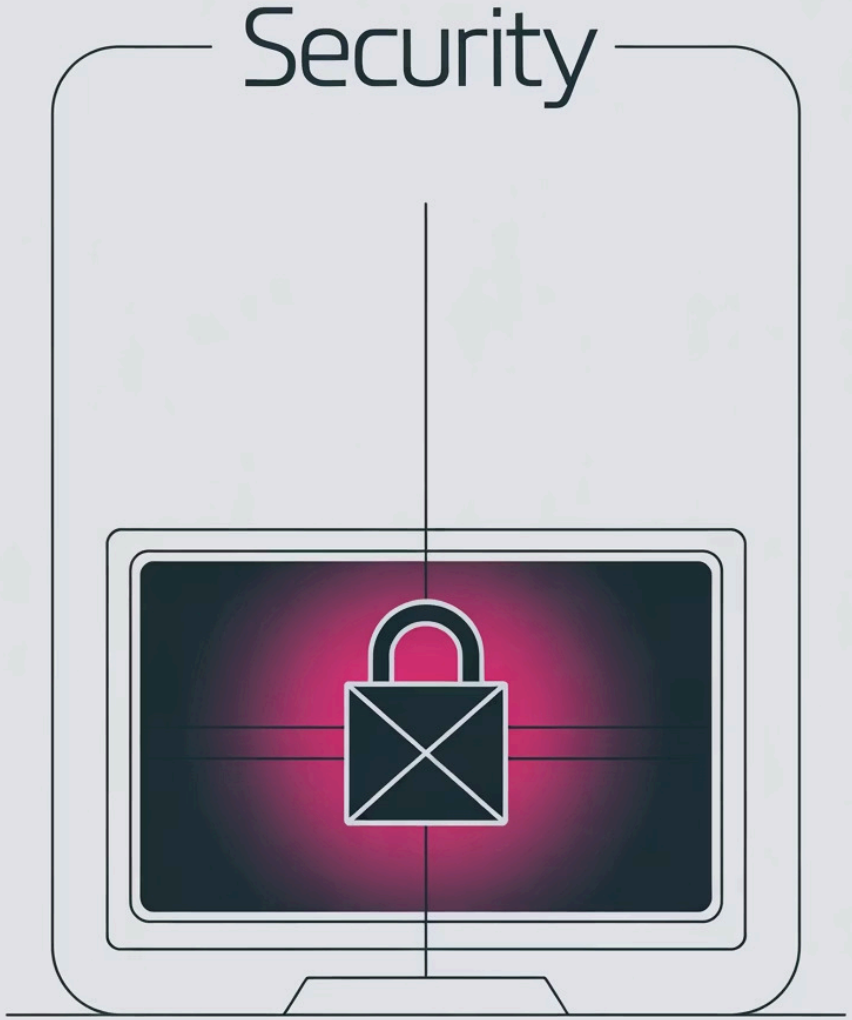


Cifrado de Datos en los Sistemas Operativos

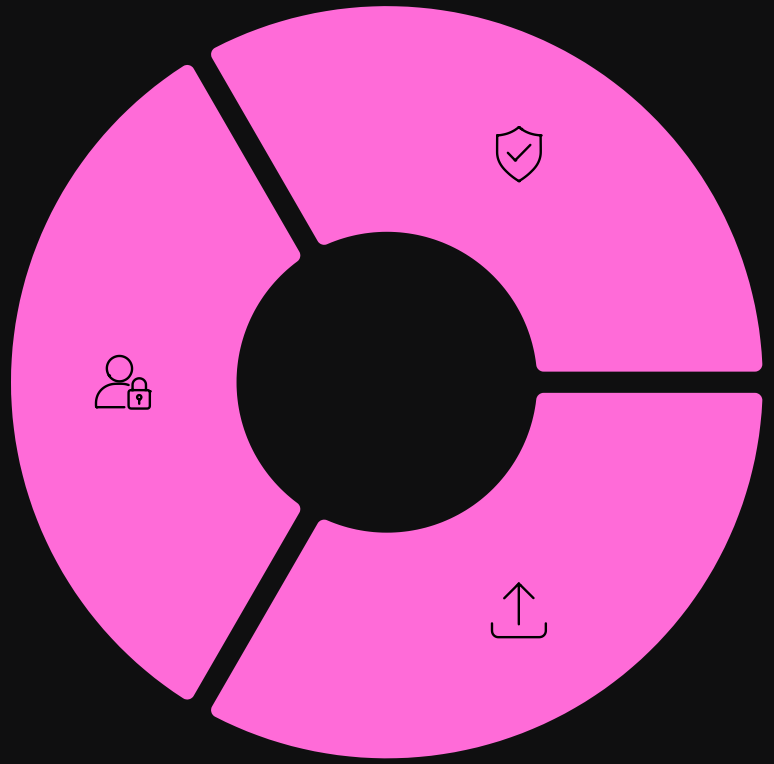
Sistemas Operativos | González Martínez Michelle Paola • Maya Torres Bruno

