CNSD

Centro Nacional de Seguridad Digital

Guía para comprobar que tus dispositivos están cifrados (Windows, Android, MacOS, iOS)

PERÚ | Presidencia del Consejo de Ministros

Ponle PUNCHE y ganamos todos PERÚ

INDICE:

1.- INTRODUCCIÓN

En la actualidad, vivimos una transformación digital que ha llevado a las organizaciones y a los ciudadanos a depender en gran medida de dispositivos móviles, computadoras portátiles y servicios en la nube para realizar actividades cotidianas y laborales. Esta creciente digitalización ha traído consigo una alarmante exposición de datos, donde la pérdida, robo o acceso indebido a la información puede generar consecuencias irreversibles.

El robo de identidad, el secuestro de información mediante ransomware, la filtración de documentos confidenciales o la manipulación de información crítica no son riesgos hipotéticos: son amenazas reales que enfrentan instituciones públicas, privadas y personas a diario. En este contexto, el cifrado de dispositivos ya no es una opción técnica avanzada; es una necesidad urgente, básica y transversal a cualquier estrategia de seguridad.

El cifrado convierte los datos legibles en datos codificados que sólo pueden ser interpretados por quien posee la clave adecuada. Este mecanismo actúa como una bóveda digital que protege la confidencialidad, aun cuando el dispositivo sea sustraído o comprometido. Para los profesionales en Tecnologías de la Información (TI), el cifrado debe ser una política obligatoria desde el inicio del ciclo de vida de cualquier equipo. Concientizar sobre su uso no solo implica conocimiento técnico, sino también responsabilidad institucional y social. La seguridad de los datos que manejamos hoy define la confianza que las personas, ciudadanos y usuarios depositan en nuestras entidades mañana.

2.- .¿Qué estamos protegiendo?

Cada dispositivo digital que utilizamos es una extensión de nuestra identidad, nuestras responsabilidades laborales y nuestra información más sensible. Desde correos electrónicos corporativos hasta datos personales, desde contratos hasta fotografías familiares, toda esta información convive diariamente en computadoras, teléfonos y tablets.

Pensar que "mi información no es valiosa" es un error común que los atacantes aprovechan. El verdadero valor de los datos se revela cuando son utilizados sin consentimiento: para suplantación de identidad, fraude, espionaje empresarial o chantaje digital.

Por ello, es fundamental que los profesionales de TI y los responsables de seguridad entiendan que no se trata solo de proteger información confidencial, sino de salvaguardar la integridad institucional, la confianza del ciudadano o cliente, y la reputación digital.

Para reflexionar:

- ¿Qué tipo de información se guarda en cada dispositivo ?
- ¿Qué sucede si se pierde el equipo o es robado ?
- ¿Qué implicancias tendría un acceso no autorizado a esta información ?
- ¿Qué tan expuestos están los datos si un dispositivo es infectado por malware ?

Estas preguntas no solo aplican a usuarios finales, sino a los entornos empresariales donde un incidente puede derivar en brechas de seguridad y sanciones regulatorias.

3.Cómo funciona el cifrado

El cifrado es un proceso criptográfico que transforma la información legible (texto plano) en un formato ininteligible (texto cifrado), utilizando algoritmos matemáticos y claves secretas. Solo quien posee la clave correcta puede revertir este proceso y acceder al contenido original.

En entornos modernos, el cifrado se convierte en una barrera efectiva frente a accesos no autorizados, ya sea por pérdida de dispositivos, intrusiones o ataques de malware. El algoritmo AES (Advanced Encryption Standard), en su versión de 256 bits, es hoy uno de los más robustos y confiables utilizados a nivel internacional, adoptado incluso por gobiernos, instituciones financieras y grandes corporaciones.

