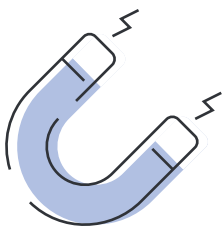


## ¿A QUIÉNES VAN DIRIGIDAS LAS HERRAMIENTAS DE BORRADO SEGURO?

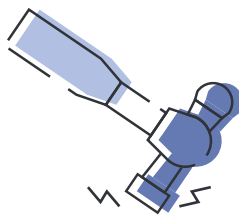
El borrado seguro de datos de un dispositivo es un proceso mediante el cual se hace irrecuperable la información que estaba almacenada en un disco duro o en una unidad de memoria extraíble. Para lograr el borrado completo de la información, se deben emplear mecanismos de destrucción y borrado adecuados, evitando que los datos queden al alcance de terceros.

## TIPOS DE HERRAMIENTAS DE BORRADO SEGURO

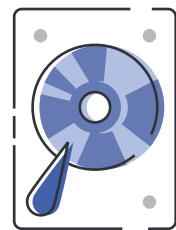
Los diferentes medios para la realización de un borrado seguro pueden ser:



La desmagnetización



La destrucción

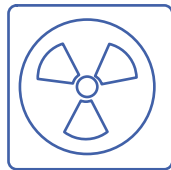


La sobrescritura del área de almacenamiento

## EJEMPLOS DE HERRAMIENTAS DE BORRADO SEGURO



Microsoft SDelete



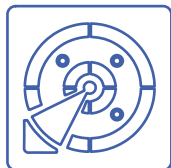
Eraser



Active@ KillDisk



HDShredder



Hardwipe



BleachBit



Darik's Boot and Nuke (DBAN)



File Shredder

## BENEFICIOS DE LAS HERRAMIENTAS DE BORRADO SEGURO

- Alargar la vida útil de los soportes magnéticos de almacenamiento.
- Lograr una mayor seguridad en el almacenamiento de datos y minimizar el riesgo de exposición o filtrado de datos.
- Contar con una alternativa a la destrucción física de los dispositivos.



Cyberzaintza, la Agencia Vasca de Ciberseguridad, pone a disposición de cualquier organización su "[Catálogo de ciberseguridad](#)", donde encontrará a los proveedores especialistas en las herramientas de borrado seguro.