Borrado seguro de datos

¿Qué es el borrado de datos seguro?

El borrado de datos seguro es un procedimiento que hace irrecuperable la información almacenada en un disco duro o unidad de memoria extraíble. Para lograr este **borrado de datos** se aplican una serie de algoritmos que borran y sobrescriben los archivos del disco duro o memoria varias veces, de manera que estos no puedan ser recuperados, ni siquiera usando herramientas específicas para ello.

Es importante señalar que eliminar un archivo o documento del ordenador o una unidad externa enviándolo a la papelera y luego vaciando esta, o recurrir a un formateo estándar de una unidad de disco, no son métodos de **borrado seguro de disco duro** y, por tanto, no se produce un **formateo seguro del disco duro**.

En estos procedimientos, la información realmente no se borra, sino que el espacio que ocupaba queda libre para volver a escribir sobre él, de manera que hasta que ese espacio no es sobrescrito, la información que supuestamente hemos eliminado puede recuperarse empleando determinadas herramientas.

¿Cómo se realiza un borrado seguro?

En equipos con sistema operativo Windows, para hacer un **borrado seguro**, es necesario emplear herramientas o **software de borrado de datos** específicos, de los que existen varios. Estos softwares emplean algoritmos para borrar y reescribir la información varias veces (habitualmente, se considera que 7 reescrituras es suficiente para considerar que la información eliminada es ya irrecuperable).

Estos son algunas recomendaciones:

Una vez escogido el software de borrado seguro que vamos a utilizar, es cuestión de seguir las instrucciones para llevar a cabo el proceso. Dependiendo del programa usado y los algoritmos que emplee, podemos estar ante un proceso más o menos largo en el tiempo.

Los equipos macOS sí cuentan con una opción de borrado de datos seguro. Podemos acceder a ella desde «Utilidad de discos», pulsando en la unidad a formatear, elegir «Borrar» y «Opciones de seguridad». Tendremos que escoger el método que reescribe el disco 7 veces.

También es posible recurrir a empresas especializadas en el borrado y destrucción de datos, que, aparte de llevar a cabo el **borrado de archivos seguro** de nuestros dispositivos y unidades de memoria externa, también certificarán dicho borrado.

Herramientas de borrado seguro

Existen diferentes software o **herramientas de borrado seguro**; entre las más usadas encontramos:

- Eraser: una herramienta de borrado seguro muy completa y popular, ya que es sencilla de usar y gratuita. Cuenta con diferentes algoritmos, incluido el método Gutmann, que realiza 35 pasadas al disco duro.7
- Microsoft SDelete: (Secure Delete) es una herramienta gratuita, es una utilidad de línea de comandos desarrollada por Microsoft que se utiliza para sobrescribir de forma segura los archivos y eliminar de manera permanente su contenido en sistemas operativos Windows. Esta herramienta está diseñada para ayudar a proteger la confidencialidad de los datos al eliminarlos de manera segura, lo que evita la posibilidad de recuperar los archivos utilizando métodos de recuperación de datos convencionales.
- Active@ KillDisk: este software es recomendable para el borrado seguro de un ordenador, ya que el programa se instala en una memoria USB para poder realizar el borrado desde el arranque del ordenador. Tiene una versión gratuita, pero también licencias de pago.

¿Qué distintos métodos de borrado seguro podemos utilizar?

Son tres los **métodos de borrado seguro** que se consideran como tales, en concreto nos referimos a:

