2.2 Sobre-escritura	26
4.2.3 Cifrado de medios.....	29
Capítulo 5: Selección del Método de Borrado Seguro.....	31
5.1 Comparación entre los Métodos Físicos.....	31
5.2 Comparación entre los Métodos Lógicos	33
5.3 Medios de almacenamiento y sus respectivos métodos de Borrado Seguro..	35
5.4 Subcontratación.....	36
Capítulo 6: Consideraciones adicionales para el Borrado Seguro.....	39
6.1 Cómputo en la nube.....	39
6.2 Validación y reporte del Borrado Seguro en medios.....	39
6.3 Trabajo en casa.....	40
Bibliografía.....	41
Anexos	44
Anexo I. Tipos de medios de almacenamiento	44
Medios de almacenamiento físico	44
Medios de almacenamiento electrónico	45
Anexo II. Controles de seguridad para el tratamiento de la información personal por medio de almacenamiento.....	49

Índice de figuras

Figura 1. “Dumpster Diving” para la recuperación de información.....	6
Figura 2. Ejemplos de medios de almacenamiento físico.....	12
Figura 3. Ejemplos de medios de almacenamiento electrónico.....	13
Figura 4. Aunque el sistema operativo indique que se eliminará la información de forma permanente, existe software con el cuál es posible recuperar el documento.....	16
Figura 5. El comando “Formatear”, elimina la “lista de archivos” no la información almacenada.....	17
Figura 6. Clasificación de los métodos para el Borrado Seguro de los datos personales.....	20

Índice de tablas

Tabla 1. Escenario de riesgo por la falta de Borrado Seguro de los medios de almacenamiento.....	7
Tabla 2. Grados de seguridad para la destrucción de documentos.....	24
Tabla 3. Grados de seguridad en los métodos de borrado por sobre-escritura.....	29
Tabla 4. Comparación entre los Métodos Físicos.....	33
Tabla 5. Comparación entre los Métodos Lógicos.....	34
Tabla 6. Medios de almacenamiento y sus respectivos métodos de Borrado Seguro.....	36
Tabla 7. Consideraciones para el tratamiento de medios de almacenamiento.....	51

Introducción.

De conformidad con lo dispuesto por el artículo 11 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Ley), uno de los principios que regula el derecho a la protección de datos personales es el de “calidad”. Este principio señala, entre otras cuestiones, que cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, es decir, borrados, suprimidos, eliminados o destruidos.

En el mismo sentido, el artículo 37 del Reglamento de la Ley establece que una vez cumplidas las finalidades del tratamiento, y cuando no exista disposición legal o reglamentaria que establezca lo contrario, el responsable deberá proceder a la cancelación de los datos personales en su posesión, previo bloqueo de los mismos, **para su posterior supresión**.

Asimismo, el artículo 38 del Reglamento de la Ley prevé la obligación de los responsables de establecer y documentar los procedimientos para la conservación, el bloqueo y la supresión de los datos personales. Cabe señalar que la supresión de datos se define en el artículo 2, fracción XII del Reglamento de la Ley, como la actividad de eliminar, borrar o destruir el o los datos personales, una vez concluido el periodo de bloqueo, bajo las medidas de seguridad previamente establecidas por el responsable del tratamiento.

De acuerdo con lo anterior, se puede observar que el principio de calidad exige que los datos personales sean suprimidos, destruidos, borrados o eliminados cuando ya no exista razón válida, legítima o lícita para su conservación. Ahora bien, la destrucción de los datos personales debe hacerse bajo procedimientos seguros que garanticen que los datos fueron borrados o eliminados de la base de datos en su totalidad y que los mismos no pueden ser recuperados, y utilizarse de manera indebida.

Para ello, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) pone a disposición la presente ***Guía para el Borrado Seguro de Datos Personales (Guía de Borrado Seguro)***, con el objeto de

orientar a los sujetos obligados, en el cumplimiento de las disposiciones establecidas en la Ley y su Reglamento, con relación al borrado de información como medida de seguridad para la protección de los datos personales.

La Guía de Borrado Seguro **es un documento de apoyo para los involucrados en el tratamiento de datos personales**, en particular para aquellos responsables o encargados del tratamiento de datos personales que están menos familiarizados con el tema de seguridad de la información, **la cual permite conocer métodos y técnicas basadas en las mejores prácticas y estándares, para la eliminación segura de los datos personales en los sistemas de tratamiento.**



Capítulo 1

El Borrado Seguro.



Capítulo 1: El Borrado Seguro

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 una organización, es importante contar con una medida de seguridad que permita minimizar el efecto de cualquier tipo de recuperación de información no autorizada, sobre los medios de almacenamiento físicos y electrónicos, relacionados con el tratamiento de datos personales que desecha una organización:

Por lo tanto, el Borrado Seguro es la medida de seguridad mediante la cual se establecen métodos y técnicas para la eliminación definitiva de los datos personales, de modo que la probabilidad de recuperarlos sea mínima.

1.1 Importancia del Borrado Seguro

En primera instancia, es importante señalar que el Borrado Seguro de los datos personales es un tema de cumplimiento legal.

La Ley desarrolla una serie de principios y deberes que establecen obligaciones concretas para los responsables del tratamiento de datos personales, a fin de crear condiciones para la protección de los datos, evitar malos manejos de los mismos, y permitir que las personas ejerzan su derecho a la autodeterminación informativa. Para el caso que nos ocupa, destaca el principio de calidad y el deber de seguridad.

El principio de calidad establece que, conforme a la finalidad o finalidades para las que se vayan a tratar los datos personales, éstos deben ser exactos, completos, pertinentes, actualizados y correctos. Asimismo, este principio señala que cuando los datos personales hayan dejado de ser necesarios para las

finalidades para la cuales se obtuvieron, deben ser eliminados, tomando en cuenta las disposiciones legales aplicables para los plazos de conservación.

En ese sentido, con independencia de que un titular de los datos personales ejerza su derecho de cancelación, el responsable del tratamiento 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, el cual se fija 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.³

Entonces tenemos que:

Plazo de conservación

= *Tiempo requerido para llevar a cabo las finalidades del tratamiento*

+ *plazos legales, administrativos, contables, fiscales, jurídicos e históricos aplicables*

+ *periodo de bloqueo.*

En algunos casos estos tres tiempos o plazos pueden coincidir.

Ahora bien, el deber de seguridad establece la obligación del responsable del tratamiento de implementar y mantener medidas de seguridad administrativas, técnicas y físicas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Así, con motivo del principio de calidad y del deber de seguridad, los datos personales deben eliminarse cuando ya no se requieren para la finalidad para la cual se obtuvieron, y su eliminación debe ser segura, de forma que se evite un uso indebido de los mismos.

³ De acuerdo con la fracción III del artículo 3 de la Ley, por bloqueo se entiende: “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”.

