Universidad Nacional Autónoma de México

“Por mi raza hablará el espíritu”

Facultad de Ingeniería

Materia: Sistemas operativos.

Profesor: Gunnar Wolf.

Integrantes del equipo:

- González Martínez Michelle Paola.
- Maya Torres Bruno.

Fecha de entrega: 5 de septiembre de 2025.

Cifrado de datos en los sistemas operativos

El cifrado de datos en sistemas operativos es una técnica de seguridad que transforma la información almacenada para que no pueda leerse sin la clave adecuada. Este cifrado integrado garantiza que, ante el robo o pérdida del dispositivo, los datos permanezcan protegidos del acceso no autorizado. Los sistemas operativos modernos implementan el cifrado de forma transparente para el usuario, cifrando y descifrando automáticamente los datos "detrás de escena" mientras se usa el sistema.

Cuando hablamos de seguridad informática es importante mencionar a la "Tríada CIA". CIA (en sus siglas en inglés) significa confidencialidad, integridad y disponibilidad. La tríada de la CIA es un modelo común que constituye la base para el desarrollo de sistemas de seguridad. Se utilizan para encontrar vulnerabilidades y métodos para crear soluciones. La tríada CIA es esencial para la seguridad de la información, ya que orienta a los equipos en cómo abordar cada aspecto. Cumplir con estos tres principios fortalece el perfil de seguridad de la organización y mejora su capacidad de respuesta ante amenazas. En el caso del cifrado de datos se cubre principalmente la confidencialidad, pero también aporta integridad, ya que evita modificaciones no autorizadas en los datos.

Implementación del cifrado en sistemas operativos

Para lograr cifrado transparente, intervienen varios componentes técnicos:

- **Sistema de archivos cifrado:** Algunos sistemas integran el cifrado directamente en el sistema de archivos (como APFS en macOS o EFS en Windows NTFS). Alternativamente, se implementa mediante una capa debajo del sistema de archivos usando drivers especiales que cifran/descifran bloques sobre la marcha.
- **Gestión de claves:** El sistema genera una clave maestra aleatoria para cifrar el volumen, protegida a su vez por la contraseña del usuario. Los sistemas aprovechan hardware dedicado: Windows usa TPM (Trusted Platform Module), mientras que Mac usa Secure Enclave para proteger las claves de forma segura.

  Un módulo de plataforma segura (TPM) es un chip especializado de la placa base del equipo diseñado para mejorar la seguridad al almacenar de forma segura las claves criptográficas usadas para cifrado y descifrado. Garantiza que el sistema operativo y el firmware sean auténticos y no se hayan alterado. Los TPM se pueden implementar como chips discretos, que son componentes independientes en la placa base, o como soluciones integradas dentro del procesador principal.

- **Proceso de E/S cifrada:** Cuando se escriben datos, el sistema aplica algoritmos como AES antes de guardarlos en disco. Al leer, los descifra antes de entregarlos a las aplicaciones. Según Microsoft (s.f.), "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. El FDE es según AxCrypt

(s.f.), "como cerrar las puertas exteriores de una casa, aunque no cierre cada habitación interna".

Implementaciones específicas

1. **Windows – BitLocker**

BitLocker es la solución de cifrado integrada en Windows (ediciones Pro, Enterprise y Education). Según Microsoft (s.f.), "El cifrado de unidad BitLocker es una característica de protección de datos que se integra con el sistema operativo Windows". Utiliza AES con claves de 128 o 256 bits en modo XTS.

El cifrado AES (Advanced Encryption Standard) se refiere al estándar de cifrado avanzado establecido por el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos en 2001. AES utiliza bloques de 128 bits y permite el uso de claves de 128, 192 y 256 bits, lo que ofrece una alta flexibilidad y niveles variados de seguridad.