Una técnica de seguridad que transforma la información almacenada para que no pueda leerse sin la clave adecuada, garantizando que los datos permanezcan protegidos del acceso no autorizado.

La Tríada CIA: Base de la Seguridad

Confidencialidad

Protección contra acceso no autorizado a la información



Integridad

Garantía de que los datos no sean alterados

Disponibilidad

Acceso a la información cuando se necesita

El cifrado de datos cubre principalmente la confidencialidad, pero también aporta integridad al evitar modificaciones no autorizadas.

Implementación en sistemas operativos

Sistema de archivos cifrado

Integración directa en el sistema de archivos (APFS en macOS, EFS en Windows) o mediante una capa debajo del sistema usando drivers especiales.

Gestión de claves

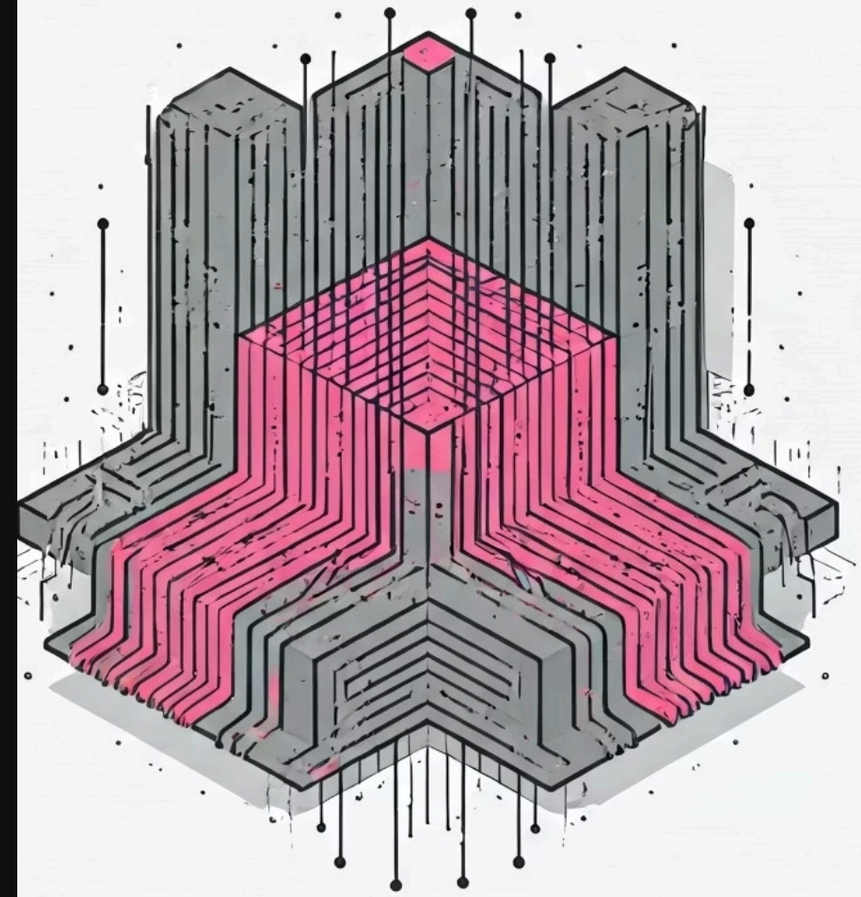
El sistema genera una clave maestra aleatoria protegida por la contraseña del usuario. Windows usa TPM mientras que Mac usa Secure Enclave.

