2025

Encuesta CISO América Latina

kaspersky

latam.kaspersky.com

Introducción

Los profesionales de la ciberseguridad de todo el mundo enfrentan desafíos cada vez más complejos para mantener seguros los datos y sistemas de sus organizaciones. Los activos digitales desempeñan un papel cada vez más importante en todos los sectores industriales, el volumen y la complejidad de los ciberataques están en aumento, las nuevas tecnologías, en constante evolución, están disponibles tanto para los ciberdelincuentes como para quienes los combaten.

En América Latina, a los responsables de la toma de decisiones relativas a la ciberseguridad les resulta difícil establecer prioridades para sus organizaciones y encontrar el presupuesto para soluciones que se integren con los sistemas existentes y actualicen eficazmente las medidas de protección para responder a demandas que están en constante evolución. Un nuevo estudio encargado por Kaspersky ilustra el reconocimiento generalizado de que un enfoque proactivo es la única base sólida para avanzar en la ciberprotección, pero que la mayoría de las organizaciones no han implementado las soluciones correspondientes. De hecho, la implementación de medidas de protección estándar sigue siendo incompleta.

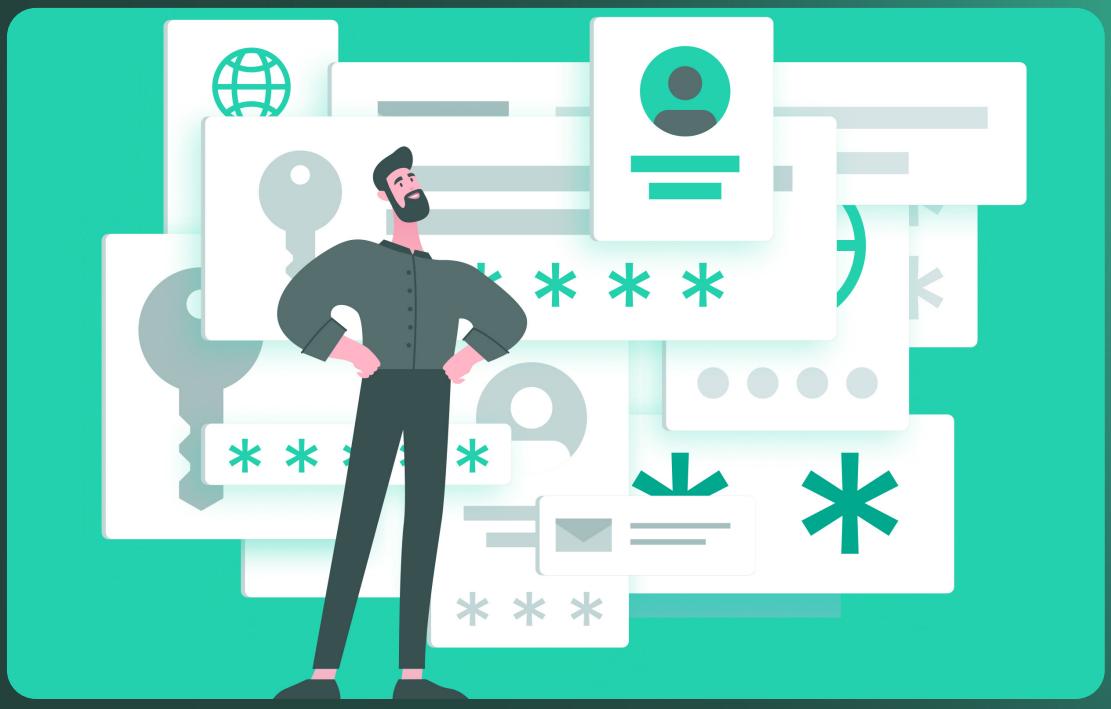
Ante una clara falta de comprensión del estado de las configuraciones de protección actuales y de las oportunidades para crear sistemas más resilientes, es vital ofrecer no sólo las últimas soluciones, sino también acceso a información y asesoría a empresas de todos los tamaños en el mercado latinoamericano.

