KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Tecnología de cifrado

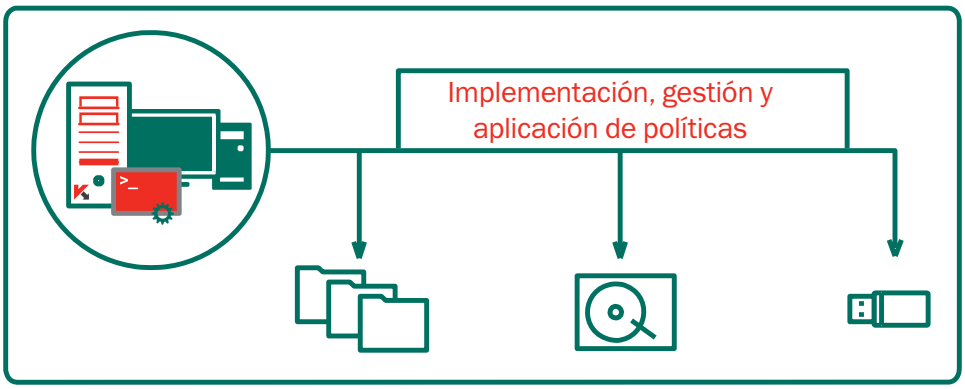
Evite el acceso no autorizado a los datos debido a la pérdida o el robo del dispositivo, o el malware que sustrae datos.

La protección proactiva de datos y el cumplimiento es un imperativo global. La tecnología de cifrado de Kaspersky Lab protege los datos valiosos de la pérdida accidental y el robo del dispositivo, y los ataques de malware dirigidos. Gracias a la combinación de potentes tecnologías de cifrado con las tecnologías de protección de endpoints líderes del sector de Kaspersky Lab, nuestra plataforma integrada protege los datos en reposo y en movimiento.

Como se trata de una solución desarrollada por Kaspersky Lab, es muy fácil de implementar y gestionar desde una consola de gestión centralizada con una única política.

Evite la pérdida de datos y el acceso no autorizado a la información con la tecnología de cifrado de Kaspersky Lab:

- **Cifrado completo de disco (Full Disk Encryption, FDE)**
- **Cifrado de archivos/ carpetas (FLE)**
- **Dispositivos extraíbles e internos**



ADMINISTRADO MEDIANTE UNA ÚNICA CONSOLA DE GESTIÓN

CRIPTOGRAFÍA SEGURA ESTÁNDAR DEL SECTOR

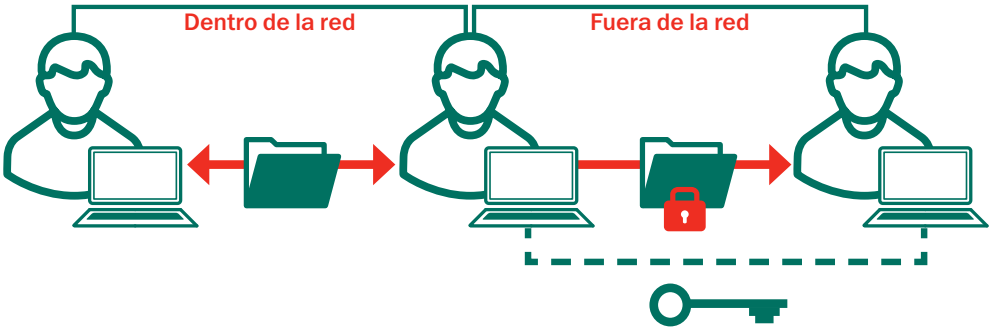
Kaspersky Lab utiliza el estándar de cifrado avanzado (AES, del inglés Advanced Encryption Standard) con una longitud de clave de 256 bits y gestión y custodia simplificadas. Es compatible con la tecnología Intel® AES-NI y las plataformas UEFI y GPT.