Al revisar las tendencias en 2014⁴ sobre vulneraciones a la seguridad de la información, **se puede identificar que una de las principales causas de incidentes a la seguridad de los datos personales, se debe a los dispositivos incorrectamente desechados, reutilizados, perdidos, extraviados y robados.**

El término “*Dumpster Diving*” o en su traducción literal “buceo en el basurero” se refiere a la búsqueda de bienes y objetos, para ser aprovechados, dentro de los basureros de zonas habitacionales, empresas y otros depósitos de desperdicios. Si bien esta práctica es, para algunos, un mecanismo de supervivencia o un pasatiempo, en el contexto de la seguridad de los datos personales, **se trata de una técnica que utilizan los atacantes para hacerse de información valiosa sobre las personas o las organizaciones**⁵ (Fig. 1).



Figura 1. “*Dumpster Diving*” para la recuperación de información.

Es sabido que los atacantes buscan obtener documentos, dispositivos de almacenamiento, equipo de cómputo, o cualquier elemento involucrado en el tratamiento de datos personales, con la intención de **recuperar dicha información utilizando diversos métodos o técnicas.**

Los métodos de recuperación de información pueden ir desde procedimientos casi artesanales, como el de recolectar documentos rotos para buscar las piezas, como si se tratara de un rompecabezas y armarlo con cinta; hasta

⁴ *Data Breach QuickView – 2014 Data Breach Trends*, Risk Based Security, febrero de 2015, consultable en: <https://www.riskbasedsecurity.com/reports/2014-YEDataBreachQuickView.pdf>

⁵ Véase: HADNAGY Christopher, *Social Engineering: The Art of Human Hacking*, Wiley, 2011. El “buceo en basureros” puede formar parte de uno de los procesos en pruebas de penetración denominado “Recolección de información”.

técnicas más sofisticadas como la utilización de software especializado en la recuperación de información “borrada” de un dispositivo de almacenamiento.

Por otro lado, para la seguridad de los datos personales, el riesgo es **el potencial o la probabilidad** de que una **amenaza** explote alguna o varias **vulnerabilidades** existentes en los **activos** de información y produzca algún **impacto negativo o daño**.

En suma, el **escenario de riesgo** relacionado con la **falta de Borrado Seguro** de los medios de almacenamiento en una organización, puede expresarse de la siguiente forma:

Escenario de riesgo por la falta de Borrado Seguro de los medios de almacenamiento				
Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad
Datos personales en medios de almacenamiento desechados o reutilizados.	Una persona que utilice técnicas de recuperación de información.	Falta de técnicas seguras y definitivas para el Borrado Seguro de los datos personales.	Daño económico y moral tanto a los titulares de los datos personales como a la organización.	Alta

Tabla 1. Escenario de riesgo por la falta de Borrado Seguro de los medios de almacenamiento.

Asimismo, el escenario de riesgo reflejado en la tabla anterior también puede expresarse como:

La probabilidad de que se materialice el riesgo, de que una persona utilice técnicas de recuperación de información, para obtener datos personales de los medios de almacenamiento desechados o reutilizados por la organización, es alta, debido a la falta de técnicas seguras de borrado o bien por el uso de técnicas dudosas o no definitivas para el borrado de los datos personales, lo cual puede causar daño económico y moral tanto a los titulares de los datos personales como a la organización.

Crear y analizar escenarios de riesgo permite tener una imagen más clara del problema, el cual podría ser, en este caso, evitar un daño a los titulares de los datos personales y a la organización misma. Esto debido a la falta de Borrado Seguro de los medios de almacenamiento que se desechan en una organización. Entonces, para mitigar dichos riesgos, se deberán implementar técnicas de Borrado Seguro.

Para conocer más sobre el análisis del riesgo se puede consultar la *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales (Guía para el SGSDP)* y el *Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas*, disponibles en la sección de Seguridad de los Datos Personales del portal de Internet del INAI⁶.

1.2 Beneficios del Borrado Seguro

- ✔ Eliminar adecuadamente los activos en desuso representa una medida de seguridad efectiva para minimizar las 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, compensación de daños y pérdida de clientes e inversionistas.

1.3 Sistema de Gestión de Seguridad de Datos Personales

⁶ <http://inicio.ifai.org.mx/SitePages/Documentos-de-Interes.aspx?a=m8>

El Borrado Seguro no debería ser una medida de seguridad aislada dentro de las organizaciones, sino que debería estar estrechamente ligada al ciclo de vida de los activos, y principalmente, a la protección de los datos personales en los sistemas de tratamiento.

En este sentido, el INAI promueve la adopción de un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), a través de sus Recomendaciones publicadas en el Diario Oficial de la Federación, el 30 de octubre de 2013.⁷

La implementación de un SGSDP proporciona varias ventajas operativas que permiten un mejor aprovechamiento respecto de la simple ejecución de métodos de Borrado Seguro, por ejemplo permite:

- Definir **alcances, objetivos y políticas**, en el tratamiento de datos personales, incluidos los procesos que requieran Borrado Seguro.
- Tener un **inventario de los datos personales en los sistemas de tratamiento.**
- Gestionar **los medios de almacenamiento** involucrados en el tratamiento de datos personales.
- **Establecer plazos de conservación de los datos personales y de los medios de almacenamiento.**
- Tener una 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 de los datos personales.

Para consultar más detalles sobre la implementación del SGSDP, puede consultarse la *Guía para el SGSDP*, disponible en la sección de seguridad de los datos personales del sitio web del INAI.⁸

⁷ Recomendaciones en materia de seguridad de datos personales, consultables en: http://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013

⁸ <http://inicio.ifai.org.mx/SitePages/Documentos-de-Interes.aspx?a=m8>

Asimismo, 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, entre otros.
- 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.



Capítulo 2

Medios de almacenamiento.

Capítulo 2: Medios de almacenamiento.

Para definir los métodos de borrado, **es necesario establecer la naturaleza de los activos**, es decir, si los datos personales se almacenan en un medio de almacenamiento físico o un medio de almacenamiento electrónico.

2.1 Medios de almacenamiento físico

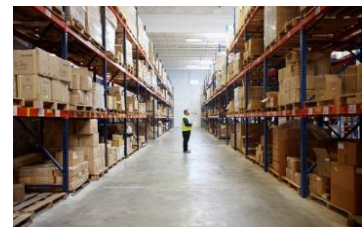
Los medios de almacenamiento físico son todo recurso inteligible a simple vista y con el que se puede interactuar sin la necesidad de ningún aparato que procese su contenido para examinar, modificar o almacenar datos personales, por ejemplo los expedientes de personal almacenados en un archivero.⁹



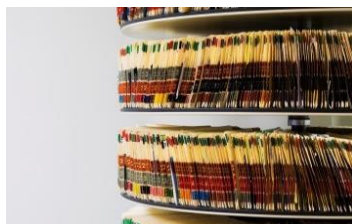
Archiveros



Gavetas / cajones



Bodegas



Estantes



Documentos



Carpetas

Figura 2. Ejemplos de medios de almacenamiento físico.

