Universidad Anáhuac México

Guía borrado seguro

Comisión de Protección de Datos Personales

CONTENIDO

<< Volver al inicio

ALCANCE

La presente guía tiene por campo de aplicación:

- Orientar a las áreas de la Universidad Anáhuac México en el cumplimiento de las disposiciones establecidas en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) (en adelante, Ley) y su Reglamento, en relación con el borrado de información como medida de seguridad para la protección de los datos personales.

- Conocer métodos y técnicas basadas en las mejores prácticas y estándares, para la eliminación segura de los datos personales en los sistemas de tratamiento.

- En virtud de lo anterior, de conformidad con el artículo 17, fracciones III y IV del Reglamento de Integración y Operación de la Comisión de Protección de Datos Personales de la Universidad Anáhuac México, la Comisión de Protección de Datos Personales tiene a expedir las siguientes:

DISPOSICIONES GENERALES

¿Qué es 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.

¿Por qué es importante el 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, estos deben ser exactos, completos, pertinentes, actualizados y correctos. Asimismo, señala que cuando los datos personales hayan dejado de ser necesarios para las finalidades para las 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.

Plazo de conservación

= Tiempo requerido para llevar a cabo las finalidades de 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.

¿Cuáles son los beneficios del borrado seguro?

Eliminar adecuadamente los medios de almacenamiento 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.

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.

Medios de almacenamiento físico

Los medios de almacenamiento físico son todos los recursos inteligibles a simple vista y con los 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.

<< Volver al inicio

Medios de almacenamiento electrónico

Los medios de almacenamiento electrónico son todos los recursos a los que se puede acceder solamente 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, a los discos duros (tanto los propios del equipo de cómputo como los portátiles), memorias extraíbles como USB o SD, CD, Blu-Ray, entre otros. También podemos contemplar como medio de almacenamiento electrónico, el uso de servicios de almacenamiento en línea.

BORRADO SEGURO

¿Qué métodos NO borran de forma segura los datos personales?

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, ya que 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.

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:

I. Los comandos de borrado por defecto de los sistemas operativos: Cuando se utiliza un comando como "borrar" o "eliminar" 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".
II. "Formatear": Cuando se formatea un medio de almacenamiento, 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.

¿CÓMO BORRAR DE MANERA SEGURA LOS 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, se deben analizar los medios más eficaces que conviene implementar para evitar que se pueda recuperar la información que ya no requieren.

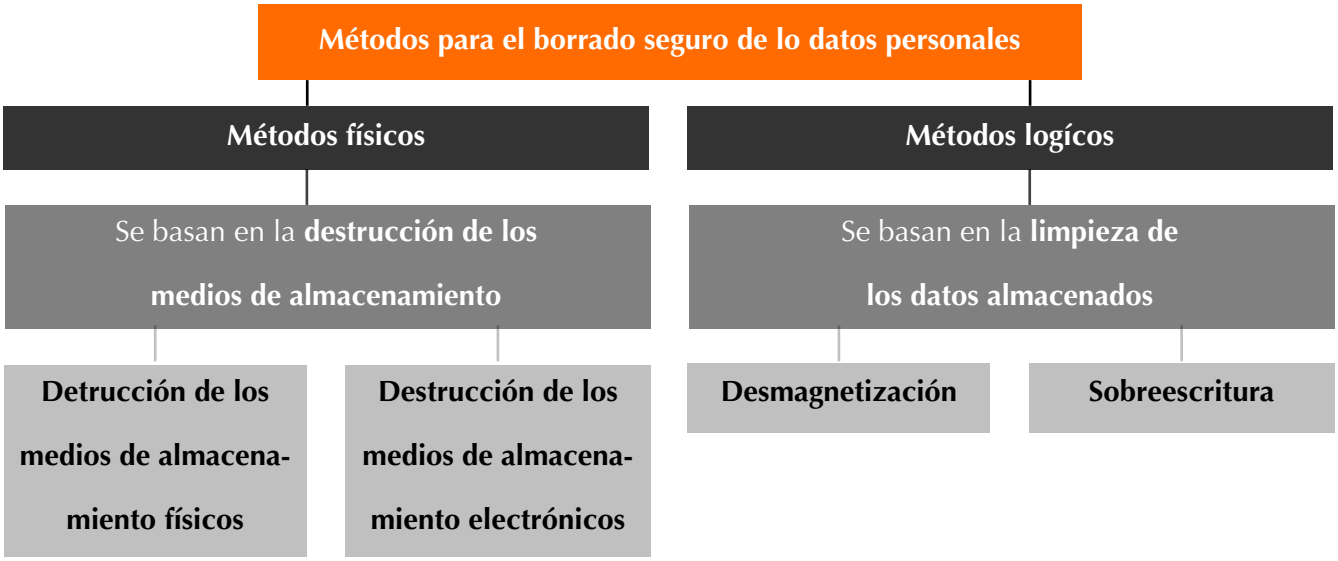
Las técnicas de borrado seguro buscan que no sea posible recuperar la información, tanto física como

electrónica, y evitan que personas no autorizadas puedan tener acceso a esos datos. De acuerdo con estándares internacionales en la materia, 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 medioambiente. El método de borrado debe producir el mínimo de emisiones y desperdicios que afecten al medioambiente.