Para que el cifrado sea realmente efectivo, se deben cumplir tres condiciones clave:

1. Claves seguras y únicas: La fortaleza del cifrado depende directamente de la complejidad de la clave utilizada. Las claves débiles, predecibles o compartidas comprometen toda la protección.
2. Persistencia del cifrado: El cifrado debe mantenerse activo durante todo el ciclo de uso del dispositivo, incluso en estados de suspensión o hibernación
3. Complemento con autenticación fuerte: No basta con cifrar. Se debe re-stringir el acceso mediante mecanismos sólidos como contraseñas complejas, autenticación multifactor o biometría.

En resumen, el cifrado no solo protege la información almacenada; es una declaración activa de defensa digital. Es el equivalente moderno de una caja fuerte inviolable en el mundo físico.

4. Cifrado en Windows 10/11

Importancia:

El sistema operativo Windows es el más extendido en entornos institucionales, y por ello representa una superficie de ataque recurrente. Si un equipo Windows no está cifrado, basta con retirar su disco duro para acceder a toda la información, sin necesidad de contraseñas. BitLocker, herramienta nativa de Microsoft, permite cifrado completo del disco duro, protegiendo la confidencialidad en escenarios de robo, pérdida o intrusión.

Verificación y activación de BitLocker :

1. Accede a: Panel de control > Sistema y seguridad > Cifrado de unidad BitLocker.
2. Verifica si aparece como "Activado" para la unidad del sistema.
3. Si no ves la opción, valida que estés usando Windows 10/11 Pro, Enterprise o Education.

Pasos para activarlo:

Haz clic en "Activar BitLocker".
Selecciona el método de desbloqueo (contraseña, PIN o unidad USB).
Guarda la clave de recuperación en una ubicación segura (no en el mismo equipo).
Inicia el cifrado completo de la unidad. El proceso puede durar varias horas.

Recomendación:

En entornos corporativos, se recomienda administrar BitLocker mediante Directivas de Grupo (GPO) o plataformas de gestión como Microsoft Intune para asegurar cumplimiento estandarizado.

Mas información

5. Cifrado en Android (7.0 o superior)

Importancia:

La flexibilidad de Android lo hace ideal para entornos laborales móviles, pero también lo convierte en un objetivo frecuente de ataques. Si el dispositivo no está cifrado, cualquier acceso físico (como el robo del equipo) puede exponer datos de correos, documentos, credenciales o plataformas de trabajo remoto..

Verificación del cifrado:

1.- Ir a: Ajustes > Seguridad > Cifrado y credenciales.
2.- Confirmar que la opción "Cifrado del dispositivo" aparece como activada.
3.- Establecer un PIN fuerte (si no hay uno, el cifrado puede no estar activo).

Cifrado de tarjeta SD (si aplica):

Ir a Seguridad > Cifrado de tarjeta SD.
Seleccionar qué archivos serán cifrados.
Conectar a una fuente de energía y esperar la finalización del proceso.

Recomendación:

Se recomienda la integración de dispositivos Android en una solución MDM (Mobile Device Management) para forzar el cifrado y políticas de acceso desde consola centralizada.

MAS INFORMACIÓN

6. Cifrado en iOS (iPhone y iPad)

Importancia:

Los dispositivos Apple cifran automáticamente su contenido, pero este cifrado solo es efectivo cuando se ha configurado un código de acceso.
Si no hay código, el cifrado queda inutilizado.
Dado que muchos altos ejecutivos y funcionarios utilizan iOS,
la verificación de esta configuración es crítica..

Pasos para verificar el cifrado:

1.- Ingresar a Ajustes > Face ID o Touch ID y código.
2.- Confirmar que existe un código configurado.
3.- Desplazarse hasta el final para verificar el mensaje: "La protección de datos está habilitada".

Notas técnicas::

iOS utiliza cifrado de hardware (AES-256).
El contenido permanece cifrado mientras el dispositivo está bloqueado.

Recomendación:

Combinar cifrado con políticas de acceso remoto, bloqueo y borrado a través de Apple Business Manager o plataformas MDM.

