



UNIVERSIDAD DE SEVILLA

Guías de Seguridad

Guía para el borrado seguro de información



Índice

1. Introducción	5
2. Cuándo realizar un borrado seguro	5
3. Métodos de borrado seguro	5
3.1. Borrado lógico (software)	5
3.2. Borrado criptográfico	6
3.3. Destrucción física	6
4. Buenas prácticas del borrado seguro	6
Anexo I: Herramientas de borrado seguro	7
Herramientas de Software libre (Open Source)	7
Herramientas de software propietario	8



1. Introducción

El borrado seguro de equipos consiste en eliminar toda la información de un dispositivo de forma irreversible, para que nadie pueda recuperar los datos posteriormente. Es una práctica clave en seguridad informática y protección de datos personales, ya que permite:

- Proteger información confidencial
- Evitar filtraciones de datos
- Cumplir con normativas de protección de datos

2. Cuándo realizar un borrado seguro

Cuando se eliminan archivos vaciando la papelera de reciclaje o haciendo un formateo rápido de dispositivos, los datos siguen existiendo físicamente en el disco y pueden recuperarse con software especializado. Por ello es necesario utilizar un procedimiento seguro siempre que se vaya a dar de baja, reciclar o reutilizar por un tercero un dispositivo que almacene datos, incluyendo:

- Ordenadores de sobremesa
- Portátiles
- Servidores
- Discos duros HDD
- SSD
- Pendrives USB
- Smartphones
- Tablets

El [Procedimiento de baja, donación y reutilización de equipos informáticos en la Universidad de Sevilla](#) detalla los trámites administrativos necesarios.

3. Métodos de borrado seguro

3.1. Borrado lógico (software)

Se utilizan herramientas que sobrescriben los datos varias veces para que no puedan recuperarse.

Características:

- Sobrescritura múltiple de sectores
- Cumple estándares como DoD 5220.22-M
- Permite generar certificados de borrado

3.2. Borrado criptográfico

Consiste en eliminar o destruir las claves de cifrado de un disco. Muy usado cuando el disco está cifrado con:

- BitLocker
- FileVault

Al eliminar la clave, los datos quedan inaccesibles.

3.3. Destrucción física

Se destruye el soporte de almacenamiento en los siguientes casos:

- Cuando la naturaleza del soporte no permita un borrado seguro.
- Cuando así lo requiera el procedimiento asociado al tipo de información contenida por ser esta extremadamente sensible.

Algunos mecanismos de destrucción física:

- Trituración del disco
- Perforación de platos
- Desmagnetización (degaussing)
- Incineración controlada

4. Buenas prácticas del borrado seguro

Cuando los equipos contengan información sensible o datos personales clasificados de nivel alto por la LOPDyGDD (ideología, afiliación sindical, religión, creencias, origen racial o salud) se utilizarán para la destrucción y/o borrado sistemas, productos o equipos cuyas funcionalidades de

seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. Tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas.

- Borrado seguro de la información: se utilizarán productos certificados siempre que sea posible y siguiendo las recomendaciones del NIST SP 800-88 conforme a la Guía CCN-STIC 804 del Centro Criptológico Nacional.
- Destrucción: en caso que se detecte la necesidad de destrucción del equipo se procederá siguiendo las directrices de la Guía CCN-STIC 804, con el fin de evitar un posible acceso indebido a la información contenida.
- Si el equipo contiene información de los Sistemas corporativos y/o datos personales, el usuario debe avisar al responsable de la información correspondiente, que registrará el borrado, la destrucción y la baja del equipo en el registro correspondiente (CMDB en el caso de información corporativa con o sin datos personales o registro correspondiente del fichero declarado en el caso de contenga datos personales protegidos por la LOPDyGDD).
- Los Responsables del Servicio y de la Información determinarán si es necesario disponer de copias de seguridad de la información y registros de *logs*, y plazos de conservación para el cumplimiento legal.
- Si se contrata el borrado o destrucción de equipos a una empresa, esta tendrá que entregar un certificado de seguridad a la Universidad de Sevilla, que garantice que los datos no se podrán recuperar.

