Configuración de dispositivos y sistemas informáticos

Bastionado de Redes

Curso de Especialización en Ciberseguridad

01

Hardening I

¿QUÉ ES EL HARDENING?

→ Proceso de securizar un sistema reduciendo su superficie de vulnerabilidad.

→ Permite mitigar las amenazas y vulnerabilidades

→ Nunca termina:

Sistema no estático + nuevos ataques
=
Necesidad de fortalecer

ETAPAS

→ Kernel

→ Arranque

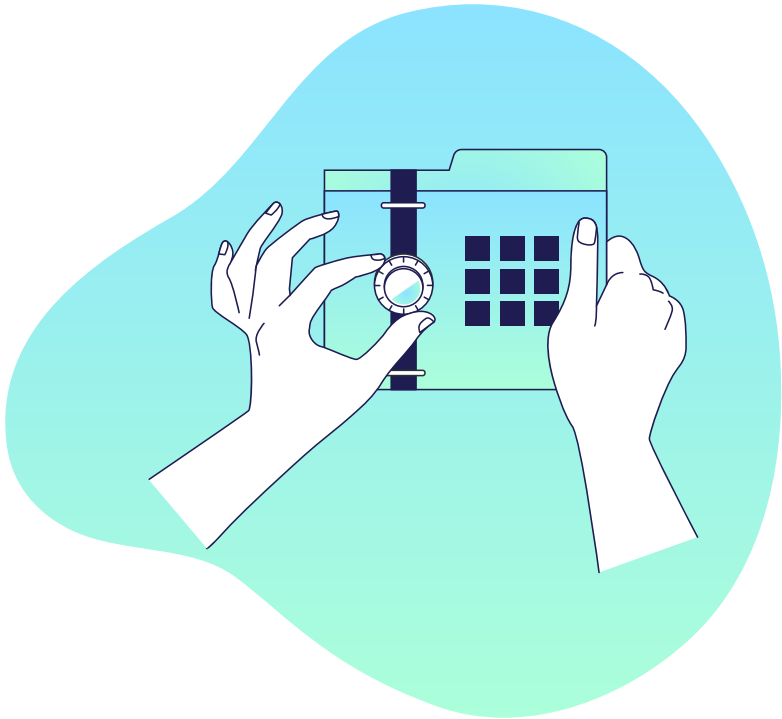
→ Post arranque (funcionamiento del sistema)

→ Aplicaciones

KERNEL

→ Instalación de un nuevo kernel/distribución:
  → Obtener las últimas versiones de los fuentes o binarios del kernel o distribución
  → Instalar el kernel/distribución

→ Amenazas:
  → Fuentes/distribución
  → Control de descarga - Comprobar hash o firma
  → Compilar el kernel: Tools y opciones de compilación

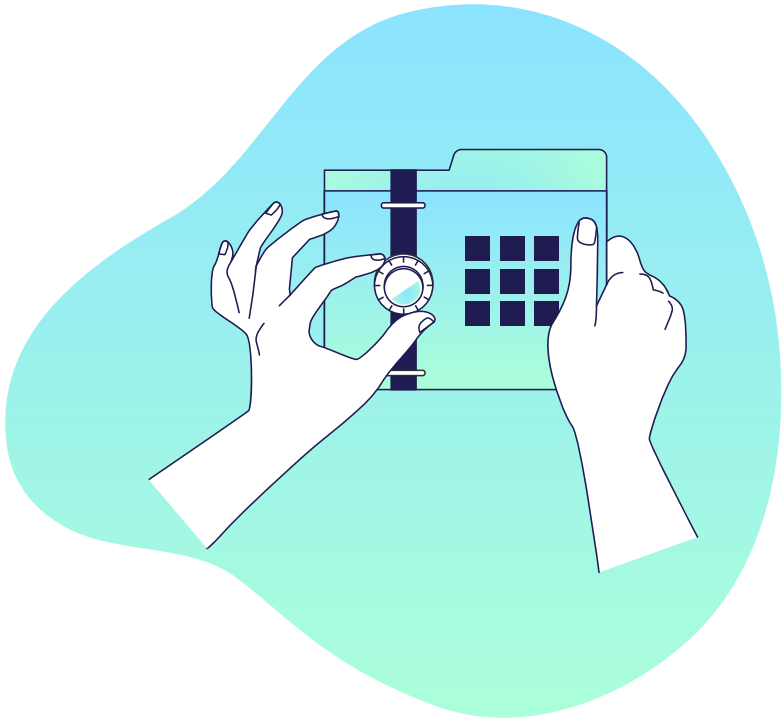


INSTALACIÓN KERNEL

→ ¿Qué debemos considerar?