- **Destrucción física:** Consiste en destruir físicamente cualquier soporte de almacenamiento (sea este digital o físico), evitando así cualquier posibilidad de recuperación de la información. Existen diferentes métodos de destrucción física:
- **Desintegración, pulverización, fusión e incineración:** Cualquiera de estos métodos tiene como fin destruir completamente el soporte de almacenamiento. Se llevan a cabo en lugares autorizados para ello, donde la destrucción se hace forma segura y eficaz.
- **Trituración:** Se emplean para destruir papeles o soportes de almacenamiento flexibles. Es imprescindible que el tamaño de los fragmentos sea lo suficientemente pequeño como para que resulte imposible la recuperación de la información.
- **Desmagnetización:** Consiste en exponer los soportes de almacenamiento (discos duros, unidades de memoria externa, DVDs, etc.) a un potente campo magnético, que eliminar los datos almacenados en dicho soporte. Dependiendo del tamaño, forma y tipo de soporte magnético usado, la potencia necesaria para borrar los datos varía.
- **Sobre-escritura:** Consiste en escribir (sobre-escribir) un patrón de datos sobre los datos contenidos en un soporte de almacenamiento digital. Para garantizar que el borrado y **formateo seguro** de los datos, es necesario sobre-escribir la totalidad de la superficie de almacenamiento. Este

método de borrado seguro no se puede usar en discos que tengan partes dañadas, ni en CD y DVDs regrabables. En el caso de los discos duros SSD, hay estudios que demuestran que es posible recuperar información de los chips de memoria, por lo que no sería enteramente recomendable usarlo en ellos.

Cabe señalar que salvo la sobre-escritura, los otros dos métodos de borrado seguro de datos dejan inservible el dispositivo, por lo que no puede volver a utilizarse.

¿Por qué debemos realizar un borrado seguro de datos?

Hay varios motivos para realizar un borrado seguro de datos, especialmente para las empresas, puesto que en sus equipos, dispositivos móviles corporativos y unidades de memoria externa, como discos duros o pendrives, pueden guardar información confidencial, tanto de la propia empresa como referente a los datos personales de sus clientes y empleados.

Deshacerse de un ordenador o una unidad de memoria externa que no haya sido sometida a un borrado seguro y que un tercero pueda recuperar dicha información y utilizarla, se considera una brecha de seguridad, por lo mismo, siempre que sea necesario eliminar información confidencial, recurriremos a un borrado de datos seguro.

Otras razones para proceder con el borrado de datos seguro es evitar que información sensible o confidencial de la empresa (como datos financieros, estratégicos, contables, fiscales o información relativa a acuerdos, o propiedad industrial o intelectual, por ejemplo) caiga en manos de terceros, que pueden intentar usarla en su beneficio.

Aunque estamos hablando, sobre todo, de la importancia del borrado de datos seguro para las empresas, es algo que también debemos aplicar como particulares, especialmente cuando vendemos un ordenador de segunda mano o se lo legamos a alguien. Ya hemos dicho que formatear su disco duro no es suficiente y que si la persona que lo recibe siente curiosidad, podría recuperar los archivos que tuviéramos guardados en él. Por ello, recurrir a un borrado seguro en estas circunstancias siempre es recomendable.

La política de borrado seguro

Finalmente, para asegurarnos de que cumplimos con el borrado de datos seguro en la empresa o institución, se recomienda elaborar una **política de borrado seguro de la información** de los dispositivos electrónicos que emplea la empresa o institución y que vayan a ser retirados o cedidos a terceros ajenos a la misma.

La política de borrado seguro de una empresa o institución, que puede formar parte de sus procedimientos de protección de datos, deberá contemplar los siguientes elementos:

- Gestión de soportes (dispositivos):
    - Llevar un seguimiento de los dispositivos de la empresa, las personas o departamentos responsables de los mismos, la información que contienen y su clasificación en cuanto a confidencialidad para la empresa.
    - Supervisar los dispositivos que almacenan copias de seguridad de los datos de la empresa.
    - Asegurar que se cumple siempre la cadena de custodia cuando se trasladan dispositivos fuera de la empresa.
- Documentar las operaciones de borrado realizadas:
    - Emplear programas o herramientas de borrado que permitan obtener un registro documentado del proceso de borrado.
    - Si el borrado no se produce de manera suficiente por un fallo del dispositivo, esto debe documentarse y recurrir a métodos de destrucción física del dispositivo.