2.2 Medios de almacenamiento electrónico

Los medios de almacenamiento electrónico (**Fig. 3**), son 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. Podemos considerar entre estos medios, por ejemplo, a los discos duros (tanto los propios del

⁹ Véase la sección Medios de almacenamiento físico del Anexo I.

equipo de cómputo como los portátiles), memorias extraíbles como *USB* o *SD*, *CDs*, *Blu-rays*, entre otros.¹⁰ También podemos contemplar como medio de almacenamiento electrónico, el uso de servicios de almacenamiento en línea.



Medio magnético



Medio óptico



Medio magneto-óptico



Medio en estado sólido



Medio de almacenamiento en la nube

Figura 3. Ejemplos de medios de almacenamiento electrónico.

Por equipo de cómputo se entiende cualquier dispositivo electrónico que permita el procesamiento de información, por ejemplo, computadoras de escritorio, laptops, tabletas, teléfonos inteligentes, entre otros.

En el **Anexo 1** de esta guía se encuentra una clasificación más extensa de los medios de almacenamiento, así como algunas consideraciones sobre su tratamiento y sus posibles vulneraciones de seguridad.

Con estas definiciones es más fácil decidir cuál es la técnica de Borrado Seguro correspondiente, sin embargo, una organización debe establecer, respecto a su grado de madurez y modelo de negocio, un sistema de clasificación de sus activos considerando su ciclo de vida. Para profundizar sobre ese tema, se recomienda consultar la *Guía para el SGSDP* y el *Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas*, antes señalados.

¹⁰ Véase la sección Medios de almacenamiento electrónico del Anexo I.



Capítulo 3

Métodos no seguros para el Borrado de datos personales.



Capítulo 3: Métodos no seguros para el Borrado de datos personales.

Los métodos de este apartado son utilizados de forma común para borrar información o destruir sus medios de almacenamiento, sin embargo, ninguno de ellos es seguro, ya que es posible invertir el proceso para recuperar de manera parcial o total datos personales.

3.1 Para medios de almacenamiento físico

- **La destrucción manual:** Romper archivos y documentos a mano, con tijeras o rasgarlos con un *cutter* es un método inseguro para desechar este tipo de activos. Este método permite que una persona mal intencionada pueda recuperar los fragmentos de la basura y los ensamble a modo de rompecabezas para extraer información importante.
- **Tirar documentos de forma íntegra a la basura:** Arrojar a la basura documentos con información valiosa o utilizarlos como papel de reciclaje es una conducta aún más riesgosa que la anterior.

3.2 Para medios de almacenamiento electrónico

Los sistemas operativos de los equipos de cómputo o dispositivos ordenan la información en archivos dentro de sus medios de almacenamiento (por ejemplo, en un disco duro). Para encontrar estos archivos en el espacio correspondiente, el sistema operativo acude a la “lista de archivos”, donde se indica tanto el nombre del archivo como su ubicación dentro del espacio de almacenamiento.

Cuando se utilizan métodos de borrado dispuestos por el propio sistema operativo, la eliminación se realiza exclusivamente en la “lista de archivos” sin que se borre 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:

- **Los comandos de borrado por defecto de los sistemas operativos:** Cuando se utiliza un comando como “borrar” o “eliminar” (**Fig. 4**), lo único que se está quitando de esa tabla es la referencia al archivo, pero la información permanece en el medio de almacenamiento, hasta que se reutilice este espacio con un nuevo archivo. Así que, con la simple utilización de algún software (en ocasiones gratuito), se podrían recuperar todos los archivos “borrados”.

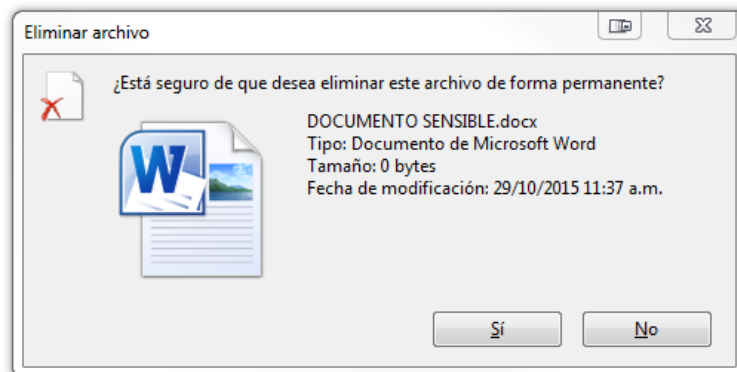


Figura 4. Aunque el sistema operativo indique que se eliminará la información de forma permanente, existe software con el cuál es posible recuperar el documento.

- **“Formatear”:** Cuando se formatea un medio de almacenamiento (**Fig. 5**), se eliminan las tablas o listas de archivos mencionadas anteriormente, pero igual que en el caso anterior, la información sigue en el dispositivo y puede recuperarse con el uso de software.

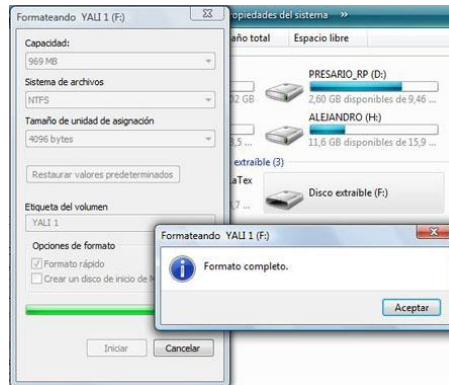


Figura 5. El comando “Formatear”, elimina la “lista de archivos” no la información almacenada.



Capítulo 4

Métodos seguros para el Borrado de datos personales.



Capítulo 4: Métodos seguros para el Borrado de datos personales.

La destrucción y borrado de información es un tema de vital importancia para proteger la confidencialidad, integridad y disponibilidad de la información, y en particular de los datos personales, por esta razón, los sujetos obligados deben analizar los medios más eficaces que conviene implementar para evitar que se pueda recuperar la información que ya no requieren.

Las técnicas de Borrado Seguro buscan que no sea posible recuperar la información tanto física como electrónica y evitan que personas no autorizadas puedan tener acceso a esos datos. De acuerdo a estándares internacionales en la materia¹¹, las características para este tipo de destrucción 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.

A continuación se detallan los diferentes métodos de Borrado Seguro, a fin de que las organizaciones puedan seleccionar aquéllos que mejor se ajusten a sus necesidades (**Fig. 6**).

¹¹ Véase el apartado de Bibliografía.