→ Habilitar claves shadow con hash
→ Elegir una clave de root fuerte
→ Crear un usuario adicional con una clave fuerte
→ Habilitar un firewall
→ No instalar paquetes que no sean necesarios: juegos, servidores de red, herramientas de desarrollo, de impresión, etc...

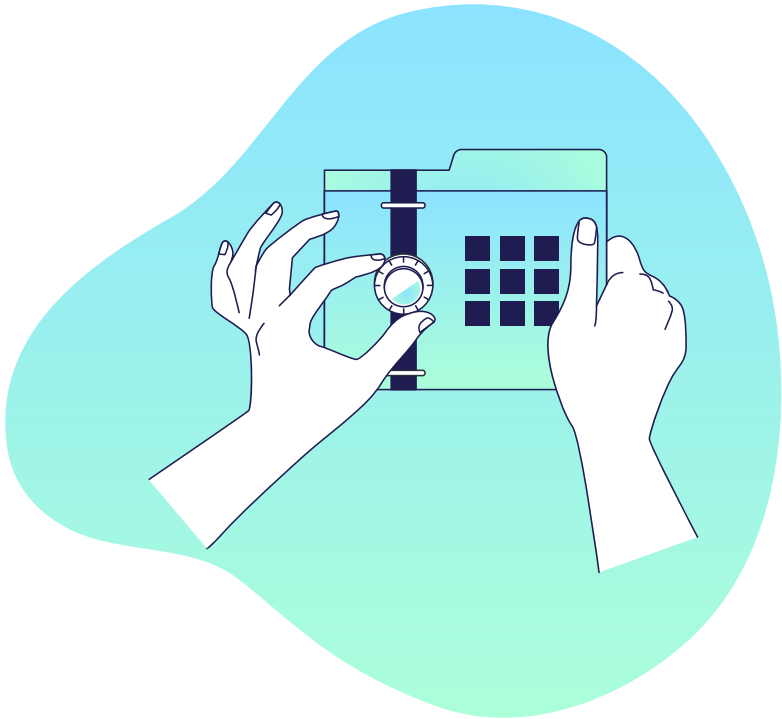
¿Deberíamos configurarlo conectado o desconectado de la red?



¿Y SI REPASAMOS UN POCO DE CRIPTOGRAFÍA?

→ md5 (1991)
- → Rápido
- → Débil
- → Un poco más robusto si añadimos un salt
- → Produce colisiones. Paradoja del cumpleaños

→ Blowfish (1993)
- → Sigue considerándose seguro
- → Rápido
- → Aún así, no es el más recomendado

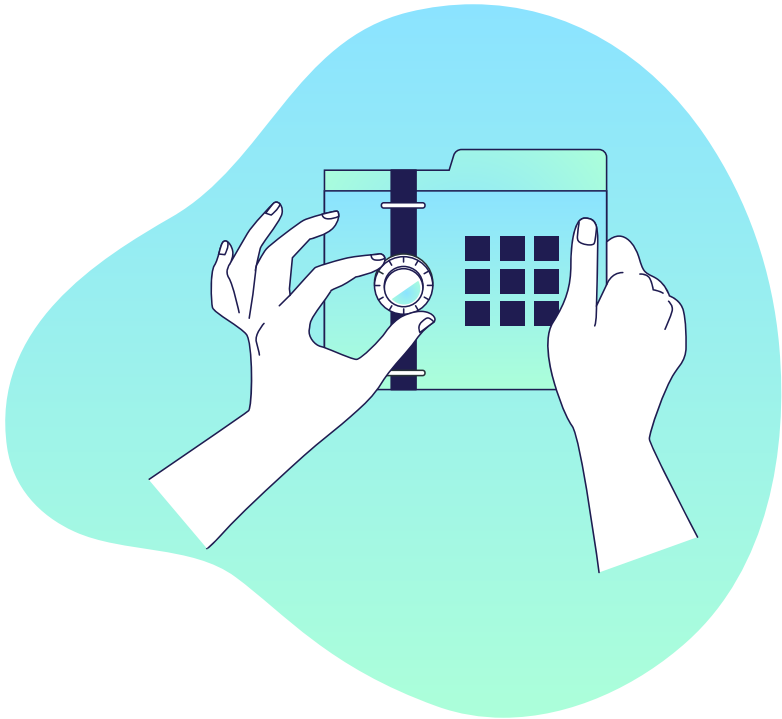


¿Y SI REPASAMOS UN POCO DE CRIPTOGRAFÍA?

