Procedimiento de borrado y destrucción de soportes de almacenamiento de información en la Universitat Politècnica de València

Aprobado por el Comité de Seguridad de la Información de la UPV el 9 de enero de 2025

1. Objetivo

El objetivo de este procedimiento es asegurar el borrado seguro de datos en dispositivos de almacenamiento utilizados por los distintos servicios y unidades de la Universitat Politècnica de València (UPV), en cumplimiento con el Esquema Nacional de Seguridad (ENS) en España, nivel MEDIO. Este procedimiento garantiza que los datos sean eliminados de manera irreversible, y que se mantenga un registro trazable del proceso.

2. Ámbito de aplicación

Este procedimiento se aplica a todos los dispositivos de almacenamiento (discos duros magnéticos, discos SSD, etc.) que contengan o hayan contenido datos personales o datos propiedad de la UPV o en general cualquier soporte que se haya utilizado con fines profesionales en la UPV. Incluye discos de ordenadores personales, servidores, unidades externas y cualquier otro medio informático utilizado en la UPV.

3. Determinación de cuándo borrar un disco

Siempre que un determinado soporte informático se vaya a reutilizar para otro propósito distinto se debe destruir toda la información que pueda contener. Tanto si la nueva utilidad que se le vaya a dar sea en la propia universidad como si forma parte de una cesión a terceros (retirada de equipos para reciclar, donaciones, etc.) se debe destruir la información almacenada de forma segura.

Debemos suponer que todos los soportes pueden contener información sensible. Los sistemas operativos actuales hacen un uso extensivo de las caches y de logs, pudiendo encontrarse registros de actividad en particiones que en principio no estaban destinadas a tal fin. Por este motivo, todo medio que haya sido utilizado en alguna actividad informática será objeto del borrado (o destrucción) antes de ser retirado o usado en otro ámbito.

El borrado seguro de discos debe llevarse a cabo en los siguientes casos:

- Antes de la reutilización de un disco en otro puesto de trabajo con un perfil de permisos o una actividad distinta a la actual.

- Antes de la donación de equipos.
- Cuando un dispositivo se retire de servicio y no vaya a ser reutilizado.
- Cuando un disco o medio se declare defectuoso y no pueda repararse. En este caso se procederá a la destrucción física.
- En el caso de finalización de contratos que impliquen la devolución de equipos.

En el caso particular de la reinstalación de ordenadores en aulas no es obligatorio el borrado, ya que es habitual que el ámbito de uso sea el mismo.

El borrado se debe producir en el momento que el disco deja de ser utiliza. No hay que esperarse a realizar el borrado cuando se vaya a hacer uso de él más adelante.

4. Responsable del borrado

El Centro de Atención a Usuarios (CAU) del ASIC es el responsable del proceso de borrado seguro de discos. Esta función puede ser delegada a los centros y departamentos de la UPV, siempre y cuando se sigan las directrices establecidas en este procedimiento.

5. Métodos de borrado de discos magnéticos y discos SSD

- **Software de borrado**: Siempre que sea posible se utilizará la herramienta «Olvido», proporcionada por el CCN-CERT, del que la UPV dispone de licencias, y se borrará el disco completo con el método de borrado CCN-ENS (1 pase). En los casos en que se solicite por parte del servicio un borrado más estricto se utilizará el procedimiento CCN-CLASIFICADO (3 pases).
- **Borrado desde el equipo en el que está instalado el disco**: En los casos en que sea posible, se realizará un borrado desde el propio equipo en el que está instalado el disco (o los discos en caso de contener más de uno). En este caso se arrancará el equipo con un disco USB que contenga un sistema operativo ligero y el software Olvido previamente instalado.
- **Borrado desde un equipo especializado**. En los casos en que no sea posible arrancar el equipo en el que estaba instalado el disco será necesario extraer los discos duros que contenga y llevarlos a las instalaciones del CAU para realizar un borrado en un equipo dedicado al borrado, equipado con bahías externas con los distintos buses existentes en el mercado, desde el cual realizar el borrado lógico.
- **Implementación descentralizada**: Los discos magnéticos y SSD pueden ser borrados directamente en los centros o departamentos. El procedimiento puede ejecutarse utilizando un ordenador sin disco fijo que cargue un software de borrado desde un USB.

6. Destrucción física de medios

Cuando no se pueda realizar el borrado lógico de la información, se procederá a la destrucción física. Por ejemplo, cuando no se disponga del software de borrado específico, no se disponga de la controladora o el bus de conexión o cuando el disco presente fallos de funcionamiento, se deberá destruir el medio físico.

6.1. Destrucción física de discos defectuosos

- **Destructores físicos de discos**: En el CAU del ASIC se dispone de un destructor físico de discos para aquellos discos que no funcionen y no puedan ser borrados de manera lógica. Este equipo asegurará la destrucción completa de los discos, garantizando que la información no pueda ser recuperada.
- **Proceso de destrucción**: Los discos defectuosos que no puedan borrarse mediante métodos lógicos deben ser identificados y transportados al ASIC para su destrucción física.
- **Evidencias de destrucción**: Como parte del proceso, se generará un registro con la fecha, el número de serie del disco y el método de destrucción, manteniendo un certificado que acredite la eliminación segura del dispositivo.

6.2. Contenedores de seguridad cambiar por espacio de acceso restringido

- **Almacenamiento temporal**: Los discos defectuosos y otros medios que no puedan ser borrados deben depositarse en contenedores de seguridad cerrados y ubicados en lugares específicos dentro del ASIC.
- **Destrucción centralizada**: La destrucción física se gestionará de manera centralizada en el ASIC, utilizando trituradoras físicas para tal fin.

7. Infraestructura y recursos necesarios

- **Equipo dedicado para borrado**: Se dispondrá de un equipo dedicado a la tarea de borrado, con múltiples interfaces de conexión para facilitar el proceso de borrado de discos de diferentes tipos.
- **Espacio para el servicio de borrado**: Debe habilitarse un espacio específico en el ASIC para llevar a cabo estas operaciones. Este espacio debe estar diseñado para albergar varios discos en paralelo y así agilizar el proceso de borrado, especialmente en grandes cantidades (como por ejemplo en donaciones o renovaciones masivas de equipos).

8. Trazabilidad y evidencias

Debe quedar registro de tanto el borrado lógico como la destrucción del soporte físico.

- **Registro de operaciones de borrado**: Cada operación de borrado debe ser registrada. El registro incluirá:
    - Tipo de disco (magnético, SSD)
    - Número de serie
    - Fecha del borrado
    - Método o software utilizado
    - Responsable del borrado
- **Certificados de borrado**: Para auditorías y cumplimiento del ENS, deben generarse certificados de borrado que se almacenen en un repositorio central accesible durante un mínimo de 5 años.

9. Guía y capacitación

- **Elaboración de una guía**: Se distribuirá una guía de borrado de datos a través de la wiki del ASIC que detalle los procedimientos y herramientas a utilizar. Esta guía estará disponible para todos los técnicos e informáticos de la UPV.
- **Capacitación**: Se realizarán sesiones de capacitación periódicas para asegurar que el personal involucrado esté actualizado en las mejores prácticas de borrado de datos y seguridad.

10. Revisión y actualización del procedimiento

Este procedimiento se revisará anualmente o cuando haya cambios relevantes en la tecnología de almacenamiento y borrado de datos.