"A los responsables de la toma de decisiones en materia de ciberseguridad les resulta difícil establecer prioridades para sus organizaciones"

Kaspersky encargó un estudio de investigación de mercado en América Latina destinado a comprender el estado actual de la gestión de la ciberseguridad y las percepciones sobre nuevas soluciones y tecnologías para garantizar la seguridad futura de los sistemas, redes e información.

La muestra de 300 entrevistas consistió en profesionales de ciberseguridad y responsables de la toma de decisiones en el ámbito de la seguridad de redes e información (CIO, CISO, CTO, profesionales de seguridad de la información que se ocupan de la seguridad de redes e información o evaluaciones de seguridad, analistas de SOC y especialistas en TI que, al menos parcialmente, se encargan de tareas de seguridad de la información). Todos trabajan en organizaciones con equipos de TI dedicados, en diversos sectores. Los mercados incluidos son Argentina (n=50), Brasil (n=50), Chile (n=50), Colombia (n=50), México (n=50) y Perú (n=50). Las fechas del trabajo de campo fueron del 25 al 31 de marzo de 2025.

Conclusiones clave



Los profesionales de ciberseguridad en Latinoamérica confían plenamente en su capacidad actual para identificar eficazmente (93%) las ciberamenazas y consideran que su historial de respuesta rápida a incidentes cibernéticos es excelente (92%). Sin embargo, como demuestra este estudio, la implementación de tecnologías de ciberseguridad en muchas organizaciones es irregular y desactualizada, y la eficacia de respuesta y resolución dista mucho de ser óptima. Como reflejo de esta realidad, un tercio (35%) afirma que esto es esencial para cerrar las brechas en su infraestructura de ciberseguridad, junto con una mayor inversión en la detección de amenazas (36%), con planes específicos para adquirir más software para este fin (51%).

De cara al futuro, los responsables de la ciberseguridad no expresan la misma certeza: el 90% afirma que, definitivamente, hay trabajo por hacer para que los datos y sistemas de sus empresas permanezcan seguros dentro de dos años, y el 45% incluso afirma que esto requerirá mucho trabajo. No es sorprendente, considerando que la mayoría ha observado un aumento significativo de ciberataques a sus organizaciones durante los últimos dos años (81%), y estos no solo están aumentando en número, sino también en sofisticación (82%).

En cuanto a tecnologías más avanzadas, menos de la mitad (42%) de las organizaciones latinoamericanas utilizan SIEM (Security Information and Event Management), sólo el 31% utiliza EDR (Endpoint Detection and Response) y un porcentaje aún menor (25%) utiliza XDR. Existen planes concretos para implementar estas tecnologías más avanzadas: un 30% para XDR y una cuarta parte para SIEM (26%) y EDR (25%). Además de tecnologías más avanzadas (38%), se necesita capacitación adicional del personal de TI actual (43%) y mayores inversiones generales en ciberseguridad (41%) para mejorar las configuraciones existentes de ciberseguridad.

A pesar de reconocer la necesidad inequívoca de diversas mejoras, establecer prioridades sigue siendo difícil, y más de la mitad (56%) no realiza una evaluación de riesgos periódica, respondiendo en cambio a ataques o eventos externos como desencadenantes para revisar su ciberseguridad actual. El análisis de causa raíz (44%) y la identificación de amenazas en tiempo real (42%) son las partes que consumen más tiempo del proceso de respuesta a incidentes, lo que refleja una posible falta de comprensión sobre los beneficios que ofrece una mayor automatización.

Percibir las tecnologías como proactivas o reactivas muestra que hay un amplio desacuerdo sobre qué las hace proactivas (desde los firewalls hasta la XDR, algunos las describen como proactivas, otros como reactivas). Sin embargo, muchos coinciden en los beneficios del uso de tecnologías proactivas, en particular la detección temprana de amenazas (52%), la mejora de la gestión de riesgos (52%), la detección de amenazas más avanzadas y tiempos de respuesta a incidentes más rápidos (ambos con 45%).