→ SHA-256 (2002)

→ Bastante seguro (por ahora....)
→ Equilibrio entre seguridad y coste computacional
→ Algoritmo eficiente
→ Alta resistencia de colisión
→ Bitcoin

¡TODO LOS HASHES RESULTANTES TIENEN 40 CARACTERES!



Seguridad en el arranque

¿Cómo creéis que podría comprometer una atacante a una máquina a la que puede acceder de forma física?

Seguridad en el arranque

→ Manipular un proceso para arrancar un sistema funcional desde CD/DVD o pendrive

→ Cambiar proceso de arranque

→ Manipular físicamente el dispositivo

Seguridad en el arranque

Dos grandes problemas:

→ Algunos sistemas permiten ciertos accesos a quienes pueden arrancar la máquina

→ No poder arrancar la máquina ya es un perfecto ataque DDoS

¿Cómo podemos evitarlo?

Seguridad en el arranque

Podemos evitarlo:

→ Protegiendo la BIOS-UEFI

→ Protegiendo el cargador de arranque

→ Deshabilitando arranques desde otros dispositivos

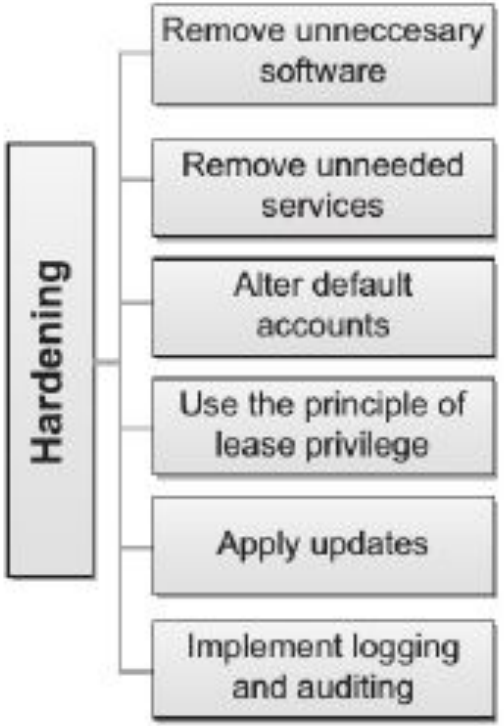
→ Protegiendo los servicios que acceden a la red en el arranque

Seguridad post arranque

¡Advertencia!

Algunos cambios pueden tener efectos inesperados en el sistema.

Una máquina de producción no es el lugar adecuado para experimentar.



Seguridad post arranque - Eliminar software

→ Eliminar todo el que sea innecesario

→ Planificar el software a instalar (mínimo necesario)

→ Eliminar/restringir el uso de compiladores y herramientas de desarrollo para evitar que construya el malware de forma local

Seguridad post arranque - Eliminar servicios innecesarios

→ Minimizar los servicios por defecto de las distribuciones (compartir información en red, localizar a otros dispositivos, transferencia de archivos....)

→ Localizar otros servicios innecesarios con nmap (puertos) y lsof.

→ Eliminar después de desactivar

Seguridad post arranque - Configurar accesos

→ Control de:

- → Consolas de acceso
- → Usuarios y grupos
- → Cuentas por defecto

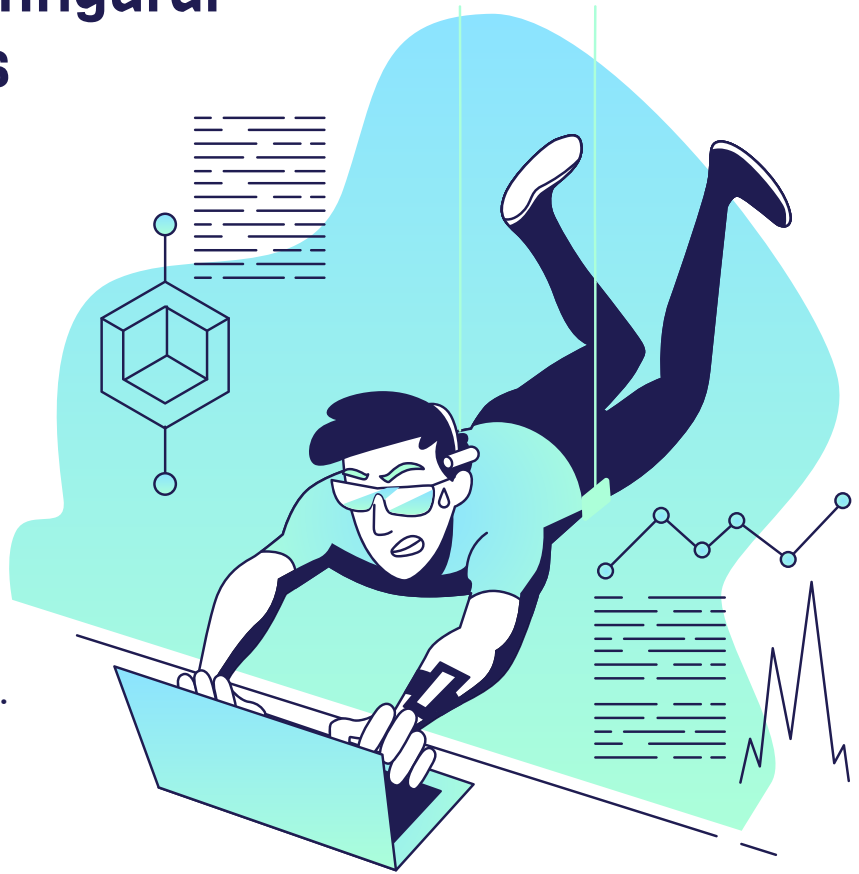
Seguridad post arranque - Configurar accesos - Consola de accesos

→ Root login. Ej: /etc/securetty o PAM

→ Controlar mensajes en las pantallas de login

→ Dan información que no deben conocer sobre nuestro sistema

→ Es buen método para ofrecer avisos y notificaciones a los usuarios legítimos. Ej. /etc/issue y /etc/issue.net



Seguridad post arranque - Configurar accesos - Usuario y grupos

→ Controlar shells

→ /sbin/nologin y /bin/false pueden subvertir
→ /dev/null no registran intentos de login

→ Claves shadow con cifrado fuerte y controlar PAM

→ Borrar usuarios y grupos no necesarios

Seguridad post arranque - Configurar accesos - Cuentas por defecto

→ Controlar cuentas estándares conocidas (mantenimiento, control servicios...)

→ Supervisar:

→ Permisos y claves

→ Shells permitidos

→ Deshabilitar si no son necesarias

Ej. Si no usamos NFS, no es necesario el usuario nfsnobody

Seguridad post arranque - Principio mínimo privilegio

“Sólo permitiremos a una parte el permiso mínimo necesario para realizar la función”

→ Asignar roles de administrador/usuario (incluso siendo la misma persona)

→ Controlar acceso a elementos del sistema de archivos (permisos sobre archivos)

Seguridad post arranque - Actualizaciones

→ Nuevos ataques = nuevos parches

→ Igual que con la instalación

→ Comprobar la integridad - firma
→ Máquina desconectada de la red

Seguridad post arranque - Log y auditoría

→ Registrar eventos significativos

- → Uso de privilegios administrativos
- → Login-out usuarios
- → Login erróneos
- → Cambios en el SO (archivos críticos)

→ Configurar syslog y revisar los logs.

→ Herramientas específicas. Ej. psacct (process account)

02

Hardening II

Estándares

→ Center for Internet Security (https://www.cisecurity.org/)

→ Federal Desktop Core Configuration (FDCC)

→ NSA Security Configuration Guides (https://csrc.nist.gov/projects/national-checklist-program)

Guías

→ CIS benchmarks (https://learn.cisecurity.org/benchmarks?category=benchmarks.os.linux)

→ NSA Security Configuration Guides (https://www.nsa.gov/Resources/Media-Destruction-Guidance/)

→ DISA STIGs (https://www.stigviewer.com/stigs)

Herramientas

→ Linux: SCAP, Lynis, Bastille, tripwire....

