

Ciberseguridad para pequeñas y medianas empresas

¿Qué fortalece a tu pequeña pero poderosa empresa?

43 %* de los ataques se dirigen a pymes

≈ \$70 000*

1 semana a 6 meses

Posible tiempo de inactividad



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

¿Qué está sucediendo y por qué es importante para tu 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 seguridad de los sistemas.



Más herramientas, más puntos de entrada

Cada servicio nuevo agrega una puerta potencial más a tu empresa.



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 coste a gran escala

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

- posibles pérdidas económicas,
- robos de datos
- y daños a tu reputación.

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

La mayoría de los ciberincidentes no empiezan con algo dramático. Empiezan con situaciones diarias y desafíos actuales.

Riesgos internos y externos



Ransomware



Operaciones que te detienen en seco



Ingeniería social



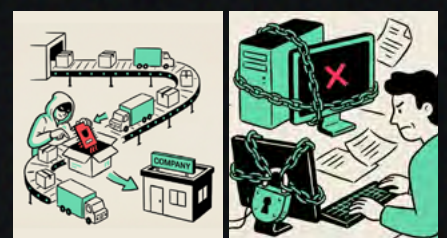
Robo de credenciales, interrupción de actividades comerciales



Ataques sin archivos y malware



Robo de datos, sistemas inestables



Ataques a la cadena de suministro



Interrupciones para los clientes y pérdida de confianza

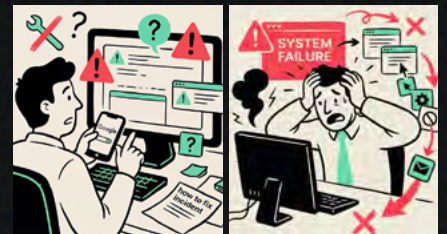
Desafíos



Rápido crecimiento de TI



Seguridad que no puede seguir el ritmo



Escasez de habilidades



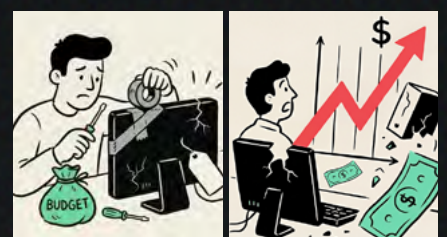
Decisiones incorrectas que empeoran situaciones



Departamento de TI sobrecargado



Amenazas no detectadas y retraso en respuestas

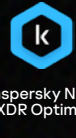
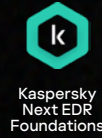


Presupuesto limitado



Costos de recuperación más altos a futuro

¿Cómo abordamos estas amenazas y desafíos en Kaspersky?



	Malware + <i>Amenazas comunes</i>	●	●	●	●
	Ransomware	●	●	●	●
	Ataques sin archivos	●	●	●	●
	Phishing	●	●	●	●
	Malware desconocido <i>Nuevo y dirigido</i>		●	●	●
	Error humano		●	●	●
	Terceros no controlados		●	●	●
	Ingeniería social			●	●
	Movimiento lateral			●	●
	Falta de recursos				●
	Continuidad empresarial				●

Servicio administrado de expertos en Kaspersky

Lo que significa la seguridad de confianza para ti

Protección automática de amenazas

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

Menor carga de trabajo para 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

Detén las amenazas evasivas antes de que se conviertan en incidentes

Recuperación rápida si ocurre un error

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

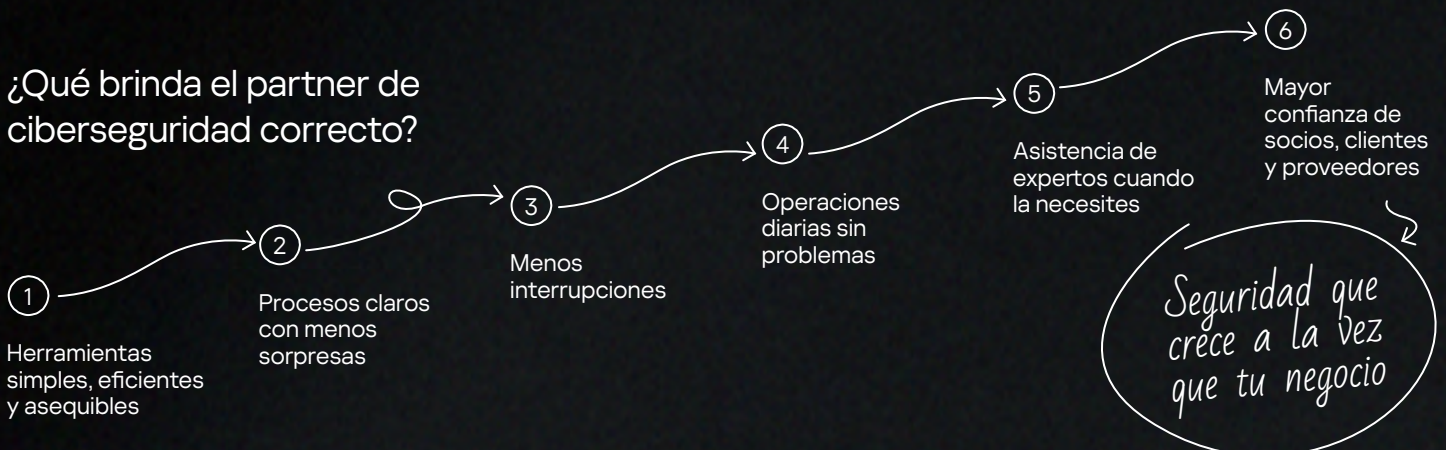
Protección contra ingeniería social

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

Seguridad experta sin crear un equipo

Obtén una protección fuerte sin el coste ni las molestias de contratar a especialistas

¿Qué brinda el partner de ciberseguridad correcto?



¿Quieres una seguridad nativa de nube creada para ti?

Obtén una protección que funcione desde el primer día

Ponte en contacto con nosotros

www.kaspersky.com

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