Proceso de E/S cifrada

"Todo bloque que permanece en el disco está cifrado, y sólo existe en forma legible temporalmente en memoria cuando un programa autorizado lo solicita".

Cifrado de disco completo vs. Archivo

El cifrado de disco completo (FDE) protege todos los datos de una partición mediante una clave maestra única, mientras que el cifrado a nivel de archivo cifra archivos individuales.



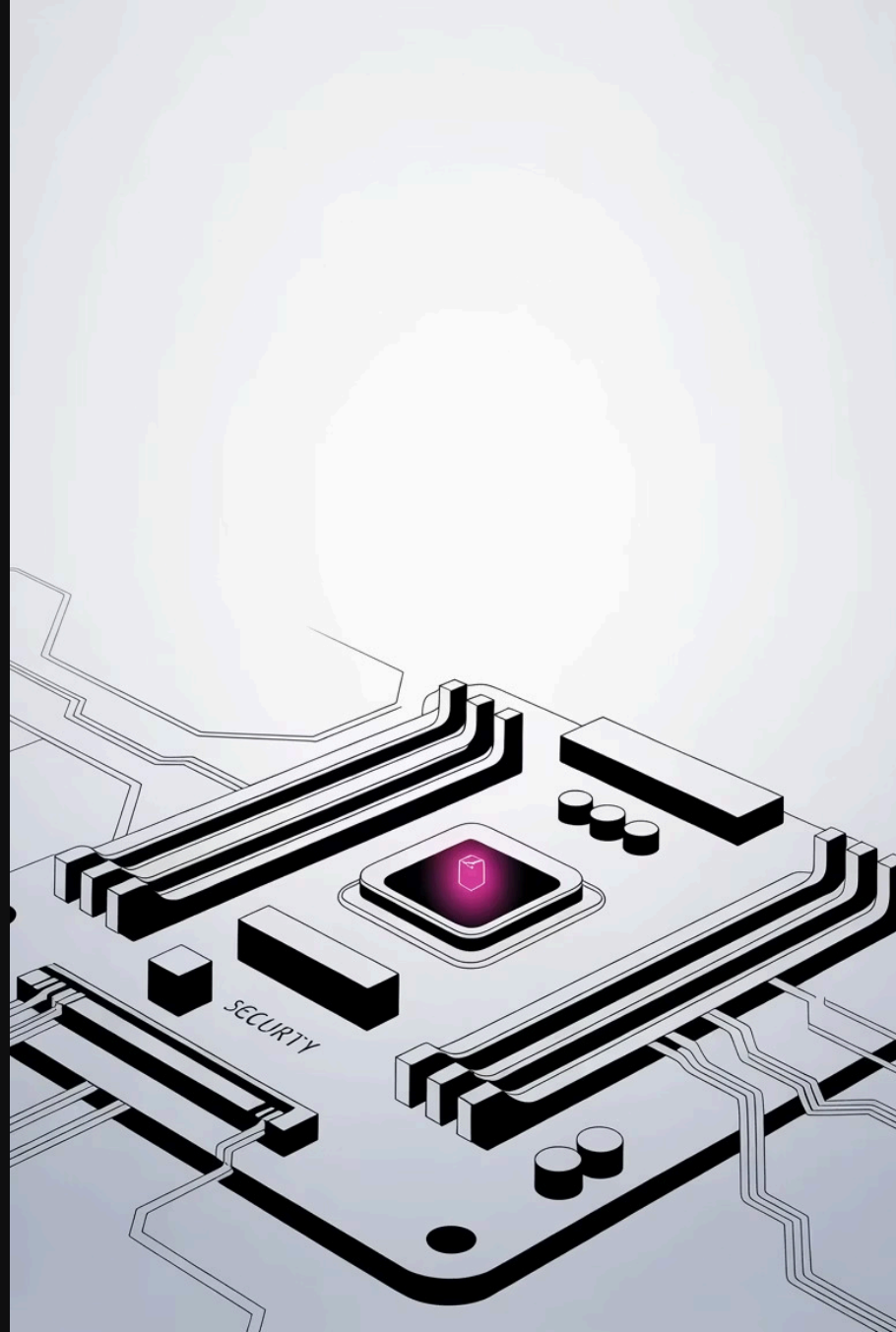
Hardware Especializado de Seguridad

TPM (Trusted Platform Module)

Chip especializado en la placa base diseñado para almacenar de forma segura las claves criptográficas. Garantiza que el sistema operativo y el firmware sean auténticos y no se hayan alterado.

Secure Enclave

Subsistema de seguridad dedicado en los dispositivos Apple. Aislado del procesador principal, genera claves criptográficas únicas para cada dispositivo, imposibles de transferir a otro equipo.



Cifrado AES: El Estándar de Protección