La información sobre los avances más recientes en tecnología para respaldar la seguridad de la información y los sistemas proviene principalmente de los proveedores (el 51% obtiene información de ellos), pero gran parte de la inteligencia sobre amenazas se recopila a mano (53%).

Se reconoce ampliamente que elevar la ciberseguridad actual al nivel de rendimiento necesario para enfrentar las amenazas futuras es un desafío serio, pero hay muchas personas que no tienen una idea clara de los pasos que deben seguir o de lo que las tecnologías avanzadas pueden ofrecerles para ayudarles a avanzar hacia un enfoque de la ciberseguridad más genuinamente proactivo.

Gestionar la ciberseguridad hoy

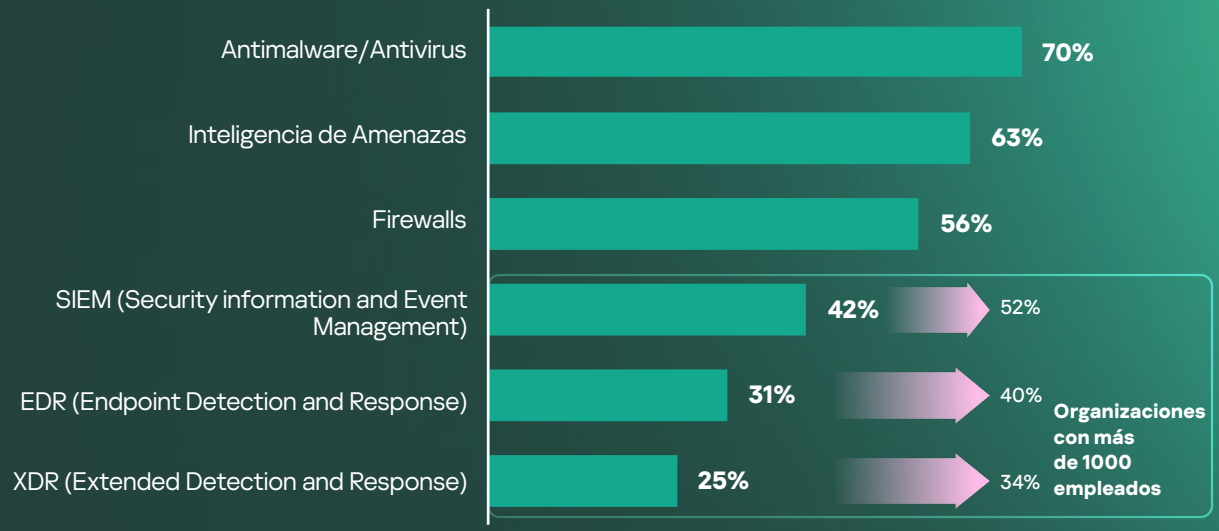
"Las organizaciones más pequeñas tienen más probabilidades de externalizar la capacidad de TI",

Todas las organizaciones que participaron en el estudio cuentan con equipos de TI dedicados, que recurren a recursos internos y externos para obtener a la experiencia y el personal necesarios. Más de la mitad (56%) cuenta con un equipo interno, el 30% combina profesionales de TI internos y externos en sus equipos, y el 14% cuenta con equipos totalmente externos. Como era de esperar, las organizaciones más pequeñas son más propensas a recurrir a proveedores de TI externos, ya que suelen tener menos personal disponible: el 20% de las PyMEs (hasta 499 empleados) externalizan completamente sus equipos de TI, pero solo el 5% de las organizaciones con más de 1,000 empleados recurre a esta modalidad.

La confianza en sus capacidades de protección es generalmente alta en las empresas latinoamericanas: más del 90% en general dice que tiene plena confianza en su capacidad para identificar amenazas cibernéticas de manera efectiva y cree que su historial en responder rápidamente a las amenazas cibernéticas es excelente.

Casi dos tercios consideran que los datos y sistemas de su organización están muy bien o incluso extremadamente bien protegidos (64%), y casi todos (97%) enfatizan que la prevención de ciberataques es una prioridad clave para sus organizaciones. Alrededor del 90% en general afirma haber realizado inversiones considerables en la prevención de vulnerabilidades en sus redes y sistemas. Esto es especialmente relevante para las organizaciones grandes: 97% de las que cuenta con más de 1000 empleados confirma haber dedicado importantes recursos a este objetivo, en comparación con sólo el 88% de las que tienen menos de 500 empleados.