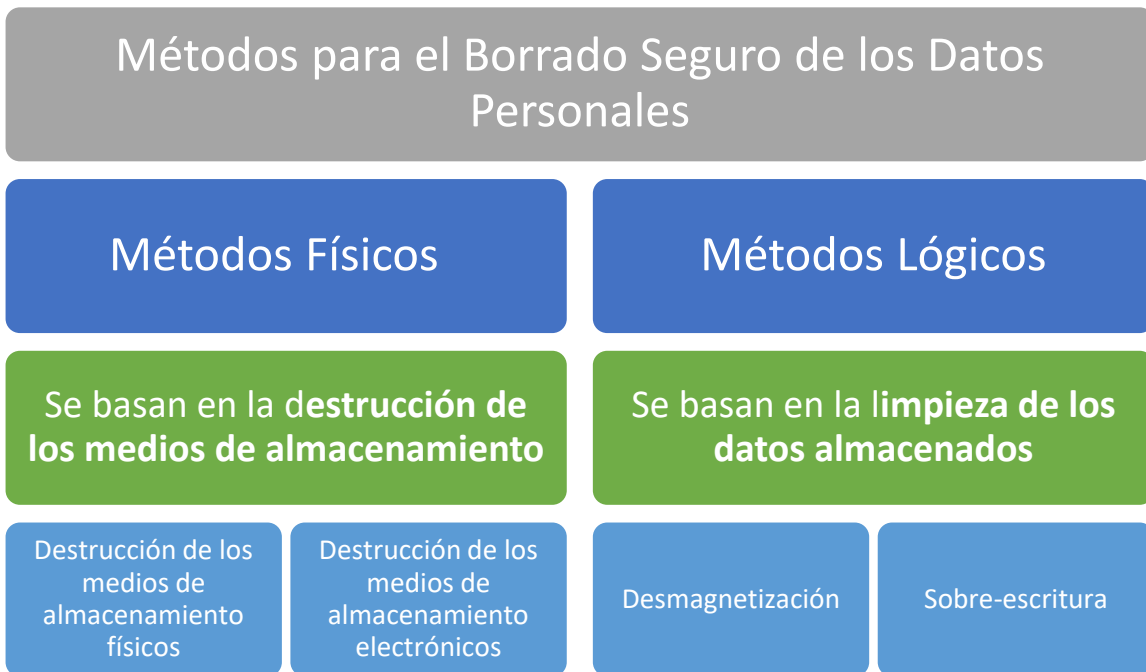


Figura 6. Clasificación de los métodos para el Borrado Seguro de los datos personales.

4.1 Métodos Físicos de Borrado

Los Métodos Físicos son aquellos que implican un daño irreversible o la destrucción total de los medios de almacenamiento, tanto físico como electrónico.

4.1.1 Destrucción de los medios de almacenamiento físico

Dentro de las técnicas de destrucción para los medios de almacenamiento físico se encuentran:

1) Trituración

Uno de los procesos más intuitivos para la destrucción de activos, tales como documentos, carpetas o archivos, es la trituración.

Las principales características que se deben considerar para la adquisición de una trituradora son 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:

- **En línea recta o tiras:** Cortan el documento en tiras delgadas. **Se recomienda usar el corte en tiras de 2 mm de ancho o menos**, a fin de evitar que la información pueda ser recuperada rearmando los fragmentos.
- **En corte cruzado o en partículas:** Corta el documento de forma vertical y horizontal generando fragmentos diminutos, denominados “partículas”, **lo cual hace prácticamente imposible que se puedan unir.**

La norma DIN 32757 es un estándar que se ha adoptado a nivel mundial para la destrucción de documentos, creada por el Instituto Alemán para la Estandarización. Esta norma establece cinco grados de seguridad y determina el tamaño máximo de las tiras o partículas en función de la criticidad de la información.

Además, de acuerdo con la *Guía para el SGSDP*¹² se sugiere contemplar el riesgo inherente de los datos personales en los sistemas de tratamiento, es decir, el valor significativo tanto para los titulares y responsables, como para cualquier persona no autorizada que pudiera beneficiarse de ellos.

A continuación se ofrecen ejemplos de categorías para los sistemas de tratamiento de datos personales según su riesgo inherente:

- a) Nivel estándar:** Esta categoría considera información de identificación, contacto, datos laborales y académicos de una persona física identificada o identificable, tal como: nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo, lugar de trabajo, experiencia laboral, datos de contacto laborales, idioma o lengua, escolaridad, trayectoria educativa, títulos, certificados, cédula profesional, entre otros.

¹² <http://inicio.ifai.org.mx/SitePages/Documentos-de-Interes.aspx?a=m8>

b) Nivel sensible: Esta categoría contempla los datos que permiten conocer la *ubicación física* de la persona, tales como la dirección física e información relativa al tránsito de las personas dentro y fuera del país.

También son datos de nivel sensible aquéllos que permitan inferir el *patrimonio* de una persona, que incluye entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores y fianzas. Incluye el *número de tarjeta bancaria de crédito y/o débito*.

Son considerados también los datos de *autenticación* con información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica y cualquier otro que permita autenticar a una persona.

Dentro de esta categoría se toman en cuenta los datos *jurídicos* tales como antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

Finalmente, se contemplan los datos personales sensibles de la Ley, es decir, aquéllos que afecten a la esfera más íntima de su titular. Por ejemplo, se consideran sensibles los que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave a la integridad del titular.

c) Nivel especial: Esta categoría corresponde a los datos cuya naturaleza única, o bien debido a un cambio excepcional en el contexto de las operaciones usuales de la organización, pueden causar daño directo a los titulares, por ejemplo la *Información adicional de tarjeta bancaria* que considera el número de la tarjeta de crédito y/o débito mencionado

anteriormente en combinación con cualquier otro dato relacionado o contenido en la misma, por ejemplo fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal (PIN).

Las categorías antes descritas de la *Guía para el SGSDP* son sólo una orientación, ya que el Pleno del INAI no ha emitido criterios institucionales al respecto, además de que ciertos datos personales que en principio no se consideran sensibles o de alto riesgo, podrían llegar a serlo dependiendo del contexto en que se trate la información.

En la tabla siguiente se muestra una relación entre el nivel de seguridad que se debe utilizar para destruir documentos, de acuerdo a la norma DIN 32757, dependiendo de la clasificación asignada a cada medio de almacenamiento en los sistemas de tratamiento.

Nivel de riesgo por sistema de tratamiento	Nivel del estándar	Tamaño máximo del fragmento	Tipo de documento
No recomendable	1. General	Tiras de 12 mm de ancho.	Documentos generales que deben hacerse ilegibles.
No recomendable	2. Interno	Tiras de 6 mm de ancho	Documentos internos que deben hacerse ilegibles.
Estándar	3. Confidencial	Tiras de 2 mm de ancho. Partículas de 4x80 mm.	Documentos confidenciales.
Sensible	4. Secreto	Partículas de 2x15 mm.	Documentos de importancia vital para la organización que deben mantenerse en secreto.

