

# BORRADO SEGURO DE DATOS

¿Cómo eliminar la información para dejar limpios los dispositivos?



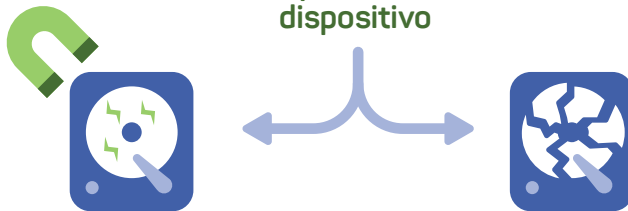
## Borrados más habituales



Esta forma de borrar **no es segura**. La información **no se elimina** totalmente y **se puede recuperar**.

## Formas seguras de borrado de datos

Si no se quiere reutilizar el dispositivo



### DESMAGNETIZACIÓN

Exposición de los soportes de almacenamiento a un potente campo magnético, que elimina los datos almacenados en el dispositivo.  
Sólo válido para dispositivos de almacenamiento magnético: discos duros, disquetes, cintas magnéticas de backup, etc...

### DESTRUCCIÓN FÍSICA

Inutilización del soporte que almacena la información en el dispositivo para evitar la recuperación posterior de los datos.  
Diferentes tipos de técnicas: desintegración, pulverización, fusión, incineración y trituración.  
Válido para todo tipo de dispositivos: disco duro, USB, CD, DVD...

Si se quiere reutilizar el dispositivo




### SOBRE-ESCRITURA

Para asegurar la completa destrucción se debe escribir la totalidad de la superficie de almacenamiento.  
Se realiza accediendo al contenido de los dispositivos y modificando los valores almacenados, por lo que no se puede utilizar en aquellos que están dañados ni en los que no son regrabables, como los CD y DVD.  
Válido para todos los dispositivos regrabables: discos duros, USB,...

# BORRADO SEGURO DE DATOS

¿Cómo eliminar la información para dejar limpios los dispositivos?



Soporte	Tipo	Destrucción física	Desmagnetización	Sobre-escritura
 Discos Duros	Magnético	✓	✓	✓
 Discos Flexibles	Magnético	✓	✓	✓
 Cintas de Backup	Magnético	✓	✓	✓
 CD	Óptico	✓	✗	✗
 DVD	Óptico	✓	✗	✗
 Blu-ray Disk	Óptico	✓	✗	✗
 Pen Drive	Electrónico	✓	✗	✓
 Discos Duros SSD	Electrónico	✓	✗	✓