El cifrado AES transforma datos legibles en un formato codificado que solo puede ser revertido a su forma original mediante una clave específica. El proceso comienza con la división de los datos en bloques de 128 bits. Cada bloque se somete a una serie de transformaciones que incluyen sustitución de bytes, permutación de filas, mezcla de columnas y la adición de una clave de ronda. Estos pasos se repiten en múltiples rondas, cuyo número depende del tamaño de la clave utilizada: 10 rondas para una clave de 128 bits, 12 rondas para una clave de 192 bits y 14 rondas para una clave de 256 bits. Cada ronda introduce complejidad adicional, incrementando la seguridad del cifrado.

El modo XTS es un modo de operación de AES diseñado para el cifrado de discos. Utiliza dos claves independientes y un "tweak" (valor de retoque) derivado de la posición de cada bloque en el disco, de manera que incluso si dos bloques contienen la misma información, el resultado cifrado será diferente. Esto elimina patrones repetitivos, permite el acceso aleatorio eficiente a sectores individuales. El texto es casi (pero no del todo) doblemente encriptado usando dos claves independientes. El descifrado de los datos se lleva a cabo mediante la inversión de este proceso.

Durante el arranque, BitLocker verifica a través del TPM que no se hayan alterado componentes críticos. Si todo es correcto, el TPM libera la clave y el volumen se descifra automáticamente. Lo que garantiza que los datos permanezcan seguros incluso si el dispositivo se pierde o se roba. El TPM almacena las claves de cifrado, lo que dificulta a los usuarios no autorizados acceder a tus datos. La clave de recuperación es un identificador de 48 dígitos que debe guardarse en lugar seguro para emergencias.

2. **macOS – FileVault**

FileVault cifra todo el contenido del disco de arranque de la Mac. En Mac modernos con Apple T2 o Apple Silicon, según Apple (s.f.), "el almacenamiento interno está siempre cifrado a nivel de hardware, y activar FileVault simplemente añade una capa adicional: vincula el cifrado a la contraseña del usuario". Apple (s.f.) también indica que utiliza "cifrado AES de 256 bits en modo XTS (AES-XTS)".

La gestión de claves se realiza dentro del Secure Enclave: según Apple (s.f.), "ni siquiera la CPU principal ve las claves sin cifrar". Según AxCrypt (s.f.), FileVault opera "silenciosamente en segundo plano" – el usuario apenas nota su presencia durante el uso diario.

Secure Enclave es un subsistema de seguridad dedicado que se integra en el sistema en un chip (SoC) de Apple. Secure Enclave está aislado del procesador principal para ofrecer una capa adicional de seguridad y está diseñado para mantener la seguridad de los datos sensibles del usuario. Genera claves criptográficas únicas para cada dispositivo, imposibles de transferir a otro equipo.

Cuando una app o el sistema necesita validar datos sensibles (como una huella, Face ID o una contraseña), el procesador principal envía la solicitud al Secure Enclave, este la procesa de forma segura y solo devuelve el resultado, sin exponer nunca la información original.

FileVault cifra el volumen entero con AES-XTS. Este algoritmo está diseñado para trabajar sobre bloques de datos (típicamente de 512 bytes o 4096 bytes, según el sistema de archivos) y no sobre todo el disco de una sola vez. Es importante aclarar que el firmware no descifra el disco de manera inmediata; su función se limita a mostrar la interfaz de autenticación en la etapa de arranque. Solo después de que el usuario introduce la clave de acceso se inicia el proceso de desbloqueo, lo que permite acceder a los bloques del volumen de forma progresiva, en lugar de liberar todo el contenido del medio de almacenamiento desde el inicio. FileVault 2 como otros sistemas equivalentes (BitLocker en Windows, LUKS en Linux) implementa el descifrado on-the-fly: cada bloque se descifra en el momento en que el sistema operativo lo solicita, en memoria, y no se guarda en disco descifrado.

3. **Linux – LUKS**

LUKS (Linux Unified Key Setup) es el estándar para cifrado de disco en Linux, combinado con dm-crypt. Según Red Hat (s.f.), "LUKS es la opción predeterminada para cifrar volúmenes en Red Hat Enterprise Linux". Permite múltiples contraseñas para desbloquear la misma clave maestra: según Red Hat (s.f.), "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)".