El cifrado AES (Advanced Encryption Standard) es el estándar establecido por el NIST en 2001:

División en bloques

Los datos se dividen en bloques de 128 bits para su procesamiento

Transformaciones

Cada bloque se somete a sustitución de bytes, permutación de filas, mezcla de columnas y adición de clave

Múltiples rondas

10 rondas (clave 128 bits), 12 rondas (192 bits) o 14 rondas (256 bits)

El modo XTS utiliza dos claves independientes y un "tweak" derivado de la posición de cada bloque, eliminando patrones repetitivos.

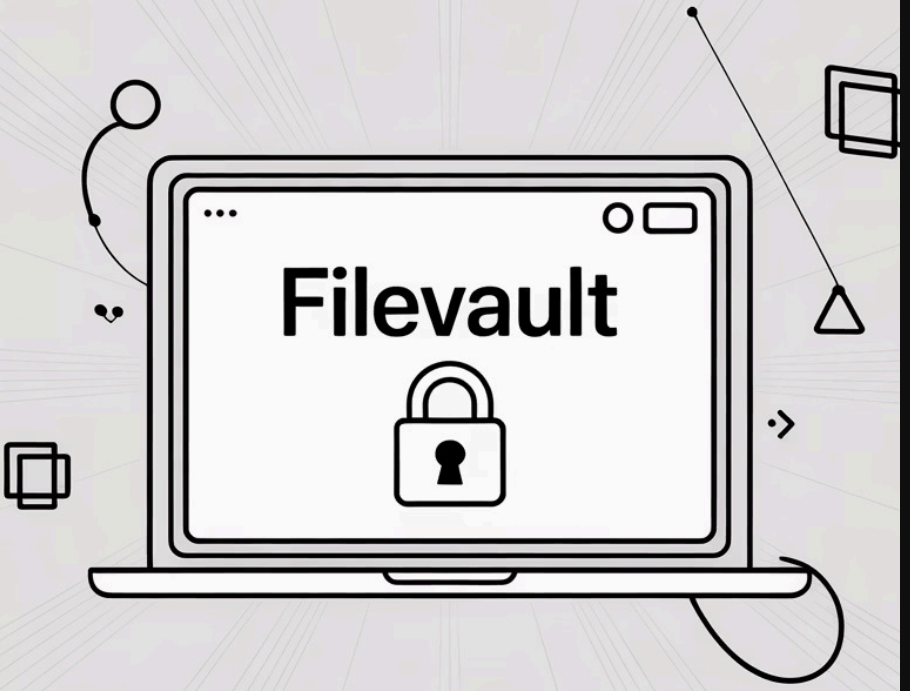
BitLocker (Windows)

Características

- Disponible en ediciones Pro, Enterprise y Education
- Utiliza AES con claves de 128 o 256 bits en modo XTS
- Verificación de integridad durante el arranque mediante TPM

Funcionamiento

El TPM valida la integridad del sistema y libera la clave automáticamente si todo es correcto, garantizando que los datos permanezcan seguros incluso si el dispositivo se pierde o se roba.