Especial	5. Alto Secreto	Partículas de 0.8x12 mm.	Documentos clasificados para los que rigen exigencias de seguridad muy elevadas.
-----------------	-----------------	--------------------------	--

Tabla 2. Grados de seguridad para la destrucción de documentos.

En general, para la protección de los datos personales, se recomienda utilizar la clasificación que sugiere la *Guía para el SGSDP*, respecto a los sistemas de tratamiento de datos personales según su riesgo inherente, en combinación con la norma DIN 32757, o cualquier otro estándar internacional o mejores prácticas en la materia.

De la norma DIN32757, se recomienda utilizar los niveles 3 “Confidencial”, 4 “Secreto” y 5 “Alto Secreto”, en correspondencia con los niveles Estándar, Sensible y Especial de la *Guía para el SGSDP*.

2) Incineración

La incineración de medios de almacenamiento físico consiste en su destrucción a través del uso del fuego. Actualmente la práctica de la incineración no es muy recomendable por cuestiones relacionadas con el cuidado del medio ambiente, sin embargo, es una opción segura para la destrucción de los datos personales, **siempre y cuando se valide que el activo se redujo a cenizas.**

3) Químicos

En algunos casos también es posible destruir documentos por medio de químicos, sin embargo esta opción tampoco es muy recomendable por temas ecológicos.

4.1.2 Destrucción de los medios de almacenamiento electrónicos

La destrucción de medios de almacenamiento electrónico utiliza técnicas tales como:

- **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.

La destrucción de medios de almacenamiento electrónico tiene el **carácter de un proceso industrial robusto**, por lo que a la mayoría de las organizaciones les puede resultar más práctico la subcontratación del servicio, además de que la eliminación definitiva del activo puede contar con opciones de tratamiento de desperdicios y de reciclaje para hacer que el proceso sea más amigable con el ambiente.

Cuando se trate de un proceso más pequeño, por ejemplo el de desechar un disco duro del equipo personal, es recomendable aplicar algún método lógico (que se verán en la siguiente sección) y posteriormente realizar una destrucción minuciosa del dispositivo (por ejemplo, haciendo varios hoyos en el dispositivo con un taladro), antes de enviarlo a un centro de reciclaje o depositarlo en algún contenedor genérico de “basura electrónica”.

4.2 Métodos Lógicos de Borrado

Los métodos lógicos son aquellos que implican la sobre-escritura o modificación del contenido de medio de almacenamiento electrónico.

4.2.1 Desmagnetización

Este método expone a los dispositivos de almacenamiento a un campo magnético a través de un dispositivo denominado desmagnetizador. Debido a las fuerzas físicas del proceso, es posible que el hardware donde se encuentra la información se vuelva inoperable, por lo que se recomienda aplicar este método si no se volverá a utilizar el medio de almacenamiento.

La desmagnetización se considera más segura que algunos procesos de destrucción física, ya que altera directamente el contenido de información y no al medio de almacenamiento en sí mismo.

La potencia requerida para borrar el dispositivo depende de su tamaño y forma, y para hacer efectivo el borrado, se requiere de una configuración particular para cada medio de almacenamiento. Por la naturaleza del equipo necesario para este proceso, suele utilizarse bajo un esquema de contratación del servicio.

4.2.2 Sobre-escritura

Consiste en sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de **escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.**

El método más simple consiste en realizar una sola sobre-escritura, y para implementar una mayor seguridad se pueden efectuar múltiples sobre-escrituras o “pasadas” con variaciones en los caracteres grabados al medio de almacenamiento.

Una ventaja particular de la sobre-escritura es que las herramientas se pueden utilizar para borrar un archivo o carpeta específica, sin necesidad de alterar o detener la operación de todo un medio de almacenamiento o equipo de cómputo.

En la tabla siguiente se muestran distintos métodos de borrado utilizados por las herramientas de software que existen en el mercado, con su respectiva descripción y nivel de seguridad¹³, donde a mayor grado, mayor nivel de seguridad en el borrado.

¹³ Véase: <http://www.lc-tech.com/pc/file-definitions/?lang=es>

Método de borrado	Características de la sobre-escritura aplicada el medio de almacenamiento	Nivel de Seguridad
Grado 1. Super Fast Zero Write	1. Valor fijo (0x00) una vez cada 3 sectores	Bajo
Grado 2. Fast Zero Write	1. Valor fijo (0x00) una vez todos los sectores	Bajo
Grado 3. Zero Write	1. Valor fijo (0x00) en todo el área	Bajo
Grado 4. Random Write	1. Valores aleatorios. La fiabilidad aumenta con la cantidad de pasadas	Medio
Grado 5. Random & Zero Write	1. Valores aleatorios 2. Valor fijo (0x00) 3. Valores aleatorios 4. Escritura de valor cero	Medio
Grado 6. US Navy, NAVSO P-5239-26 – MFM. Para discos codificados con MFM (Modified Frequency Modulation)	1. Valor fijo (0xffffffff) 2. Valor fijo (0xbfffffff) 3. Valores aleatorios 4. Se verifica la sobre-escritura	Medio
Grado 7. US Navy, NAVSO P-5239-26 – RLL. Para discos duros y soportes ópticos (CD, DVD, Blu Ray)	1. Valor fijo (0xffffffff) 2. Valor fijo (0x27ffffff) 3. Valores aleatorios 4. Se verifica la sobre -escritura	Medio
Grado 8. Bit Toggle	1. Valor (0x00) 2. Valor (0xff) 3. Valor (0x00) 4. Valor (0xff) Total de sobre-escrituras: 4	Medio

Grado 9. Random Random Zero	<ol style="list-style-type: none"> 1. Dos veces con valores aleatorios 2. Valor fijo (0x00) 3. Dos veces con valores aleatorios 4. Con ceros 	Medio
Grado 10. US Department of Defense (DoD 5220.22-M)	<ol style="list-style-type: none"> 1. Valor fijo determinado 2. Valor complementario (0xff) 3. Valores aleatorios 4. Se verifica la sobre-escritura 	Medio
Grado 11. US Air Force, AFSSI5020	<ol style="list-style-type: none"> 1. Valor fijo (0x00) 2. Valor fijo (0xff) 3. Valor aleatorio constante 4. Se verifica sobre-escritura de un mínimo del 10% del disco 	Medio
Grado 12. North Atlantic Treaty Organization (OTAN) NATO standard	<ol style="list-style-type: none"> 1. Seis veces con valores fijos alternativos entre cada pasada (0x00) y (0xff) 2. Valor aleatorio <p>Total de sobre-escrituras: 7</p>	Alto
Grado 13. Peter Gutmann Secure Deletion	<ol style="list-style-type: none"> 1. Valores aleatorios 4 veces sobre cada sector 2. Valores pseudo aleatorios sobre cada sector por veintisiete pasadas 3. Valores aleatorios durante cuatro pasadas sobre cada sector 	Alto

	Total de sobre-escrituras: 35	
Grado 14. US Department of Defense (DoD 5220.22-M) + Gutmann Method	Combina los grados 13 y 10 Total de sobre-escrituras: 35	Muy Alto

Tabla 3. Grados de seguridad en los métodos de borrado por sobre-escritura.

