

# ▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS Advanced

Las herramientas de seguridad combinadas con funciones de optimización de TI abundan en esta valiosa gama de soluciones de Kaspersky Lab.

El nivel de protección Advanced de Kaspersky ofrece la solución de protección y gestión que tu organización necesita para aplicar la política de TI, mantener a los usuarios libres de malware, evitar las pérdidas accidentales de datos y, además, mejorar la eficacia en TI.

## Las funciones de protección y gestión que necesitas.

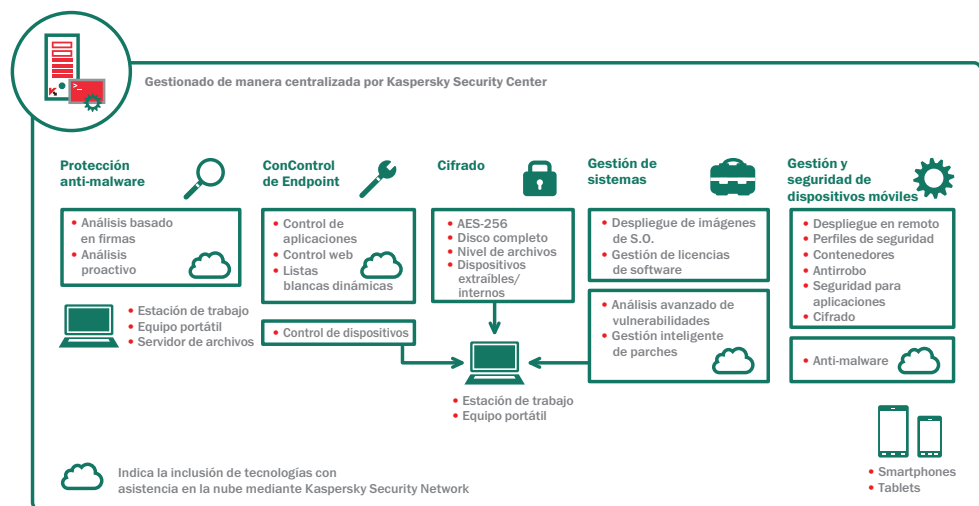
En Kaspersky hemos integrado potentes funciones empresariales en todos los niveles de protección de las soluciones que ofertamos, utilizando siempre una tecnología sencilla e idónea para empresas de cualquier tamaño.

## ¿Qué nivel de protección es el más adecuado para ti?

- CORE
- SELECT
- **ADVANCED**
- TOTAL

### FUNCIONES INCLUIDAS:

- ANTI-MALWARE
- FIREWALL
- PROTECCIÓN CON ASISTENCIA EN LA NUBE MEDIANTE KASPERSKY SECURITY NETWORK
- CONTROL DE APLICACIONES
- MARCADO DE APLICACIONES EN LISTA BLANCA
- CONTROL WEB
- CONTROL DE DISPOSITIVOS
- PROTECCIÓN DE SERVIDORES DE ARCHIVOS
- MOBILE DEVICE MANAGEMENT (MDM)
- SEGURIDAD PARA TERMINALES MÓVILES (PARA TABLETS Y SMARTPHONES)
- CIFRADO
- CONFIGURACIÓN E IMPLEMENTACIÓN DE SISTEMAS
- CONTROL DE ADMISIÓN A LA RED
- ANÁLISIS AVANZADO DE VULNERABILIDADES
- GESTIÓN DE REVISIONES



## ▶ LA ÚNICA PLATAFORMA DE SEGURIDAD DEL SECTOR

### Una única consola de gestión

A través de un único "panel de cristal", el administrador puede ver y gestionar todo el sistema de seguridad: equipos virtuales y dispositivos tanto físicos como móviles.

### Una única plataforma de seguridad

Kaspersky Lab ha desarrollado nuestra consola, módulos de seguridad y herramientas de forma interna en lugar de adquirirlos de otras empresas. Eso significa que los programadores que trabajan en el mismo código base han desarrollado tecnologías que interactúan entre sí y funcionan de forma conjunta. Esto se traduce en estabilidad, políticas integradas, generación de informes útiles y herramientas intuitivas.

### Un único coste

Todas las herramientas provienen de un único proveedor y se proporcionan mediante una única instalación, para que no tengas que pasar por un nuevo proceso de presupuestación y justificación para alinear tus riesgos de seguridad con tus objetivos empresariales.

## CIFRADO Y PROTECCIÓN DE DATOS:

### CIFRADO EXHAUSTIVO

Te permite elegir entre el nivel de disco completo o el de archivo, respaldado por el algoritmo Advanced Encryption Standard (AES), con cifrado de 256 bits, para proteger información empresarial de vital importancia en caso de robo o pérdida de dispositivos.

### COMPATIBILIDAD CON DISPOSITIVOS EXTRAÍBLES

Aumenta tu seguridad mediante políticas que aplican el cifrado de datos en dispositivos extraíbles.

### USO COMPARTIDO DE DATOS SEGURO

Significa que los usuarios pueden crear fácilmente paquetes cifrados y autoextraíbles para garantizar que los datos estén protegidos al compartirlos mediante dispositivos extraíbles, correo electrónico, redes o la web.