LUKS emplea técnicas para robustecer las contraseñas contra ataques: según Red Hat (s.f.), "aplica key stretching (derivación intensiva, usando PBKDF2) de modo que probar sistemáticamente contraseñas sea muy lento para un atacante". El valor predeterminado es según Red Hat (s.f.), "AES en modo XTS 512-bit (esencialmente AES-256)".

Diferencias entre las distintas implementaciones:

En resumen, BitLocker, FileVault y LUKS utilizan el estándar AES, pero con diferencias importantes en su implementación. BitLocker (Windows) emplea AES en modo XTS con claves de 128 o 256 bits, gestionadas y liberadas de forma segura a través del chip TPM, lo que garantiza integridad en el arranque. FileVault (macOS) también utiliza AES-XTS, pero exclusivamente con claves de 256 bits, y su administración de llaves se realiza dentro del

Secure Enclave, de modo que ni siquiera la CPU principal accede a ellas en texto claro. En Linux, LUKS combina AES-XTS con el subsistema dm-crypt y permite configuraciones flexibles de tamaño de clave (comúnmente 256 bits), reforzadas mediante funciones de derivación como PBKDF2 o Argon2; además, la clave maestra nunca se guarda en disco en texto claro, sino en un encabezado que contiene varias copias cifradas desbloqueables con diferentes contraseñas.

Aspectos técnicos clave

Algoritmos de cifrado: La mayoría de sistemas emplean AES (Advanced Encryption Standard) en variantes de 128 y 256 bits. Según Microsoft (s.f.), "Las implementaciones de cifrado de los SO modernos se basan en algoritmos de grado militar como AES-256, lo que asegura un nivel de protección muy alto".

Impacto en el rendimiento: El impacto es mínimo en escenarios actuales. Según Microsoft (s.f.), "BitLocker típicamente introduce solo una pequeña sobrecarga, a menudo de porcentajes de un solo dígito en las operaciones de almacenamiento". Esto se debe a optimizaciones de hardware y software, especialmente las instrucciones AES-NI en procesadores modernos.

Una operación de lectura/escritura en almacenamiento persistente (como disco duro o SSD) es varios órdenes de magnitud más lenta que el acceso a memoria. Por ello, añadir la ligera penalización del cifrado con aceleración por hardware (AES-NI) no representa un impacto perceptible en el rendimiento real del sistema.

Proceso de autenticación durante el arranque: Cada plataforma maneja el desbloqueo de forma distinta:

- Windows: El TPM valida la integridad del sistema y libera la clave automáticamente si todo es correcto
- macOS: El firmware muestra la pantalla de inicio de sesión antes de desbloquear el volumen
- Linux: El initramfs solicita la contraseña durante el arranque temprano

Almacenamiento seguro de claves: Nunca existe una copia de la clave maestra en texto claro permanentemente:

- Windows usa el TPM para proteger las claves con hardware
- macOS las almacena en el Secure Enclave
- Linux almacena la clave maestra cifrada en el encabezado LUKS mediante funciones de derivación (PBKDF2 en LUKS1, Argon2 en LUKS2), haciéndola computacionalmente imposible de recuperar sin la contraseña correcta

Es importante destacar que BitLocker, FileVault y LUKS comparten una característica fundamental: los tres protegen los datos "en reposo", es decir, cuando la máquina está apagada o la unidad no está montada. Una vez que el sistema está desbloqueado y en funcionamiento, las aplicaciones autorizadas pueden acceder a los datos normalmente. Esta protección en reposo es crucial porque garantiza que, en caso de robo o pérdida del

dispositivo, los datos permanecen inaccesibles sin las credenciales adecuadas, independientemente del sistema operativo utilizado.