Algunos equipos de cómputo y medios de almacenamiento ya contemplan entre sus mecanismos de seguridad, funciones de Borrado Seguro integradas en su arquitectura.

Para conocer si estas funciones, o bien otras herramientas de software, tienen un nivel de seguridad aceptable, **es necesario revisar con el fabricante o en Internet el método de borrado utilizado**, así como las características de la sobre-escritura al medio de almacenamiento. Para ello, puede resultar de utilidad la tabla anterior.

4.2.3 Cifrado de medios

Cuando un archivo electrónico o medio de almacenamiento se encuentra cifrado, es posible aplicar el denominado “borrado criptográfico” (*Cryptographic Erase* o *CE*), para borrar únicamente las claves que se utilizaron para cifrar el medio de almacenamiento o archivo. Esto deja únicamente datos en un formato tal que es imposible obtener información de ellos sin dichas claves.

La efectividad de esta técnica depende:

- Del tipo de cifrado utilizado en el medio de almacenamiento o archivo.
- Del nivel de seguridad del método de borrado aplicado a las claves.



Capítulo 5

Selección del método de Borrado Seguro.

Capítulo 5: Selección del Método de Borrado Seguro.

El método de borrado adecuado para cada organización depende de factores tales como su modelo de negocio, el volumen y tipo de datos personales que manejan y el presupuesto con el que cuentan para este procedimiento. A continuación se presentan tres tablas comparativas que pueden permitir decidir sobre el mejor método para su organización.

5.1 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

		<p>demostrar el cumplimiento normativo</p> <p>Es necesario generar evidencia de la destrucción, por ejemplo con certificados, actas, fotografías y bitácoras de la destrucción. Puede resultar peligroso.</p>
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.

		<ul style="list-style-type: none"> • 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.
--	--	---

Tabla 4. Comparación entre los Métodos Físicos.

5.2 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.

		<ul style="list-style-type: none"> • 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.
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.

Tabla 5. Comparación entre los Métodos Lógicos

5.3 Medios de almacenamiento y sus respectivos métodos de Borrado Seguro

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	<ul style="list-style-type: none"> • CD-ROM / DVD-R • HD-DVD • Blu-Ray (BD-R) • Disco UDO 	<ul style="list-style-type: none"> • Destrucción física
Óptico (dispositivos regrabables)	<ul style="list-style-type: none"> • CD-RW / DVD-RW • Blu-Ray re-gradable (BD-RE) 	<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 (Flash drive) 	<ul style="list-style-type: none"> • Sobre-escritura • Destrucción física

	<ul style="list-style-type: none"> • Dispositivo de estado sólido 	
--	--	--

Tabla 6. Medios de almacenamiento y sus respectivos métodos de Borrado Seguro.

5.4 Subcontratación

El tamaño de la organización y el volumen de datos personales que maneja son factores clave para determinar si el proceso debe realizarse de manera local o a través de la contratación de un tercero.

Si el volumen de medios de almacenamiento es bajo y/o la eliminación de activos se realiza de manera esporádica, la subcontratación es la opción. En particular hay que considerar que los métodos físicos y la desmagnetización requieren de equipo de grado industrial, por lo que sus costos de instalación y operación son considerables y a veces no aptos para todas las organizaciones.

Sin embargo, también hay que considerar que para las operaciones cotidianas podría ser útil contar con trituradoras de papel de grado 3 o 4 y con software de Borrado Seguro de grado 6 (es decir con verificación de la sobre-escritura), lo cual no requiere de un tercero, sino de la adquisición de equipo de oficina y licencias de software.

En caso de realizar una subcontratación, es necesario tomar en cuenta las siguientes consideraciones:

- **Si el Borrado Seguro se realiza en las instalaciones de un tercero**, esto implica posibles gastos de transporte, así como la necesidad de establecer medidas para el resguardo, registro y vigilancia de los medios de almacenamiento. Por lo que se debe ser cuidadoso con este proceso a fin de que no existan fugas de información o pérdidas de activos.
- **Se requiere establecer un contrato donde se defina de forma detallada el servicio que prestará el tercero**, así como las responsabilidades de ambas partes.
- **Se debe verificar si el proveedor cuenta con credenciales, certificaciones, o cualquier prueba de que el Borrado Seguro se realiza en un ambiente controlado.**

- **Es importante atestiguar el borrado y solicitar al prestador de servicio un certificado o acta del proceso de borrado realizado.**

Sin importar si el Borrado Seguro se hace dentro de la organización, o bien a través de una subcontratación, se debe administrar la generación de evidencia de dicho proceso, por ejemplo con certificados, actas, fotografías y bitácoras de la destrucción, a fin de que ante un procedimiento del INAI se pueda demostrar el cumplimiento de esta medida de seguridad.



Capítulo 6

Consideraciones adicionales para el Borrado Seguro.



Capítulo 6: Consideraciones adicionales para el Borrado Seguro.

En esta sección se abordarán algunos temas que son importantes para optimizar los procedimientos relacionados a la implementación del Borrado Seguro en las organizaciones.

6.1 Cómputo en la nube

El cómputo en la nube es una tecnología importante que optimiza las operaciones y costos de las organizaciones, por ejemplo a través del correo electrónico o del almacenamiento de información a través de Internet, sin embargo respecto al tema de Borrado Seguro, puede implicar algunos desafíos importantes, debido a la ubicuidad de acceso y a la replicación de la información.

El primer punto importante respecto al Borrado Seguro es que **la información no se encuentra del todo bajo el control de la organización, y es almacenada en la infraestructura de un tercero. En este sentido, la mejor herramienta con la que se cuenta es el contrato de servicio.**

Además de las cláusulas de borrado, se deben revisar las políticas del proveedor respecto a las copias de seguridad y respaldos que realiza de la información. De ser posible, se debe solicitar al proveedor evidencia del proceso de borrado que realiza.

En cuanto a la utilización de los servicios, hay que tomar en cuenta que muchos proveedores ofrecen sincronización del contenido a través de múltiples dispositivos, **lo que implica que a veces no es suficiente borrar la información de un solo dispositivo.**

6.2 Validación y reporte del Borrado Seguro en medios

Se recomienda establecer mecanismos de validación de la ejecución del Borrado Seguro, con el objetivo de confirmar que los datos personales en el medio de almacenamiento fueron eliminados de forma eficiente. Éste proceso puede encargarse a personal que no haya estado involucrado en la ejecución del Borrado Seguro.