A continuación se detallan los diferentes métodos de borrado seguro, a fin de que las áreas de la Universidad Anáhuac México puedan seleccionar aquellos que mejor se ajusten a sus necesidades:

Clasificación de los métodos para el borrado seguro de los datos personales



GUÍA PARA BORRADO SEGURO DE DATOS PERSONALES

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.

<< Volver al inicio

Destrucción de los medios de almacenamiento físico

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

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 re-armando 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, 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:

<< Volver al inicio

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.

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 aquellos 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, aquellos 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 otra, cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave a la integridad del titular.

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).

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

<< Volver al inicio

Grados de seguridad para la destrucción de documentos

Nivel de riesgo por sistema de tratamiento	Nivel del estándar	Tamaño máximo del fragmento	Tipo de documento
No recomendable	General	Tiras de 12 mm de ancho	Documentos generales que deben hacerse ilegibles
No recomendable	Interno	Tiras de 6 mm de ancho Tiras de 2 mm de ancho	Documentos internos que deben hacerse ilegibles
Estándar	Confidencial	Partículas de 4 x 80 mm	Documentos confidenciales
Sensible	Secreto	Partículas de 2 x 15 mm	Documentos de importancia vital para la organización que deben mantenerse en secreto
Especial	Alto secreto	Partículas de 0.8 x 12 mm	Documentos clasificados para los que rigen exigencias de seguridad muy elevadas

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 medioambiente, 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.

Químicos

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

<< Volver al inicio

Destrucción de los medios de almacenamiento electrónico

La destrucción de medios de almacenamiento electrónicos utiliza técnicas 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 más adelante) 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.

Métodos lógicos de borrado

Los métodos lógicos son aquellos que implican la sobreescritura 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 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.

Sobreescritura

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 sobreescritura, y para implementar una mayor seguridad se pueden efectuar múltiples sobreescrituras o “pasadas” con variaciones en los caracteres grabados al medio de almacenamiento.

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

<< Volver al inicio

Método de borrado	Características de la sobreescritura aplicada el medio de almacenamiento	Nivel de Seguridad
Grado 1. Super Fast Zero Write	Valor fijo (0x00) una vez cada 3 sectores	Bajo
Grado 2. Fast Zero Write	Valor fijo (0x00) una vez todos los sectores	Bajo
Grado 3. Zero Write	Valor fijo (0x00) en toda el área	Bajo
Grado 4. Random Write	Valores aleatorios. La fiabilidad aumenta con la cantidad de pasadas	Medio
Grado 5. Random & Zero Write	• Valores aleatorios • Valor fijo (0x00) • Valores aleatorios • Escritura de valor cero	Medio
Grado 6. US Navy, NAVSO P-5239-26 – MFM. Para discos codificados con MFM (Modified Frequency Modulation)	• Valor fijo (0xffffffff) • Valor fijo (0xbfffffff) • Valores aleatorios • Se verifica la sobreescritura	Medio
Grado 7. US Navy, NAVSO P-5239-26 – RLL. Para discos duros y soportes ópticos (CD, DVD, Blu Ray)	• Valor fijo (0xffffffff) • Valor fijo (0x27ffffff) • Valores aleatorios • Se verifica la sobreescritura	Medio
Grado 8. Bit Toggle	• Valor (0x00) • Valor (0xff) • Valor (0x00) • Valor (0xff) Total de sobreescrituras: 4	Medio
Grado 9. Random Random Zero	• Dos veces con valores aleatorios • Valor fijo (0x00) • Dos veces con valores aleatorios Con ceros	Medio

Grado 10. US Department of Defense (DoD 5220.22-M)	• Valor fijo determinado • Valor complementario (0xff) • Valores aleatorios • Se verifica la sobreescritura	Medio
Grado 11. US Air Force, AFSSI5020	• Valor fijo (0x00) • Valor fijo (0xff) • Valor aleatorio constante • Se verifica sobre-escritura de un mínimo del 10% del disco	Medio
Grado 12. North Atlantic Treaty Organization (OTAN) NATO standard	• Seis veces con valores fijos alternativos entre cada pasada (0x00) y (0xff) • Valor aleatorio Total de sobreescrituras: 7	Alto
Grado 13. Peter Gutmann Secure Deletion	• Valores aleatorios 4 veces sobre cada sector • Valores pseudo aleatorio sobre cada sector por veintisiete pasadas • Valores aleatorios durante cuatro pasadas sobre cada sector Total de sobreescrituras: 35	Alto
Grado 14. US Department of Defense (DoD 5220.22-M) + Gutmann Method	Combina los grados 13 y 10 Total de sobreescrituras: 35	Muy Alto

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 sobreescritura al medio de almacenamiento. Para ello, puede resultar de utilidad la tabla anterior.

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.

CONSIDERACIONES ADICIONALES PARA EL BORRADO SEGURO

En este apartado se abordarán algunos temas que son importantes para optimizar los procedimientos relacionados a la implementación del borrado seguro.

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.

<< Volver al inicio

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.

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. Este 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

Trabajo desde 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.

Campus Norte
Av. Universidad Anáhuac núm. 46,
col. Lomas Anáhuac, Huixquilucan,
Estado de México, C.P. 52786
Tel.: 55 56 27 02 10

Campus Sur
Av. de los Tanques núm. 865,
col. Torres de Potrero, Álvaro Obregón,
Ciudad de México, C.P. 01840
Tel.: 55 56 28 88 00

anahuac.mx/mexico