Conclusión

Los sistemas operativos modernos incorporan cifrado integrado que protege la información mediante algoritmos fuertes como AES-256, gestionando las claves de forma segura con apoyo de hardware especializado. El cifrado de disco completo se ha convertido en una práctica estándar debido al mínimo impacto en rendimiento y la enorme mejora en protección de datos. Una vez activado, según Microsoft (s.f.), "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). Recuperado de Soporte de Apple: https://support.apple.com/es-es/guide/security/sec4c6dc1b6e/web
2. Apple. (2024). Secure Enclave. Apple Support. Recuperado de https://support.apple.com/es-es/guide/security/sec59b0b31ff/web
3. Apple Inc. (2025). Intro to FileVault. En Mac deployment documentation. Recuperado el 6 de septiembre de 2025 de https://support.apple.com/es-mx/guide/deployment/dep82064ec40/web
4. AxCrypt. (2021, 20 de septiembre). Cifrado de disco vs cifrado de archivos [Entrada de blog]. Recuperado de AxCrypt Blog: https://axcrypt.net/es/blog/disk-encryption-vs-file-encryption/
5. Ciberseguridad.com. (s. f.). Cifrado AES (Estándar de cifrado avanzado). Recuperado el 6 de septiembre de 2025, de https://ciberseguridad.com/guias/prevencion-proteccion/criptografia/cifrado-aes/#%C2%BFQue_es_el_cifrado_AES_Estandar_de_cifrado_avanzado
6. De los Llanos Dueñas, A. (2024, marzo). Cifrado cuántico: El futuro de la seguridad digital. Minery Report. Recuperado de https://mineryreport.com/blog/cifrado-cuantico-futuro-seguridad-digital/
7. Escudo Digital. (2024, 10 de agosto). ¿Qué es la criptografía cuántica o cifrado cuántico? Escudo Digital. Recuperado de https://www.escudodigital.com/ciberseguridad/que-es-criptografia-cuantica-cifrado-cuantico.html
8. Fortinet. (s. f.). CIA Triad. Fortinet. Recuperado de https://www.fortinet.com/lat/resources/cyberglossary/cia-triad
9. Kingston. (2023, 17 de enero). ¿Qué es el cifrado XTS? Kingston Technology. Recuperado de https://www.kingston.com/latam/blog/data-security/xts-encryption
10. Microsoft. (2023). BitLocker y Administrador de claves distribuidas (DKM) para el cifrado. Recuperado de Microsoft Learn: https://learn.microsoft.com/es-es/purview/office-365-bitlocker-and-distributed-key-manager-for-encryption

11. Microsoft. (2025). Preguntas más frecuentes sobre BitLocker. Recuperado de Microsoft Learn: https://learn.microsoft.com/es-es/windows/security/operating-system-security/data-protection/bitlocker/faq
12. Microsoft. (s. f.). ¿Qué es un módulo de plataforma segura (TPM)? Microsoft Support. Recuperado el 6 de septiembre de 2025, de https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-un-m%C3%B3dulo-de-plataforma-segura-tpm-705f241d-025d-4470-80c5-4feeb24fa1ee
13. Red Hat. (2025). Capítulo 8. Cifrado de dispositivos de bloque mediante LUKS (Documentación de RHEL 8: Endurecimiento de la seguridad). Recuperado de docs.redhat.com: https://docs.redhat.com/es/documentation/red_hat_enterprise_linux/8/html/security_hardening/encrypting-block-devices-using-luks_security-hardening
14. Schneider, J., & Smalley, I. (2023, 1 de diciembre). ¿Qué es la criptografía cuántica? IBM. Recuperado de https://www.ibm.com/es-es/topics/quantum-cryptography
15. Stack Overflow. (2009). How much faster is the memory usually than the disk? Stack Overflow. https://stackoverflow.com/questions/1371400/how-much-faster-is-the-memory-usually-than-the-disk
16. Whitestack. (s. f.). Cifrado AES. Whitestack. Recuperado el 6 de septiembre de 2025, de https://whitestack.com/es/blog/cifrado-aes/#elementor-toc__heading-anchor-0