En particular, para medios electrónicos, se puede aplicar algún mecanismo para revisar o auditar el proceso de Borrado Seguro.

Como parte fundamental de la evidencia del proceso de Borrado Seguro es conveniente contar con un registro de los medios a los cuales se les aplicó la eliminación de datos personales, para los medios de almacenamiento de tipo magnético, óptico, magneto-óptico o de estado sólido, es posible consolidar un reporte con la siguiente información:

- Fabricante del dispositivo
- Modelo
- Número de serie
- Tipo de medio
- Método de Borrado Seguro aplicado
- Herramienta utilizada (si es el caso)
- Método de revisión
- Personas involucradas en el proceso de Borrado Seguro
- Personas involucradas en el proceso de revisión
- Fecha de ejecución

6.3 Trabajo en casa

Por último, también se debe considerar que algunas organizaciones han optado por implementar un modelo de negocio donde los empleados realizan *home office* o trabajo en casa. En estos casos, se **deben implementar medidas de seguridad para garantizar que los activos con datos personales sean trasladados a la oficina para así garantizar que sean destruidos o eliminados de forma adecuada**. Para hacer esto posible, se recomienda implementar programas de concientización para los empleados, enfocados en la importancia de proteger los datos personales en custodia de la organización.

Bibliografía

La presente *Guía de Borrado Seguro* consideró las siguientes referencias para su elaboración:

Contexto Nacional

- Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias. (Actualizado en febrero de 2016).
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Recomendaciones en materia de seguridad de datos personales (Publicadas en el DOF el 30 de Octubre de 2013).
- Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales emitida por el INAI.
- Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas emitida por el INAI
- Estudio sobre recomendaciones generales para la destrucción segura de datos personales en ambiente físico y electrónico. (Diciembre de 2014)

Contexto Internacional

- BS 10012:2009 Data protection – Specification for a personal information management system.
- COBIT 5 Framework.
- Estudio sobre almacenamiento y Borrado Seguro de información del Observatorio INTECO.
- SANS FOR408: Windows Forensic Analysis

- ICO. Deleting personal data.
- ISO/IEC 27001:2013, Information Technology - Security techniques – Information security management systems – Requirements.
- ISO/IEC 27002:2013, Information Technology - Security techniques – Code of practice for security management.
- ISO/IEC 29100:2011, Information Technology - Security techniques -- Privacy framework.
- ISO 15489-1:2001, Information and documentation - Records management.
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems.
- NIST SP 800-88 Guidelines for Media Sanitization (Revision 1).
- SANS Forensics
- The OCDE Privacy Framework.



Anexos



Anexos

Anexo I. Tipos de medios de almacenamiento

Los datos personales tratados por una organización pueden almacenarse, de forma física y/o electrónica, en distintos tipos de medios, los cuales deben contar con medidas de seguridad que garanticen su confidencialidad, disponibilidad e integridad durante el periodo que sea necesario. A continuación se proporciona información más detallada de los medios de almacenamiento mencionados en esta guía.

Medios de almacenamiento físico

Existen distintos medios de almacenamiento de documentos físicos:

- a) **Archiveros.** Es muy común encontrar información personal en archiveros que no se encuentren protegidos con llaves y que por lo tanto cualquier persona con acceso a las instalaciones pueda obtener información general, o incluso sensible y/o patrimonial.
- b) **Gavetas.** El personal de las organizaciones resguarda información personal en sus gavetas, sin embargo no siempre son lo suficientemente cuidadosos como para proteger este medio a través del uso de llaves.
- c) **Bodegas.** Muchas organizaciones utilizan bodegas para almacenar su archivo muerto. Es muy común encontrar en este tipo de repositorios, gran cantidad de datos personales e información relevante del negocio, que ya no se requieren y que sólo están ocupando espacio e implicando un riesgo para la organización y los titulares de los datos personales.
- d) **Estantes.** Las organizaciones suelen almacenar expedientes y carpetas con información personal en estantes de oficinas. En muchas ocasiones esta información está disponible para cualquier persona que tenga acceso a las instalaciones.
- e) **Oficinas.** Es común identificar información personal en oficinas, ya sea sobre los escritorios, en tableros de corcho, o en áreas de impresión. En muchas ocasiones las oficinas cuentan con áreas de impresión donde se utilizan hojas reciclables. Se recomienda prestar atención en el tipo de documentos

que se mandan a reciclar con el objetivo de validar que no se utilicen hojas que puedan contener datos personales y/o información confidencial de la organización, ya que pudieran ser divulgados o expuestos y utilizados para finalidades distintas a las legítimas y establecidas en el aviso de privacidad del responsable.

- f) **Carpetas.** Es común que las organizaciones resguarden sus documentos en carpetas, sin embargo éstas no siempre son almacenadas en lugares seguros.

La principal característica de la información resguardada en los medios antes señalados consiste en que se encuentra en papel. Las técnicas de destrucción que se pueden utilizar están enfocadas a la destrucción de los documentos, no al medio de almacenamiento.

Medios de almacenamiento electrónico

Existen distintos medios de almacenamiento de información electrónica:

- a) **Medio magnético.** Estos dispositivos se basan en la aplicación de campos magnéticos que causan una reacción de partículas, lo que a su vez hace que cambien de posición, la cual se mantiene una vez que se deja de aplicar el campo magnético. Las posiciones representan los datos almacenados. Algunos ejemplos de este tipo de medios son:
- **Disco duro.** Es el principal medio de almacenamiento, se utiliza para guardar información, archivos de programas, software, multimedia, entre otro tipo de archivos en un equipo de cómputo.
 - **Disco duro externo o portátil.** Se utiliza para almacenar grandes cantidades de información (multimedia, archivos, software, texto, etc.) en un medio que puede ser fácilmente transportable.

- **Cintas magnéticas.** Se utilizan principalmente para realizar respaldos de bases de datos, servidores o equipos de organizaciones.

La principal característica de estos medios consiste en el uso de las propiedades magnéticas de los materiales para guardar información. Los métodos de destrucción de este tipo de dispositivos se enfocarán en la posibilidad de sobrescribir información o en la destrucción total del dispositivo.

b) Medio óptico (discos ópticos). Dispositivos capaces de guardar datos utilizando un rayo láser. La información queda grabada en la superficie de manera física por medio de ranuras microscópicas quemadas, es por esto que las ralladuras pueden ocasionar la pérdida de los datos.