→ Windows: Secunia Online Software Inspector, Microsoft Baseline Security Analyzer (MBSA)

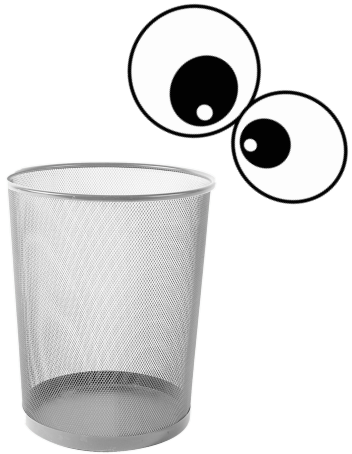
Facilitan el proceso pero... hay pocas, pueden estar desactualizadas, limitadas en soporte o difíciles de usar

03

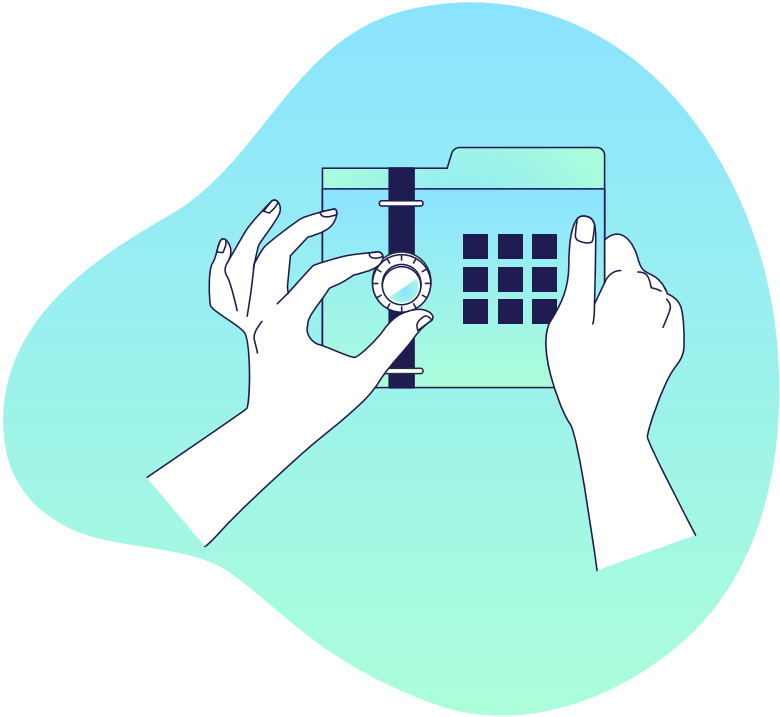
Limpieza de memoria

Limpieza de memoria

Si ya no nos hace falta un dispositivo de almacenamiento... ¿cómo nos deshacemos de él?



¡Cuidado con el Dumpster Diving!

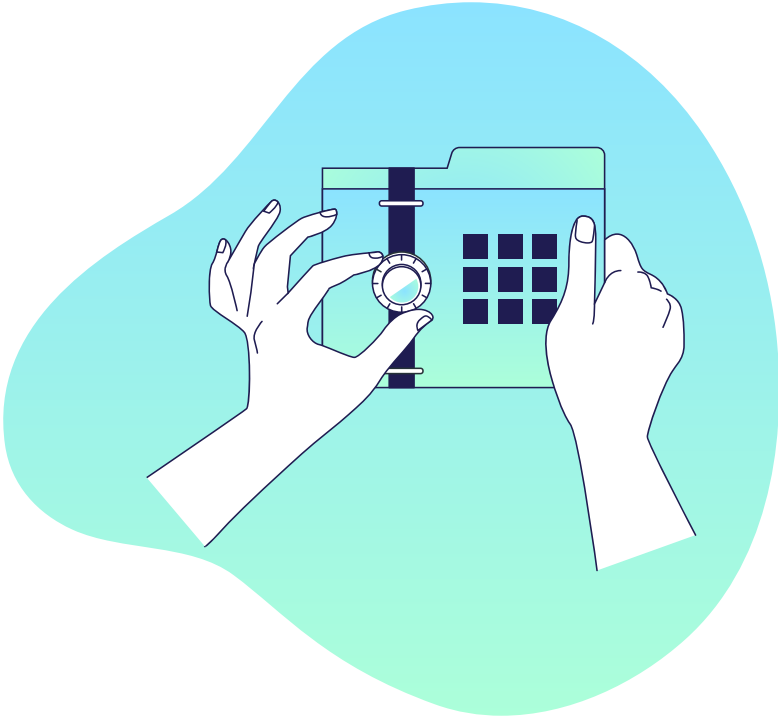


Limpieza de memoria

¿Cómo borramos de forma segura un dispositivo de almacenamiento?