En todo caso, se recomienda:

- Hacer copia de seguridad antes del borrado
- Usar herramientas certificadas
- Verificar el borrado tras el proceso
- Documentar el procedimiento (auditoría)
- Generar certificado de destrucción o borrado

Anexo I: Herramientas de borrado seguro

Herramientas de Software libre (Open Source)

DBAN: herramienta de borrado seguro arrancable desde USB o CD. Permite borrar completamente discos duros mediante varios métodos de sobrescritura. Muy utilizada en entornos técnicos para borrado completo de HDD antes de reutilizar equipos. No es la mejor opción para SSD recientes.

Nwipe: proyecto open source basado en DBAN compatible con hardware más reciente. Permite seleccionar diferentes algoritmos de borrado seguro. Ideal para entornos Linux.

BleachBit: herramienta de limpieza de sistemas disponible para Linux y Windows. Permite eliminar archivos temporales y realizar borrado seguro de archivos individuales. Muy útil para mantenimiento de sistemas porque hace borrado selectivo.

Shred: comando incluido en sistemas Linux. Sobrescribe archivos varias veces para impedir su recuperación. Se usa desde terminal y es muy común en administración de sistemas para borrado de archivos.

Secure Delete: herramienta gratuita desarrollada por Microsoft dentro de Sysinternals. Permite borrar archivos y espacio libre de forma segura en Windows. Utiliza múltiples pasadas de sobrescritura.

Herramientas de software propietario

Blancco Drive Eraser: una de las soluciones profesionales más utilizadas en empresas. Certificada para cumplir normativas de seguridad y auditoría. Genera informes y certificados de borrado. Compatible con HDD, SSD y centros de datos.

KillDisk: software profesional para borrado seguro de discos. Permite crear medios de arranque para eliminar datos de forma completa. Soporta múltiples estándares de borrado.

Eraser: herramienta para Windows enfocada en eliminar archivos o carpetas específicas. Permite programar tareas de borrado automático. Usa diferentes algoritmos de sobrescritura.

CCleaner: incluye función para borrar espacio libre de forma segura. Fácil de usar para usuarios no técnicos.

BitRaser Drive Eraser: solución empresarial con certificaciones de seguridad. Permite borrar discos completos, archivos y dispositivos externos. Genera reportes para auditoría y cumplimiento normativo.

A continuación se incluye una comparativa de las herramientas con los tipos de dispositivos a los que aplican:

Herramienta	Tipo de dispositivo	Funciones principales	Sistemas compatibles	Ventajas
DBAN	HDD, portátiles, PCs	Borrado completo del disco mediante múltiples algoritmos de sobrescritura	Arranque independiente (Linux-based)	Muy fiable, fácil de usar, ampliamente conocida
nwipe	HDD, servidores, PCs	Borrado seguro con diferentes estándares (DoD, Gutmann, etc.)	Linux	Compatible con hardware moderno, open source
Shred	HDD, servidores	Sobrescritura segura de archivos o dispositivos	Linux / Unix	Ligero, integrado en el sistema, automatizable
BleachBit	Portátiles, PCs	Eliminación segura de archivos y limpieza del sistema	Windows / Linux	Interfaz sencilla y open source
Secure Delete	HDD, portátiles	Eliminación segura de archivos y espacio libre	Windows	Herramienta oficial de Microsoft, ligera
Blancco Drive Eraser	HDD, SSD, servidores, portátiles	Borrado certificado, informes y auditoría	Windows, Linux, arranque independiente	Cumple estándares internacionales, ideal para empresas
KillDisk	HDD, SSD, servidores	Eliminación completa del disco con múltiples algoritmos	Windows, Linux, arranque independiente	Compatible con muchos dispositivos y formatos
Eraser	HDD, portátiles	Borrado seguro de archivos individuales o carpetas	Windows	Programación de tareas y fácil uso
BitRaser Drive Eraser	HDD, SSD, servidores	Borrado certificado y generación de reportes	Windows, Linux	Enfocado a cumplimiento normativo y auditorías

Además de estas hay otras muchas herramientas de borrado disponibles en Internet y continuamente aparecen nuevas soluciones.