

Ciberseguridad para pequeñas y medianas empresas

¿Qué fortalece a su pequeña pero poderosa empresa?

43%* de los ataques se dirigen a pymes

≈ \$70 000*

1 semana a 6 meses
Posible tiempo de inactividad

El costo promedio de un incidente (pérdida de datos, phishing, ransomware, fraude, daño a la reputación)

¿Qué está sucediendo y por qué es importante para su empresa?

Las plataformas en la nube, el trabajo remoto, los dispositivos móviles, los servicios y herramientas en línea, y la automatización con IA simplifican varios aspectos de las operaciones diarias, pero también aumentan la complejidad y dificultan la protección de los sistemas.



Cada herramienta adicional expande la superficie de ataque: todo nuevo servicio habilita una puerta de entrada para las ciberamenazas.



Tiempo y personal limitados

Los pequeños equipos de TI no pueden supervisar todo a cada momento.



Trabajo fuera del control empresarial

Usar dispositivos y cuentas personales en el trabajo deja los datos sin protección y expone a la empresa a posibles multas.



Más ataques potenciados por IA

La IA permite realizar ataques automatizados de contraseñas y phishing de bajo costo a gran escala.

Todos estos factores amenazan el crecimiento y la continuidad de la empresa, y provocan lo siguiente:

- Pérdidas económicas potenciales
- Filtraciones de datos
- Daño a la reputación

¿Qué pone en riesgo a su empresa por dentro y por fuera?

La mayoría de los ciberincidentes no son dramáticos. Empiezan con situaciones diarias y problemas reales.

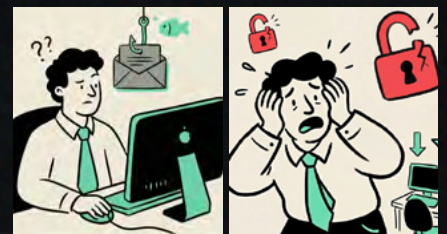
Riesgos internos y externos



Ransomware



Operaciones que se detienen en seco



Ingeniería social



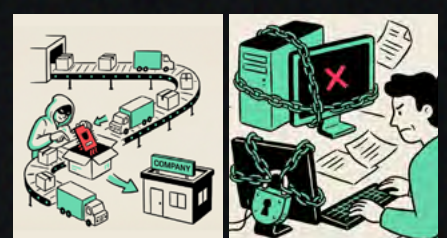
Robo de credenciales, interrupción de actividades comerciales



Ataques sin archivos y malware



Robo de datos, sistemas inestables



Ataques a la cadena de suministro



Interrupciones para los clientes y pérdida de confianza

Desafíos



Rápido crecimiento de TI



Seguridad que no puede seguir el ritmo



Déficit de competencias en la respuesta a incidentes



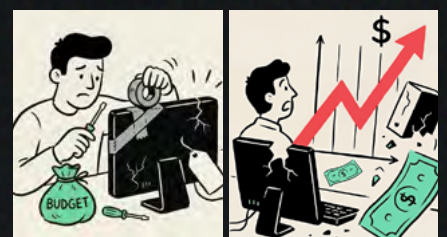
Decisiones incorrectas que empeoran situaciones



Sobrecarga en TI



Amenazas no detectadas y retraso en respuestas



Presupuesto limitado



Costos de recuperación más altos a futuro

¿Cómo abordamos estas amenazas y desafíos en Kaspersky?

	Kaspersky Next EDR Foundations	Kaspersky Next EDR Optimum	Kaspersky Next XDR Optimum	Kaspersky Next MXDR Optimum
Malware + <i>Amenazas comunes</i>	●	●	●	●
Ransomware	●	●	●	●
Ataques fileless (con vectores residentes en memoria solamente)	●	●	●	●
Phishing	●	●	●	●
Malware desconocido <i>Nuevo y selectivo</i>		●	●	●
Error humano		●	●	●
Terceros no controlados		●	●	●
Ingeniería social			●	●
Movimiento lateral			●	●
Falta de recursos				●
Continuidad empresarial				●

Servicio administrado por expertos de Kaspersky

Qué significa para usted una seguridad confiable:

Protección contra amenazas automática

Protección integrada contra amenazas masivas que reduce la necesidad de respuesta manual.

Menos trabajo para el equipo de TI

Menos tareas manuales, menos errores y más tiempo para lo importante, gracias a una implementación optimizada basada en la nube.

Detección de amenazas temprana

Detenga las amenazas evasivas antes de que se conviertan en incidentes.

Mayor facilidad para recuperarse ante un problema

Menos tiempo de inactividad: mayor estabilidad de la empresa y menos pérdida de ingresos.

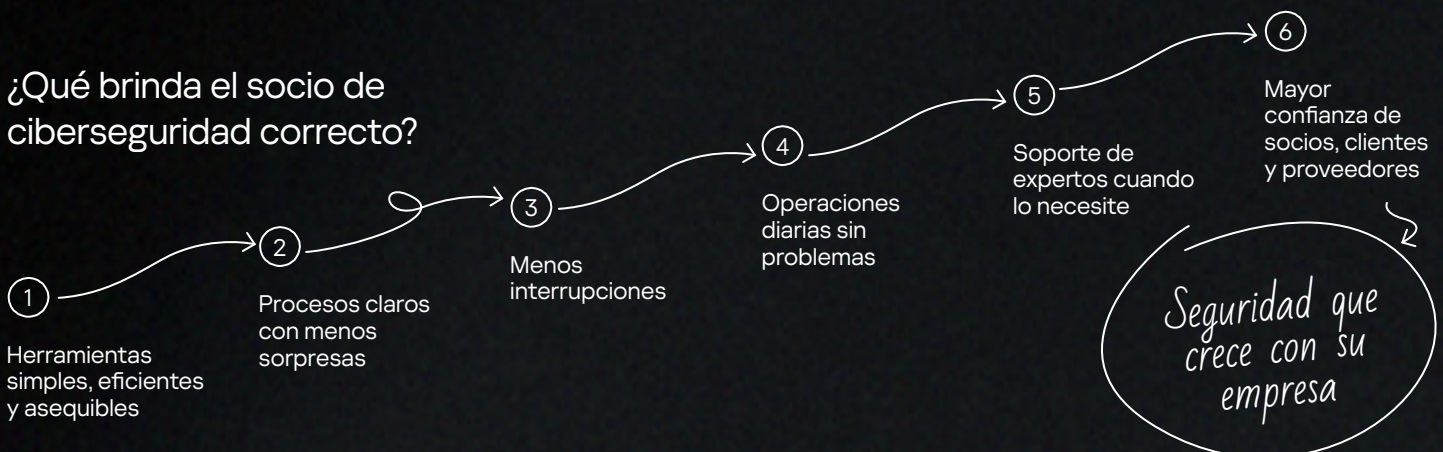
Protección contra ingeniería social

La capacitación en ciberseguridad permite que el personal detecte estafas, phishing y manipulación.

Seguridad experta sin crear un equipo

Obtenga una protección fuerte sin el costo ni las molestias de contratar a especialistas.

¿Qué brinda el socio de ciberseguridad correcto?



¿Desea una seguridad nativa de nube creada para usted?

Obtenga una protección que funcione desde el primer día.

latam.kaspersky.com

Contáctenos

© 2026 AO Kaspersky Lab.
Las marcas comerciales registradas y las marcas de servicio pertenecen a sus respectivos propietarios.