Debemos sanitizar o purgar ese medio

DBAN

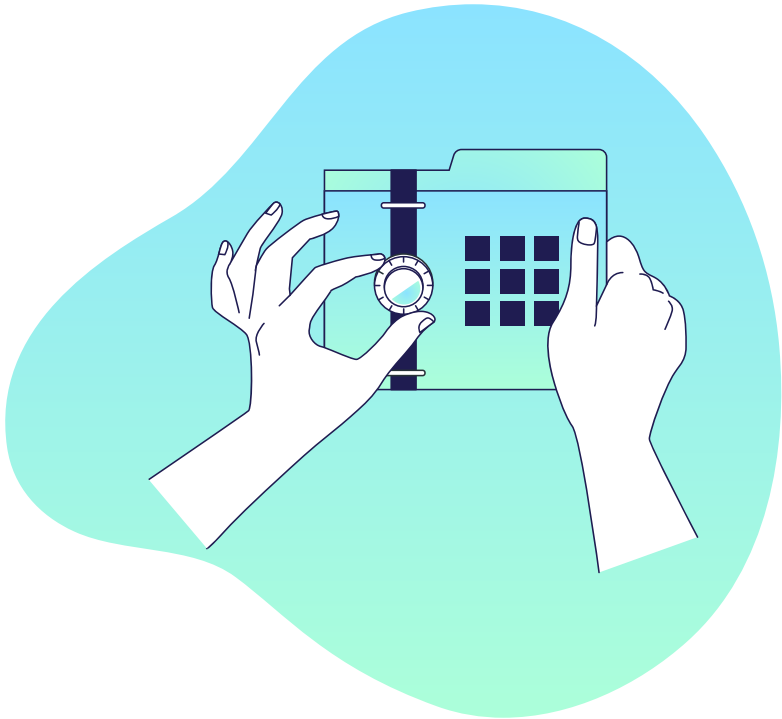


Limpieza de memoria - ISO 15713

→ **ISO 15713:2010** - Destrucción segura del material confidencial, código de buenas prácticas

→ Requisitos para la gestión y control de recogida, transporte y destrucción del material confidencial.

→ Nivel de triturado según el tipo de información a eliminar y el soporte

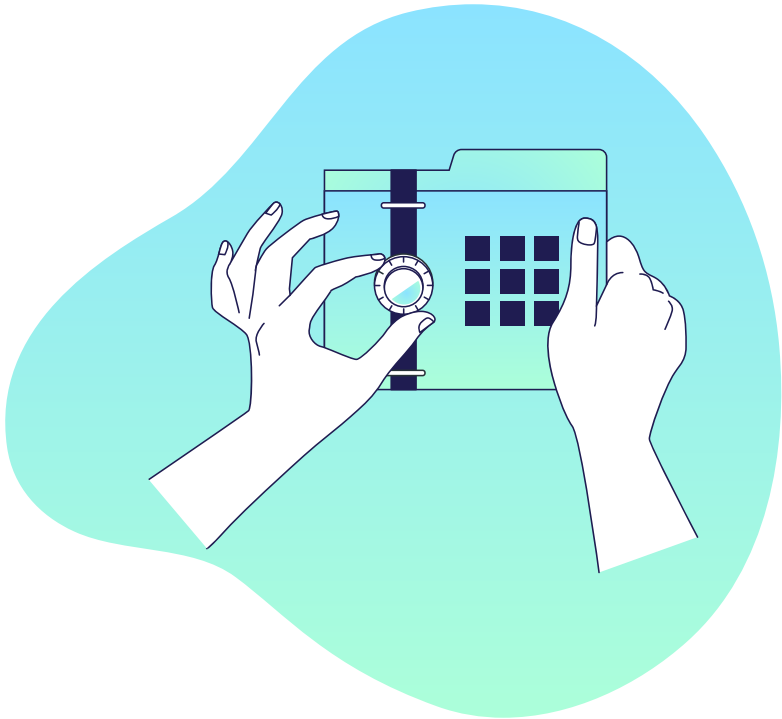


Limpieza de memoria - No destrucción de la información

→ Eliminar, Supr, Delete...