FLEXIBILIDAD TOTAL

Kaspersky Lab ofrece cifrado de archivos y carpetas (FLE) y cifrado completo de disco (FDE), abarcando así todos los casos de uso posibles. Los datos se pueden proteger tanto en las unidades de disco duro como en los dispositivos extraíbles. El "modo portátil" permite el uso y la transferencia de datos en los soportes extraíbles cifrados, incluso en equipos donde el software de cifrado no está instalado, facilitando así el intercambio de datos seguro "fuera del perímetro".

INICIO DE SESIÓN ÚNICO, TRANSPARENCIA DEL USUARIO FINAL

Desde la configuración hasta el uso diario, la tecnología de cifrado de Kaspersky Lab funciona de forma transparente en todas las aplicaciones, sin que ello reduzca la productividad del usuario final. El inicio de sesión único garantiza un cifrado perfecto: puede que el usuario final ni siquiera sea consciente de que la tecnología se está ejecutando.



El cifrado de Kaspersky Lab permite una transferencia de archivos perfecta y transparente entre los usuarios de dentro y fuera de la red.

FUNCIONES DE CIFRADO

INTEGRACIÓN PERFECTA CON LAS TECNOLOGÍAS DE SEGURIDAD DE KASPERSKY LAB

Integración completa con las tecnologías antimalware, de herramientas de control de endpoints y de tecnologías de gestión de Kaspersky Lab para una verdadera seguridad a varios niveles construida sobre una base de código común. Por ejemplo, una sola política podría implementar el cifrado en determinados dispositivos extraíbles. Aplique la configuración de cifrado mediante la misma política de antimalware, control de dispositivos y otros elementos de seguridad de endpoints. La compatibilidad con hardware de red se comprueba de forma automática antes de la implementación del cifrado; la compatibilidad con las plataformas UEFI y GPT es estándar. La compatibilidad con hardware de red se comprueba de forma automática antes de la implementación del cifrado; la compatibilidad con las plataformas UEFI y GPT es estándar.

CONTROL DE ACCESO BASADO EN FUNCIONES

En las empresas más grandes, puede delegar la gestión del cifrado mediante características de control de acceso basado en funciones. Esto permite una gestión menos compleja del cifrado.

Cómo comprarlo

La tecnología de cifrado de Kaspersky no se vende por separado. Solo está habilitada en los niveles "Advanced" y "Total" de Kaspersky Endpoint Security for Business como un componente de la plataforma de seguridad global

AUTENTICACIÓN PREVIA AL ARRANQUE (PBA)

Se requiere la introducción de las credenciales de usuario incluso antes de que el sistema operativo arranque, lo que ofrece un nivel adicional de seguridad, con el inicio de sesión único opcional. La tecnología de cifrado PBA de Kaspersky Lab también está disponible para teclados que no sean QWERTY.

AUTENTICACIÓN A TRAVÉS DE TARJETA INTELIGENTE Y TOKEN

Compatible con la autenticación de dos factores mediante marcas populares de tarjetas inteligentes y tokens, eliminando así la necesidad de nombres de usuario y contraseñas adicionales, y mejorando la experiencia del usuario final.

RECUPERACIÓN DE EMERGENCIA

Los administradores pueden descifrar los datos en caso de que se produzca un fallo de hardware o software. La recuperación de contraseñas de usuario para PBA o el acceso a datos cifrados se implementa a través de un sencillo mecanismo de desafío/respuesta.

IMPLEMENTACIÓN OPTIMIZADA, CONFIGURACIÓN PERSONALIZABLE

Para facilitar la implementación, las funciones de cifrado de Kaspersky Lab solo se activan en los niveles "Advanced" y "Total" de Kaspersky Endpoint Security for Business sin necesidad de realizar una instalación por separado. La configuración del cifrado está predefinida, pero se puede personalizar para las carpetas comunes como Mis documentos, el Escritorio, nuevas carpetas, extensiones y grupos de extensiones de archivos (como documentos de Microsoft Office o archivos de mensajes).

Kaspersky Endpoint Security for Business/Cifrado/

KASPERSKY lab