### TRANSPARENCIA PARA USUARIOS FINALES

La solución de cifrado de Kaspersky es invisible para los usuarios y no tiene efectos negativos en la productividad. Sin repercusiones en la configuración de las aplicaciones ni en las actualizaciones.

## CONTROL DE ENDPOINT

### CONTROL DE APLICACIONES

Permite a los administradores de TI establecer políticas de autorización, bloqueo o regulación de aplicaciones (o categorías de aplicaciones).

### CONTROL DE DISPOSITIVOS

Permite a los usuarios establecer, programar y aplicar políticas de datos con controles para dispositivos de almacenamiento extraíbles y otros dispositivos periféricos — conectados a un puerto USB o cualquier otro tipo de bus.

### CONTROL WEB

Significa que los controles de navegación basados en terminales hacen un seguimiento del usuario, tanto en la red empresarial como en itinerancia.

### LISTAS BLANCAS DINÁMICAS

El envío de datos de reputación de archivos en tiempo real de Kaspersky Security Network permite garantizar que las aplicaciones aprobadas estén libres de malware, así como maximizar la productividad de los usuarios.

## FUNCIONES DE PROTECCIÓN DE TERMINALES

### ANTI-MALWARE PARA TERMINALES DE CALIDAD SUPERIOR

Métodos tradicionales de eficacia demostrada basados en firmas, proactivos y basados en la nube para la detección de amenazas de malware.

### PROTECCIÓN CON ASISTENCIA EN LA NUBE

Kaspersky Security Network (KSN) ofrece una respuesta inmediata ante sospechas de amenazas, de forma mucho más rápida que los métodos de protección tradicionales. El tiempo de respuesta de KSN a una amenaza de malware puede ser de tan sólo 0,02 segundos.

**NO TODAS LAS FUNCIONES SE ENCUENTRAN DISPONIBLES EN TODAS LAS PLATAFORMAS.** Para obtener más información, consulta [www.kaspersky.com](http://www.kaspersky.com)

## CONFIGURACIÓN DE SISTEMAS Y GESTIÓN DE REVISIONES:

### GESTIÓN DE REVISIONES

Análisis exhaustivo avanzado de vulnerabilidades combinado con distribución automatizada de revisiones.

### DESPLIEGUE EN REMOTO DEL SOFTWARE

Implementación centralizada de software en los equipos cliente, incluso en sucursales.

### NETWORK ADMISSION CONTROL (NAC)

Con control de admisión a la red (NAC), puedes crear una política de red de invitados. Los dispositivos invitados (incluidos los dispositivos móviles) se reconocen automáticamente y se envían a un portal de la empresa donde se habilitan las credenciales correctas para usarlos con los recursos que hayas aprobado.

### DESPLIEGUE DE IMÁGENES DE SISTEMAS OPERATIVOS Y APLICACIONES

Fácil creación, almacenamiento y despliegue de imágenes de sistema desde una ubicación centralizada. Perfecto para migrar a Microsoft® Windows® 8.

### GESTIÓN DE HARDWARE, SOFTWARE Y LICENCIAS

Los informes de inventario de hardware y software contribuyen a mantener el control de las obligaciones de licencia de software. Así podrás ahorrar costes gracias al abastecimiento central de derechos de software.

## FUNCIONES DE SEGURIDAD MÓVIL:

### INNOVADORAS TECNOLOGÍAS ANTI-MALWARE

La combinación de tecnologías de detección basadas en firma, proactivas y con asistencia en la nube proporciona protección en tiempo real. Mayor seguridad gracias a una navegación segura y a tecnologías antisпам.

### IMPLEMENTACIÓN CON ABASTECIMIENTO INALÁMBRICO

Preconfigura e implementa aplicaciones de forma centralizada mediante SMS, correo electrónico y ordenadores.

### HERRAMIENTAS ANTIRROBO REMOTAS

Las herramientas de vigilancia de SIM, bloqueo remoto, borrado y búsqueda evitan el acceso no autorizado a los datos de la empresa en caso de robo o pérdida de un dispositivo móvil.

### CONTROL DE APLICACIONES PARA DISPOSITIVOS MÓVILES

Supervisa las aplicaciones instaladas en un dispositivo móvil, de acuerdo con las políticas de grupo predefinidas. Incluye un grupo de “aplicación obligatoria”.

### COMPATIBILIDAD CON LOS DISPOSITIVOS PERSONALES DE LOS EMPLEADOS

¿Iniciativa BYOD (trae tu propio dispositivo)? Los datos y las aplicaciones de la empresa permanecen aislados en contenedores cifrados de apariencia transparente para los usuarios. Estos datos se pueden borrar por separado.

**KASPERSKY LAB IBERIA**  
C/ VIRGILIO, Nº25, 1º B  
28223 POZUELO DE ALARCÓN  
MADRID  
ESPAÑA  
[canal@kaspersky.es](mailto:canal@kaspersky.es)  
[www.kaspersky.es](http://www.kaspersky.es)