



BORRADO SEGURO DE DATOS

El borrado seguro de datos consiste en eliminar la información digital de manera que no pueda ser recuperada **de ninguna forma**.

Hay 3 métodos disponibles para llevarlo a cabo:

Clear (Eliminación lógica)

Se sobrescriben los **datos existentes** con **ceros o patrones aleatorios**.

Purge (Eliminación profunda)

Se aplican métodos complejos e irreversibles, como el borrar **las claves de cifrado** que protegen los datos, volviendo inútil el contenido cifrado.

Destroy (Destrucción física)

Los **dispositivos de almacenamiento** se destruyen físicamente, los datos desaparecen para siempre.



Un borrado seguro debe comportarse como un agujero negro: **nada, absolutamente nada, puede escapar**.

El **NIST SP 800-88 Rev.1** es la guía de referencia más utilizada para definir métodos y procedimientos de borrado seguro de datos.

NIST

El borrado seguro no solo elimina archivos, también protege la confidencialidad, integridad y privacidad de la información. Aplicar métodos y normas reconocidas evita fugas de datos y garantiza el cumplimiento normativo.



Bibliografía

National Institute of Standards and Technology. (2014). Guidelines for media sanitization (NIST SP 800-88 Rev. 1). U.S. Department of Commerce.