MAS INFORMACIÓN

7.- Cifrado en macOS

Importancia:

Con la creciente adopción de dispositivos Apple en instituciones, es vital garantizar que las laptops y estaciones de trabajo cuenten con cifrado activo. FileVault 2, integrado en macOS, realiza cifrado completo del disco sin afectar significativamente el rendimiento..

Pasos para verificar el cifrado:

1.- Ir a Preferencias del sistema > Seguridad y privacidad > FileVault.
2.- Si aparece como desactivado, hacer clic en “Activar FileVault”.
3.- Seleccionar dónde guardar la clave de recuperación: iCloud o almacenamiento físico seguro.

Tecnología empleada:

FileVault utiliza cifrado XTS-AES-128 con una clave de 256 bits.

Recomendación:

Para entornos institucionales, se recomienda registrar y gestionar dispositivos Mac a través de soluciones como Jamf, Apple Business Manager o MDM compatibles.

MAS INFORMACIÓN

8. ¿Debo cifrar toda la información?

Sí. Todo dispositivo, ya sea institucional o personal, que acceda, procese o almacene datos sensibles debe estar cifrado de forma obligatoria. Esto incluye equipos de escritorio, portátiles, teléfonos móviles, discos externos y memorias USB. El cifrado debe asumirse como una medida de seguridad base, no como una opción..

No obstante, en escenarios donde existan limitaciones técnicas como equipos antiguos con bajo rendimiento es posible aplicar un cifrado selectivo, siempre que se realice una evaluación de riesgo clara y se prioricen los activos críticos.

"Sin cifrado, cualquier dispositivo extraviado o comprometido representa una brecha de datos inmediata".

Prioridades recomendadas en caso de cifrado selectivo:

- Carpetas que contengan información clasificada, contractual o de ciudadanos.
- Archivos con datos personales, financieros, médicos o estratégicos.
- Bases de datos, planillas o respaldos operativos.
- Dispositivos portátiles o removibles que circulan fuera del entorno institucional.
- Cualquier archivo exportado o compartido fuera de sistemas seguros

Consideración clave:

El hecho de que un dispositivo funcione correctamente no garantiza que esté protegido. La única forma efectiva de mitigar el acceso no autorizado es cifrando la información desde su origen hasta su almacenamiento final.

Conclusión:

Cifrar no es solo proteger un archivo; es blindar la confianza institucional, reducir la exposición legal y fortalecer la continuidad operativa.

9. Recomendaciones técnicas para entornos TI

El cifrado debe ser parte estructural de las políticas de seguridad de la información. Para garantizar una implementación efectiva, homogénea y sostenible en el tiempo, se recomienda adoptar las siguientes acciones desde el área de Tecnologías de la Información:

1. **Establecer el cifrado como estándar institucional:**
   Incluir la activación del cifrado completo de disco como parte del proceso de configuración inicial de cualquier equipo (laptops, smartphones, tablets, USB, etc.), sin excepción.

2. **Reforzar mecanismos de acceso:**
   Exigir el uso de contraseñas robustas o autenticación multifactor para desbloquear dispositivos cifrados. Esto impide que el cifrado sea anulado por contraseñas débiles.

3. **Integrar soluciones MDM (Mobile Device Management):**
   Implementar una plataforma MDM que permita monitorear y aplicar políticas de cifrado en tiempo real, así como detectar y bloquear dispositivos que no cumplan con los estándares.

4. **Gestionar cifrado por grupos y roles:**
   En sistemas Windows, utilizar Directivas de Grupo (GPO) para activar BitLocker automáticamente y definir condiciones de desbloqueo según nivel de riesgo o función del usuario.

5. **Realizar auditorías de cumplimiento:**
   En sistemas Windows, utilizar Directivas de Grupo (GPO) para activar BitLocker automáticamente y definir condiciones de desbloqueo según nivel de riesgo o función del usuario.

6. **Asegurar los respaldos con cifrado:**
   En sistemas Windows, utilizar Directivas de Grupo (GPO) para activar BitLocker automáticamente y definir condiciones de desbloqueo según nivel de riesgo o función del usuario.