FileVault (macOS)

Características principales

- Cifra todo el contenido del disco de arranque
- En Mac con Apple T2 o Apple Silicon, el almacenamiento interno está siempre cifrado a nivel de hardware
- Utiliza "cifrado AES de 256 bits en modo XTS (AES-XTS)"

Gestión de seguridad

La gestión de claves se realiza dentro del Secure Enclave: "ni siquiera la CPU principal ve las claves sin cifrar"

FileVault opera "silenciosamente en segundo plano" – el usuario apenas nota su presencia durante el uso diario

LUKS (Linux)

LUKS (Linux Unified Key Setup) es el estándar para cifrado de disco en Linux, combinado con dm-crypt.

Múltiples contraseñas

"Mantiene varios slots o espacios en el encabezado donde puede guardar la clave maestra cifrada con distintas contraseñas (hasta 8 en LUKS1, y hasta 32 en LUKS2)"

Protección robusta

"Aplica key stretching (derivación intensiva, usando PBKDF2) de modo que probar sistemáticamente contraseñas sea muy lento para un atacante"

Algoritmo estándar

El valor predeterminado es "AES en modo XTS 512-bit (esencialmente AES-256)"

Comparativa de Implementaciones

Característica	BitLocker (Windows)	FileVault (macOS)	LUKS (Linux)
Algoritmo	AES-XTS 128/256 bits	AES-XTS 256 bits	AES-XTS 256 bits
Gestión de claves	TPM	Secure Enclave	Encabezado LUKS
Autenticación durante el arranque	Automática con TPM	Pantalla de inicio de sesión	Contraseña en arranque
Flexibilidad	Limitada	Limitada	Alta (múltiples slots)

Todos protegen los datos "en reposo", garantizando que, en caso de robo o pérdida del dispositivo, los datos permanecen inaccesibles sin las credenciales adecuadas.

Impacto en el Rendimiento del Cifrado

Rendimiento Optimizado

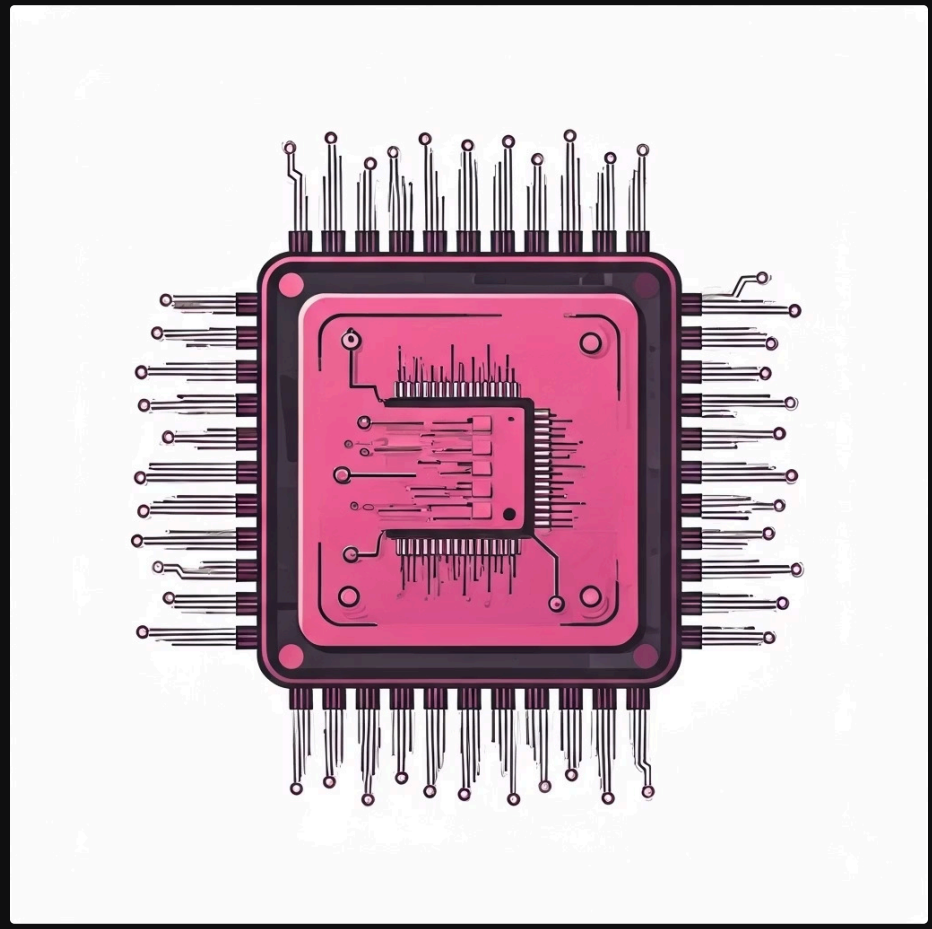
El cifrado moderno introduce una **sobrecarga mínima**, a menudo en porcentajes de un solo dígito.