- **CD-ROM / DVD-R.** Son utilizados para almacenar datos en formato digital, ya sean audio, imágenes, videos, documentos, texto, entre otros. Estos dispositivos sólo pueden utilizarse una vez para escribir información, posteriormente sólo sirven para la lectura de los datos que contienen.
- **CD-RW / DVD-RW.** Funcionan igual que un CD-ROM / DVD-R con la diferencia de que éstos pueden sobre-escribirse múltiples veces.
- **HD-DVD.** Consiste en un estándar para el DVD de alta definición.
- **Blu-Ray (BD-R).** Se utiliza para almacenar videos de alta definición y datos de alta densidad. Esta tecnología permite escribir datos solo una vez, por lo que se utiliza mayormente para lectura.
- **Blu-Ray re-grabable (BD-RE).** Es un Blu-Ray que permite escribir datos varias veces.
- **Disco UDO.** Es una especie de cartucho que almacena hasta 60 GB. Se utiliza para trabajo pesado o entornos de uso prolongado.

La principal característica de estos medios, que se debe tomar en cuenta para seleccionar una técnica de destrucción adecuada, consiste en que el estado de la superficie del dispositivo es fundamental para tener acceso a la información que se encuentra en el mismo. Si ésta se daña, la información contenida en ella ya no puede leerse, por lo que pueden aplicarse métodos de destrucción como la trituración para eliminar la información.

c) Medio magneto-óptico. Consiste en un sistema combinado que graba información de forma magnética bajo la incidencia de un rayo láser y la reproduce por medios ópticos. Tiene la capacidad de un disco óptico, pero puede utilizarse para escribir datos, múltiples veces, con la facilidad con que se hace en un disco magnético. Son medios resistentes que pueden almacenar datos durante 30 años sin distorsiones ni pérdidas, adicionalmente este tipo de medios verifican la información después de escribirla por lo que resultan confiables. Algunos ejemplos de este tipo de dispositivos son:

- **Disco magneto-óptico.** Medio óptico de almacenamiento de datos en el que la información se codifica, guarda y almacena haciendo unos surcos microscópicos con un láser sobre la superficie del disco.
- **MiniDisc.** Es un disco óptico pequeño (7 cm x 6,75 cm x 0,5 cm) y regrabable que permite almacenar audio.
- **HI-MD.** Es una evolución del MiniDisc, que permitió aumentar su capacidad 6 veces.

La característica principal de los medios magneto-ópticos consiste en que los datos se almacenan en su superficie, por lo que los métodos de destrucción de este tipo de dispositivos se enfocarán en la destrucción total del dispositivo.

- d) Medios de estado sólido.** Son dispositivos de almacenamiento que usan tecnología de memoria *flash* estática, resisten caídas y golpes ya que no tiene elementos mecánicos. Algunos dispositivos de este tipo son los siguientes:
- **Pendrive / USB.** Se utilizan para almacenar información, sin embargo puede incluir otros servicios como, lector de huella digital, radio FM, grabación de voz y reproducción de audio. Son muy útiles y prácticos por su tamaño y porque pueden almacenar gran cantidad de información.
 - **Tarjetas de memoria (Flash drive).** Se usan para almacenar fotos y videos en cámaras digitales. También se utilizan para aumentar la capacidad de almacenamiento de teléfonos móviles y tabletas.
 - **Dispositivo de estado sólido.** Usan una memoria no volátil flash. Son menos sensibles a los golpes, prácticamente no hacen ruido y tienen un menor tiempo de acceso y de latencia en comparación con los discos duros convencionales.

La principal característica de estos medios, que se debe tomar en cuenta para seleccionar una técnica de destrucción adecuada, consiste en que el dispositivo se puede utilizar varias veces para escribir información, por lo que se pueden utilizar tecnologías, métodos y/o herramientas para sobrescribir el contenido del medio.

e) Servicios de almacenamiento en la nube. Es un servicio que se accede a través de Internet, para almacenar en espacios virtualizados, archivos con contenido como imágenes, documentos, videos, bases de datos, entre otros. Este servicio normalmente es proporcionado por un proveedor de servicios.

La principal característica de estos medios, que se debe tomar en cuenta para seleccionar una técnica de destrucción adecuada, consiste en que la información es almacenada por un tercero, por lo que la destrucción de la información está a cargo del proveedor del servicio. En ese sentido, se requieren cláusulas contractuales que garanticen y obliguen al proveedor a utilizar métodos seguros para el borrado de datos personales.

Anexo II. Controles de seguridad para el tratamiento de la información personal por medio de almacenamiento

A continuación se muestran algunas medidas de seguridad útiles para el tratamiento de la información según su medio de almacenamiento, así como algunos riesgos a los que podrían estar expuestos.

Medios de almacenamiento físico		
Tipo de medio	Controles de seguridad	Riesgos
Archiveros, gavetas / cajones, bodegas, estantes, oficinas.	<ul style="list-style-type: none"> • Proteger el acceso físico al lugar en el que se encuentra el medio de almacenamiento (cámaras de seguridad, guardias, acceso restringido con tarjeta de proximidad, entre otros). 	<ul style="list-style-type: none"> • Robo del medio • Desastres naturales (incendio, inundación) • Acceso no autorizado • Pérdida del medio

	<ul style="list-style-type: none"> • Considerar la digitalización de la información. • Resguardar en ambiente físico protegido contra desastres naturales. 	
Medios de almacenamiento electrónico		
Tipo de medio	Controles de seguridad	Riesgos
Medios magnéticos	<ul style="list-style-type: none"> • Mantener un registro de los medios existentes • Asignar a un responsable • Cifrar el medio • Resguardar el acceso físico al medio • Validar estado del medio de forma periódica 	<ul style="list-style-type: none"> • Daño físico del medio • Pérdida o robo del medio
Medios ópticos	<ul style="list-style-type: none"> • Mantener un registro de los medios existentes • Asignar a un responsable • Cifrar el medio • Resguardar el acceso físico al medio • Validar estado del medio de forma periódica 	<ul style="list-style-type: none"> • Daño físico del medio • Pérdida o robo del medio
Medios magneto-ópticos	<ul style="list-style-type: none"> • Mantener un registro de los medios existentes • Asignar a un responsable • Cifrar el medio • Resguardar el acceso físico al medio 	<ul style="list-style-type: none"> • Daño físico del medio • Pérdida o robo del medio

	<ul style="list-style-type: none"> • Validar estado del medio de forma periódica 	
Medios de estado sólido	<ul style="list-style-type: none"> • Mantener un registro de los medios existentes • Asignar a un responsable • Cifrar el medio • Resguardar el acceso físico al medio • Validar estado del medio de forma periódica 	<ul style="list-style-type: none"> • Daño físico del medio • Daño lógico del medio (virus, malware, etc.) • Pérdida o robo del medio
Medios de almacenamiento en la nube	<ul style="list-style-type: none"> • Contar con un contrato claro y vigente • Definir como se protegerá la información a través de cláusulas de confidencialidad agregadas en el contrato 	<ul style="list-style-type: none"> • Divulgación de la información por ataque • Falta de claridad en las cláusulas de confidencialidad definidas con el proveedor

Tabla 7. Consideraciones para el tratamiento de medios de almacenamiento.