7. **Preparar protocolos ante pérdida o robo:**
   Definir procedimientos claros para bloquear, rastrear o eliminar remotamente los datos de dispositivos extraviados. Este plan debe estar aprobado, probado y comunicado al personal..

8 Capacitar y sensibilizar al personal:

No basta con políticas técnicas. Se requiere que los usuarios conozcan su rol en la protección de los datos y comprendan los beneficios y responsabilidades del cifrado.

9 Estandarizar materiales de soporte:

Desarrollar y distribuir guías visuales actualizadas que expliquen cómo verificar y activar el cifrado según el sistema operativo y perfil de riesgo del usuario.

10 Incluir verificación en procesos internos:

Integrar controles periódicos para asegurar que el cifrado esté activo en los dispositivos que manejan información sensible.

El cifrado no es solo una herramienta técnica, es una declaración de que la privacidad importa."

Bruce Schneier, criptógrafo y experto en seguridad informática

10. Consideraciones complementarias para entornos institucionales

10.1 Marco normativo y buenas prácticas

El uso del cifrado como medida de seguridad técnica se encuentra alineado con diversas normativas de protección de datos a nivel nacional e internacional.

En el caso peruano, la Ley N.º 29733 – Ley de Protección de Datos Personales, y su Reglamento aprobado por D.S. N.º 003-2013-JUS, establecen la obligación de implementar medidas técnicas y organizativas apropiadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales..

A nivel internacional, el uso de cifrado está contemplado como una medida clave dentro de las normas:

- ☑ ISO/IEC 27001 y 27002, sobre gestión de la seguridad de la información.
- ☑ NIST SP 800-111, que recomienda el cifrado de dispositivos portátiles y almacenamiento externo como una medida esencial.

10.2 Errores comunes que comprometen la seguridad del cifrado

A pesar de aplicar cifrado, es común encontrar fallas operativas que anulan su efectividad. Algunas de las más frecuentes son:

- ☑ Usar contraseñas débiles o repetidas como método de desbloqueo.
- ☑ Guardar la clave de recuperación en el mismo dispositivo cifrado.
- ☑ No verificar que el cifrado esté activo después de una reinstalación del sistema.
- ☑ Confiar exclusivamente en el bloqueo de pantalla sin cifrado real del disco.
- ☑ No realizar auditorías periódicas de cumplimiento y verificación.

10.3 Escenario ilustrativo: sin cifrado vs. con cifrado

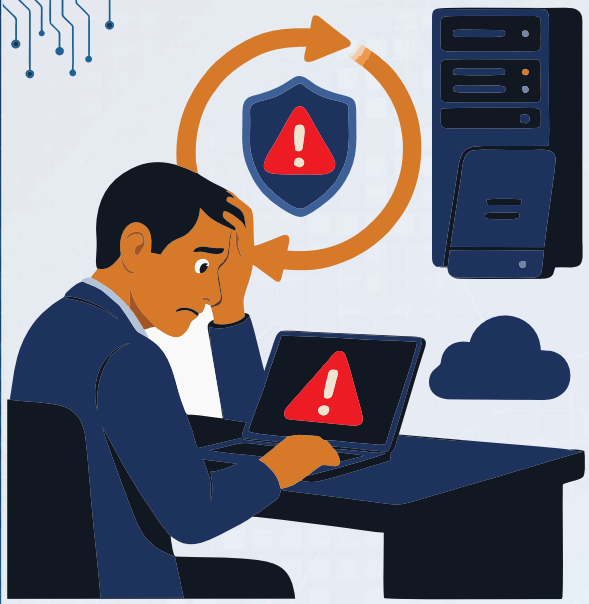
CASO 1 : Laptop extraviada sin cifrado – Gerencia Regional (Escenario de riesgo)

En julio de 2023, un especialista técnico de la Gerencia Regional de Infraestructura del Gobierno Regional de Junín perdió su laptop institucional durante un desplazamiento en transporte interprovincial. El equipo contenía información sensible relacionada con la planificación de obras públicas, contratos por adjudicar, presupuestos y reportes financieros, además de accesos guardados a sistemas internos.