→ Borrar papelera de reciclaje

→ Formatear



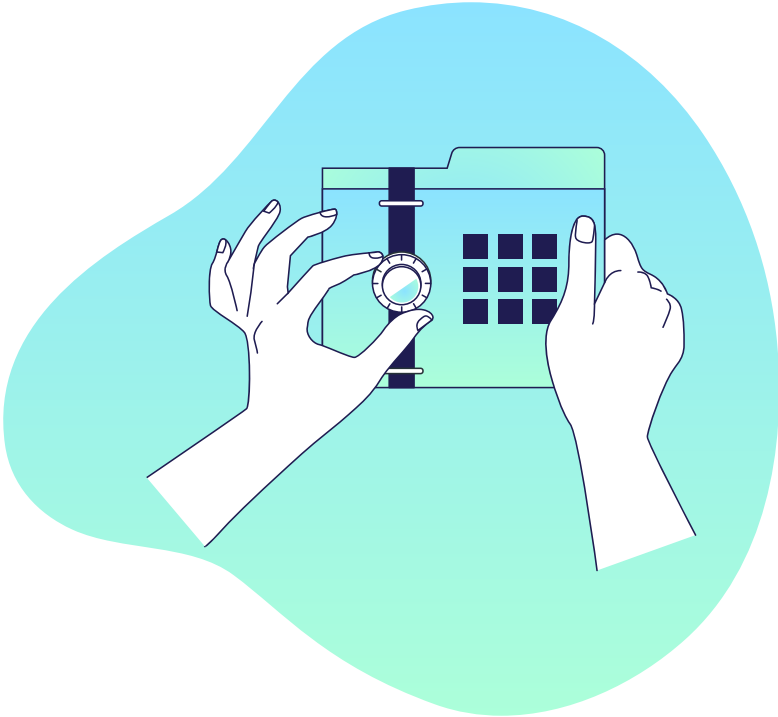
Limpieza de memoria - Destrucción de la información

→ Desmagnetización

→ Destrucción física

→ Sobre-escritura

DBAN



Limpieza de memoria - Destrucción de la información

DESTRUCCIÓN FÍSICA	DESMAGNETIZACIÓN	SOBRE-ESCRITURA
✓ Eliminación de forma segura de la información	✓ Eliminación de forma segura de la información	✓ Eliminación de forma segura de la información
✗ Un sistema de destrucción para cada soporte	✗ Una configuración del sistema para cada soporte	✓ Una única solución para todos los dispositivos
✗ Dificultad de certificación del proceso	✗ Dificultad de certificación del proceso	✓ Garantía documental de la operación
✗ Necesidad de transportar los equipos a una ubicación externa	✗ Necesidad de transportar los equipos a una ubicación externa	✓ Posibilidad de eliminación en las propias oficinas
✗ Medidas extraordinarias para garantizar la cadena de custodia	✗ Medidas extraordinarias para garantizar la cadena de custodia	✓ Garantía de la cadena de custodia
✓ Destrucción de dispositivos, no regrabables, ópticos	✗ Sólo válido para dispositivos de almacenamiento magnético	✗ No válido para dispositivos no regrabables ni ópticos
✗ Destrucción definitiva y dificultad de reciclaje de materiales	✗ Tras el proceso el dispositivo deja de funcionar correctamente	✓ Reutilización de los dispositivos con garantías de funcionamiento.

