

CRYHOD

FOR DISKS AND LAPTOPS

CIFRADO DE ORDENADORES Y DISCOS CONTRA EL ROBO O LA PÉRDIDA

La solución **CRYHOD**, con certificado Full Disk Encryption (FDE), permite cifrar de forma integral dispositivos de almacenamiento físicos y virtuales para proteger la movilidad, el teletrabajo y asegurar el reciclaje.

Riesgos

Para una empresa, la pérdida o el robo de un ordenador va mucho más allá de su valor material. La recuperación y posterior divulgación o utilización de la información del disco del equipo podría implicar una pérdida de reputación, daños industriales y financieros o violaciones normativas (RGPD, difusión limitada).

Para prevenir estos riesgos, que aumentan con el desarrollo del trabajo a distancia, es imprescindible evitar que la seguridad de las estaciones de trabajo se base en el clásico «inicio de sesión», y garantizar que únicamente los usuarios debidamente autenticados y autorizados tengan acceso a su contenido desde el momento en que el equipo se conecta o se pone en marcha.

Eso es lo que proporciona la autenticación pre-boot (PBA) combinada con el Full Disk Encryption (FDE) que ofrece **CRYHOD**, una solución europea certificada para la protección de las estaciones de trabajo, adoptada en todos los grandes ministerios franceses.

Protección del teletrabajo y la movilidad

CRYHOD permite a la empresa proteger los equipos de los empleados que salgan de las instalaciones siguiendo una estrategia global y administrada. Estas herramientas pueden ser un ordenador portátil, dispositivos USB, discos externos, máquinas virtuales locales o en el Cloud.

Protección integral de los terminales y los discos

CRYHOD puede cifrar una o todas las particiones de los ordenadores y dispositivos externos, proporcionando así un cifrado permanente de los datos que protege estos dispositivos contra la pérdida y el robo durante todo su ciclo de vida, incluso después de desecharlos.

Seguridad transparente para el usuario, sin alteraciones

El usuario introduce su clave secreta al arrancar el dispositivo y puede trabajar como de costumbre. La sesión puede abrirse a continuación automáticamente (*Single Sign On*). Los sectores de las particiones se cifran y descifran sobre la marcha, de forma que el usuario no tiene que interactuar con el producto. Cuando cierra o apaga su estación de trabajo, su contenido permanece cifrado y, por tanto, protegido.

Solución «encrypt and forget»

Una vez desplegada, se olvidará de que **CRYHOD** está ahí. Garantiza la política de seguridad de la empresa, se olvidan de ella y todos los materiales quedan protegidos.



CIFRADO

- **Cifrado de particiones** (*sistema y datos*).
- **Cifrado sobre la marcha transparente para los usuarios.**
- **Cifrado inicial en segundo plano; recuperación tras cortes de corriente; modo rápido** (*solo afecta a los sectores utilizados*) o **completo** (*para todos los sectores*).
- **Hibernación segura.**



AUTENTICACIÓN

- **Autenticación pre-boot** (*antes del arranque o al conectar*).
- **Autenticación mediante contraseña, Smart-Card o token.**
- **Apertura de sesión manual o automática** (*Single Sign On*).
- **Estación de trabajo de usuario único o multiacceso** (*estaciones compartidas/autoservicio*).



ADMINISTRACIÓN - TI

- **Despliegue a través de las infraestructuras de TI habituales** (*SCCM, AD, etc.*).
- **Gestión mínima de TI «encrypt and forget».**
- **Todos los tipos de discos y de ordenadores** (*BIOS o UEFI*).



ADMINISTRACIÓN - SEGURIDAD

- **Políticas de seguridad definidas por el responsable de seguridad.**
- **Mecanismo de recuperación de datos configurable.**
- **Rescate usuario** (*pérdida de clave o contraseña*).

CARACTERÍSTICAS TÉCNICAS

- + **Windows 7 a 10+, Ubuntu y CentOS.**
- + **Firmware BIOS o UEFI.**
- + **Cifrado AES 256.**
- + **Acceso mediante certificados/claves RSA** (*hasta 4096 bits*) y/o **contraseña** (*con fuerza configurable*).
- + **Compatible con las principales smart card PKCS#11** (*formato tarjeta o USB*).
- + **Compatible con la mayoría de las PKI del mercado.**

CERTIFICACIONES