Aunque la laptop contaba con una contraseña de inicio de sesión, no tenía cifrado de disco activo. El disco fue retirado y clonado por terceros, accediendo a la totalidad de los documentos, contraseñas almacenadas y correos electrónicos. No existía respaldo cifrado ni una solución MDM que permitiera rastrear o bloquear el equipo de forma remota.

Consecuencias:

- Fuga de datos institucionales con posibles impactos en contrataciones públicas.
- Investigación interna y observación de la OCI por omitir controles de seguridad digital.
- Pérdida de confianza por parte de proveedores y oficinas de control.



Lección:

Una contraseña de sesión no es suficiente. Sin cifrado, cualquier equipo perdido es una brecha de seguridad total.

Caso 2: Robo de equipo cifrado – Dirección de Salud

En noviembre de 2022, una laptop asignada a una analista de vigilancia epidemiológica de la Dirección Regional de Salud (DIRESA) de La Libertad fue robada durante una jornada de vacunación en una comunidad rural. El equipo contenía información operativa sobre campañas sanitarias, reportes epidemiológicos y bases de datos en análisis.

Sin embargo, el dispositivo contaba con cifrado completo de disco mediante BitLocker, activado desde el área de TI. La autenticación era por PIN fuerte, y la clave de recuperación estaba resguardada en una plataforma segura. El equipo estaba además registrado en una consola MDM institucional.

Al reportarse el robo, el dispositivo fue bloqueado de forma remota y se registró la alerta de pérdida en el sistema. Se ejecutó el protocolo de respuesta y se emitió un informe técnico.

Resultado:

- ☑ No se detectó acceso no autorizado a la información.
- ☑ Se mantuvo la confidencialidad de los datos sanitarios.
- ☑ La entidad reforzó sus controles y recibió reconocimiento interno por la correcta gestión del incidente.

Lección:

Una contraseña de sesión no es suficiente. Sin cifrado, cualquier equipo perdido es una brecha de seguridad total.

Conclusión de los casos

Estos dos escenarios ilustran de manera contundente la diferencia entre una gestión reactiva y una gestión preventiva de la seguridad digital.

En el primer caso, la ausencia de cifrado no solo expuso datos críticos, sino que también evidenció debilidades en los protocolos institucionales y generó consecuencias reputacionales, operativas y administrativas. En contraste, el segundo caso demuestra que un dispositivo adecuadamente cifrado y gestionado permite contener el riesgo, mantener la confidencialidad de la información y garantizar una respuesta técnica oportuna.

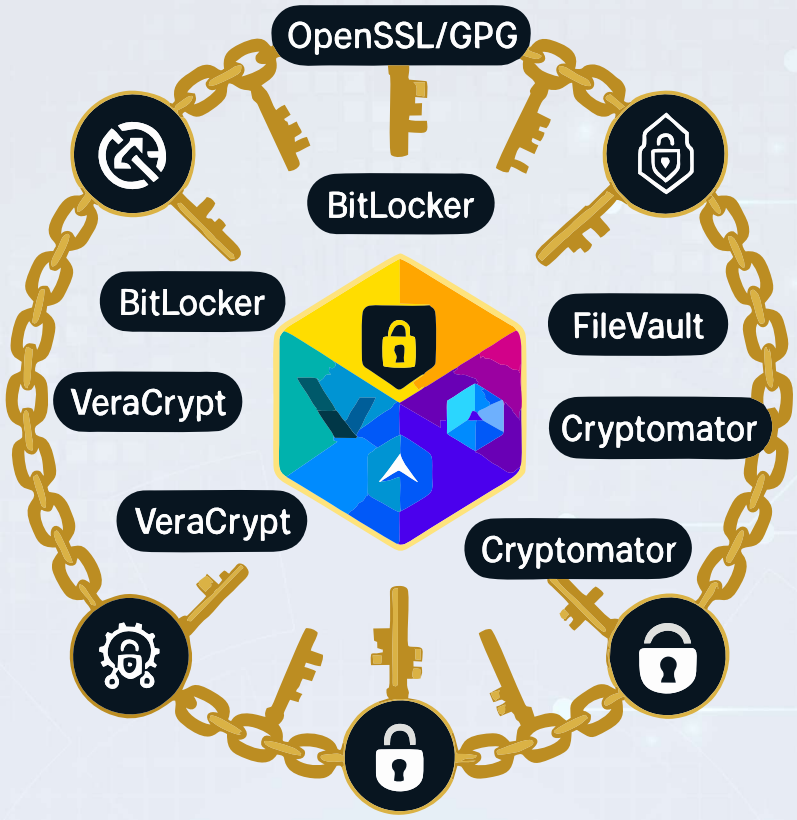
La diferencia no estuvo en el robo, sino en el nivel de preparación.