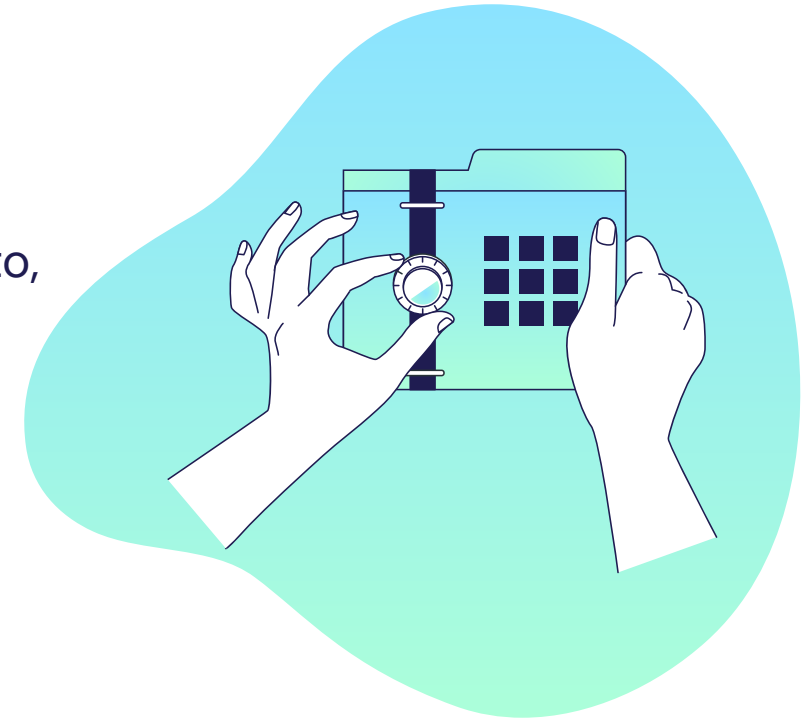
Limpieza de memoria - Destrucción de la información

SOPORTE	TIPO	DESTRUCCIÓN FÍSICA	DESMAGNETIZACIÓN	SOBRE ESCRITURA
Discos Duros	Magnético	✓	✓	✓
Discos Flexibles	Magnético	✓	✓	✓
Cintas de *Backup*	Magnético	✓	✓	✓
CD	Óptico	✓	✗	✗
DVD	Óptico	✓	✗	✗
Blu-ray Disc	Óptico	✓	✗	✗
Pen Drive	Electrónico	✓	✗	✓
Discos Duros SSD	Electrónico	✓	✗	✓

Limpieza de memoria - Política de borrado seguro

→ Gestión de soportes adecuada
    → Inventario y seguimiento
    → Supervisión dispositivos backup
    → Controlar operaciones (mantenimiento, reparación, sustitución)
    → Cadena de custodia traslados

→ Documentación de las operaciones de borrado realizadas
    → Certificado de destrucción
    → Documentar fallos destrucción



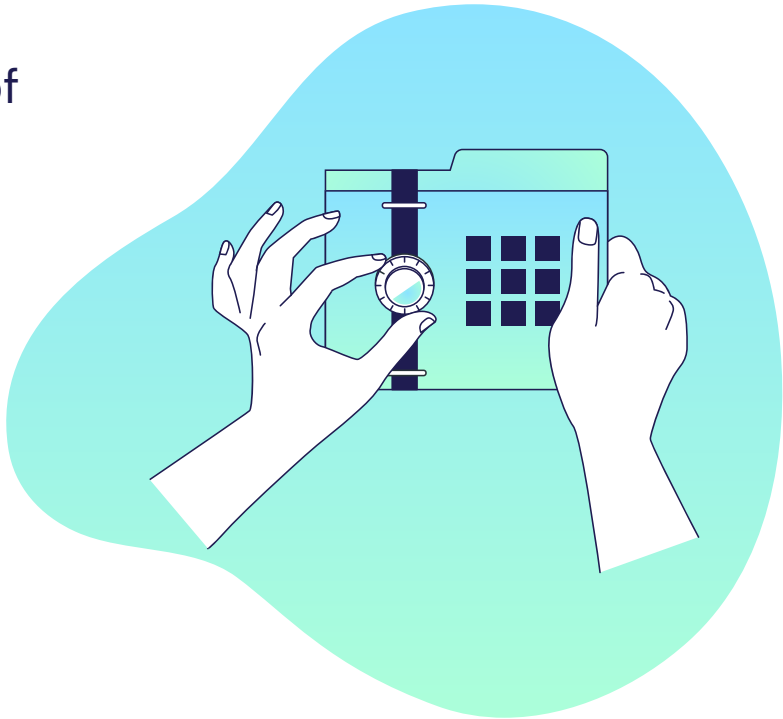
Limpieza de memoria - Sobreescritura

→ Método de las **3 pasadas** - Departament of Defense (DoD). → Método **DoD 5220-M**

→ Método **Gutmann**. Microscopios de fuerza magnética. → 35 pasadas

→ Método **Schneier** y método **VSITER** → 7 pasadas

→ NIST 800-88 → DoD 5220.22-M



Limpieza de memoria - DBAN

https://dban.org/

Práctica 3, ya disponible en Moodle.