Aceleración por Hardware

La eficiencia se logra por **instrucciones AES-NI** integradas en los procesadores, acelerando operaciones criptográficas.

Impacto Negligible

La ligera penalización del cifrado con aceleración por hardware resulta **imperceptible** en el rendimiento general del sistema.



Conclusiones

Protección estándar

Los sistemas operativos modernos incorporan cifrado integrado que protege la información mediante algoritmos fuertes como AES-256

Mínimo impacto

El cifrado de disco completo tiene mínimo impacto en rendimiento gracias a optimizaciones de hardware y software

Seguridad transparente

"El usuario trabaja normalmente y el sistema se encarga de cifrar los datos automáticamente cada vez que guarda un archivo"

Esta integración nativa refuerza significativamente la seguridad, protegiendo información sensible en un mundo donde la privacidad y protección de datos son más importantes que nunca.

Referencias

1. Apple. (2023). **Encriptación del volumen con FileVault en macOS** (Guía de Seguridad de la Plataforma Apple).
2. Apple. (2024). **Secure Enclave**. Apple Support.
3. Apple Inc. (2025). **Intro to FileVault**. En Mac deployment documentation.
4. AxCrypt. (2021, 20 de septiembre). **Cifrado de disco vs cifrado de archivos** [Entrada de blog]. Recuperado de AxCrypt Blog.
5. Ciberseguridad.com. (s. f.). **Cifrado AES (Estándar de cifrado avanzado)**.
6. De los Llanos Dueñas, A. (2024, marzo). **Cifrado cuántico: El futuro de la seguridad digital**. Minery Report.
7. Escudo Digital. (2024, 10 de agosto). **¿Qué es la criptografía cuántica o cifrado cuántico?** Escudo Digital.
8. Fortinet. (s. f.). **CIA Triad**.
9. Kingston. (2023, 17 de enero). **¿Qué es el cifrado XTS?** Kingston Technology.
10. Microsoft. (2023). **BitLocker y Administrador de claves distribuidas (DKM) para el cifrado**.
11. Microsoft. (2025). **Preguntas más frecuentes sobre BitLocker**.
12. Microsoft. (s. f.). **¿Qué es un módulo de plataforma segura (TPM)?** Microsoft Support.
13. Red Hat. (2025). **Capítulo 8. Cifrado de dispositivos de bloque mediante LUKS** (Documentación de RHEL 8: Endurecimiento de la seguridad).
14. Schneider, J., & Smalley, I. (2023, 1 de diciembre). **¿Qué es la criptografía cuántica?** IBM.
15. Stack Overflow. (2009). **How much faster is the memory usually than the disk?** Stack Overflow.
16. Whitestack. (s. f.). **Cifrado AES**. Whitestack.