El cifrado no evita la pérdida física del equipo, pero sí protege lo más valioso: la información. Adoptar medidas proactivas como el cifrado, la gestión remota y los protocolos de respuesta no solo previene incidentes, sino que fortalece la confianza institucional, el cumplimiento normativo y la resiliencia operativa..

10.4 Herramientas recomendadas para cifrado de información

Para fortalecer la implementación del cifrado en diferentes niveles, se recomienda el uso de herramientas confiables, adaptadas al tipo de usuario y dispositivo:.

Herramienta	Plataforma	Uso principal
BitLocker	Windows Pro+	Cifrado completo de disco
FileVault	macOS	Cifrado completo de disco
VeraCrypt	Windows/macOS/Linux	Cifrado de volúmenes o discos portátiles
Cryptomator	Multiplataforma	Cifrado de archivos en la nube (Dropbox, Gdrive)
OpenSSL / GPG	Línea de comandos	Cifrado individual de archivos y correo



11.Conclusión:

El cifrado no debe entenderse como una herramienta opcional ni como un complemento técnico, sino como un pilar fundamental de toda arquitectura de ciberseguridad moderna. En un contexto donde las amenazas son persistentes, sofisticadas y orientadas al robo o manipulación de datos, proteger la información desde su almacenamiento hasta su transporte es una obligación estratégica.

Implementar el cifrado en todos los dispositivos desde equipos de escritorio hasta teléfonos móviles y unidades externas no solo protege la confidencialidad, sino que también respalda la integridad institucional, fortalece la confianza del usuario y garantiza el cumplimiento normativo frente a auditorías y marcos legales de protección de datos..

La gestión del cifrado debe ser proactiva, sistemática y monitoreada. No basta con activarlo debe ser verificado, estandarizado y respaldado por políticas, controles técnicos y formación continua. Las organizaciones que adoptan esta práctica no solo mitigan riesgos, sino que demuestran una cultura de responsabilidad digital y liderazgo en ciberseguridad.

El futuro no espera: los datos son el nuevo activo crítico y quien los protege con disciplina, protege también su reputación, continuidad operativa y legitimidad ante la sociedad.

12. Referencias

- Microsoft BitLocker Documentation: https://learn.microsoft.com /en-us/windows/security/information-protection/bitlocker/bitlocker-overview
- Apple FileVault: https://support.apple.com/en-us/HT204837
- Android Encryption Overview: https://source.android.com/docs/security/features/encryption
- iOS Security Guide: https://support.apple.com/guide/security/overview-of-data-protection-security-secdb0b52c36/web
- Guías de ESET Latinoamérica y LaLibre-net (consultadas como base visual y metodológica)
- support.microsoft.com/es-es/windows/cifrado-de-dispositivo
- source.android.com/docs/security/features/encryption

PERÚ | Presidencia del Consejo de Ministros

Ponle PUNCHE y ganamos todos PERÚ

CNSD | Centro Nacional de Seguridad Digital

- alertas@cnsd.gob.pe
- incidentes@cnsd.gob.pe