

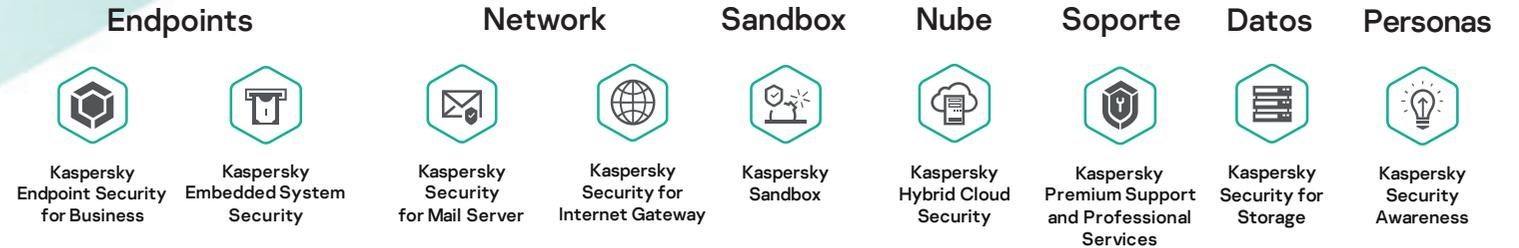
3 niveles de madurez para la ciberseguridad empresarial

1

Un panorama más amplio de las amenazas

Fundamentos de seguridad

Fortalece los sistemas y bloquea automáticamente el número máximo de amenazas posibles.



2

Amenazas avanzadas y ataques dirigidos

Protección Avanzada

Se enfoca en la detección avanzada y en una respuesta rápida ante las amenazas complejas que la protección preventiva no puede detectar.



3

Campañas específicas y ciberarmas

Enfoque integrado de la ciberseguridad

Estará preparado para ataques que se encuentren en un nivel de amenazas persistentes avanzadas (APT). Alto nivel de experiencia, capacidades avanzadas de inteligencia contra amenazas y búsqueda continua de amenazas.



Beneficios empresariales de este enfoque



Constituye la base para el desarrollo de una estrategia de ciberseguridad a largo plazo, la cual toma en cuenta las características específicas de la empresa y las tendencias en el panorama de las amenazas.



Inversión optimizada en tecnología de seguridad y reducción del TCO (Costo total Propiedad).



Reducción de los daños financieros y operativos causados por el cibercrimen.



Mayor retorno de la inversión (ROI) mediante la automatización del flujo de trabajo y la ausencia de interrupciones en los procesos empresariales.

Acercas del portafolio empresarial de Kaspersky

Crear una base de seguridad para su empresa eligiendo el producto o servicio adecuado es el primer paso. Sin embargo, desarrollar una estrategia de ciberseguridad corporativa con visión de futuro es fundamental para el éxito a largo plazo. El Portafolio de negocios de Kaspersky refleja las demandas de seguridad de los negocios de hoy, respondiendo a las necesidades de las organizaciones en diferentes niveles de desarrollo con un enfoque paso a paso. Este enfoque combina diferentes capas de protección contra todo tipo de amenazas cibernéticas para detectar ataques más complejos, responder de manera rápida y adecuada a cualquier incidente y prevenir futuras amenazas.

Para mais informações acesse latam.kaspersky.com

Iniciativa de Transparencia Global



**Proven.
Transparent.
Independent.**

Kaspersky está comprometido con brindar a sus clientes protección contra las ciberamenazas, independientemente de su origen o propósito. La iniciativa de Transparencia Global de la empresa se diseñó para involucrar a la comunidad de seguridad de la información y otras partes interesadas en la validación y verificación de la confiabilidad de los productos, los procesos internos y las operaciones comerciales. También introduce mecanismos de responsabilidad adicionales, mediante los cuales la empresa puede demostrar que aborda cualquier problema de seguridad de manera rápida y exhaustiva. Existen Centros de Transparencia en funcionamiento en varias regiones, y en América Latina, se encuentra en São Paulo - Brasil.

Por qué elegir Kaspersky

Somos una de las compañías privadas de ciberseguridad más grandes del mundo, con más de 22 años de existencia. Nuestra inteligencia de amenazas detallada y nuestra experiencia en seguridad se transforma continuamente en soluciones y servicios de seguridad innovadores para proteger a las empresas, la infraestructura crítica, los gobiernos y los consumidores finales de todo el mundo. Hay más de 400 millones de usuarios y más de 270 mil empresas protegidas. Los productos de Kaspersky son evaluados regularmente por las mejores compañías de investigación del mundo y somos muy reconocidos y premiados.

FORRESTER

"Strong Performer" in the Forrester Wave

Líder en The Forrester Wave™. Endpoint Security Suites, en el tercer trimestre del 2019 y un alto desempeño en The Forrester Wave™. Cloud Workload Security (CWS), en el cuarto trimestre de 2019.*



Best Brand of the year

Kaspersky fue reconocida como una marca del año luego de un proceso único y de votación en el principal evento de premios del World Branding Forum.



Gartner Peer Insights Customer Choice for EndPoint Protection Platform.

Kaspersky es nombrada, una vez más, en el Gartner Peer Insights del 2019 como la elección del cliente para Plataformas de Protección de Endpoint (EPP).