Las tecnologías de ciberseguridad empleadas actualmente reflejan principalmente enfoques tradicionales, e incluso la implementación de medidas de protección estándar sigue siendo incompleta. Casi un tercio (30%) no utiliza software antivirus o antimalware, más de un tercio no utiliza inteligencia de amenazas y el 44% no dispone de firewall. Si bien incluso menos organizaciones utilizan SIEM, EDR y XDR, las empresas más grandes tienen una probabilidad significativamente mayor de utilizarlos.



¿Cuáles de las siguientes tecnologías de seguridad ya forman parte de su estrategia actual de seguridad de la información?

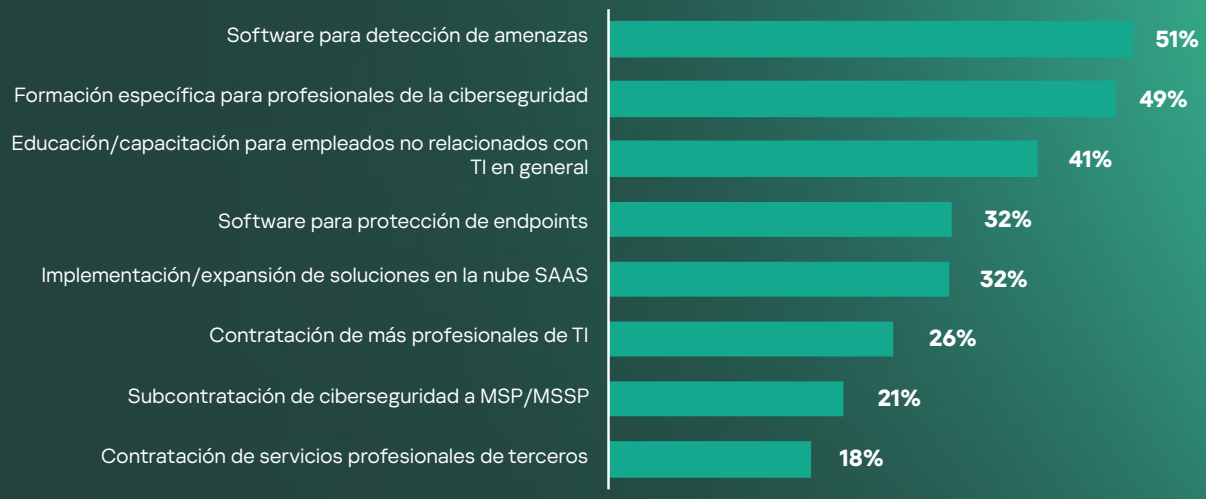
A pesar de su confianza, a los profesionales de la ciberseguridad les preocupa la rápida evolución del panorama de amenazas: el 81% ha observado un volumen mucho mayor de ciberataques en los últimos dos años y el 82% informa de una complicación significativamente mayor de estos ataques. Como reflejo de esta preocupación, sólo el 10% cree que su configuración actual de ciberprotección está preparada para el futuro, mientras que hasta un 45% afirma que queda mucho trabajo por hacer para garantizar la seguridad futura de los datos y sistemas de su organización.

En línea con esto, una proporción considerable de quienes aún no utilizan tecnologías más avanzadas planean hacerlo próximamente: el 30% desea incorporar XDR a su arsenal de defensa, el 26% SIEM y el 25% EDR. Una cuarta parte (26%) también planea empezar a utilizar inteligencia de amenazas para mejorar sus capacidades de ciberseguridad.

En general, el 38% considera que contar con más herramientas de software para aumentar la eficacia de su configuración de protección es una prioridad para cerrar la brecha de capacidad, el 41% considera que es necesaria una mayor inversión en general y a la cabeza de la lista está la capacitación adicional del personal de TI actual (43%).

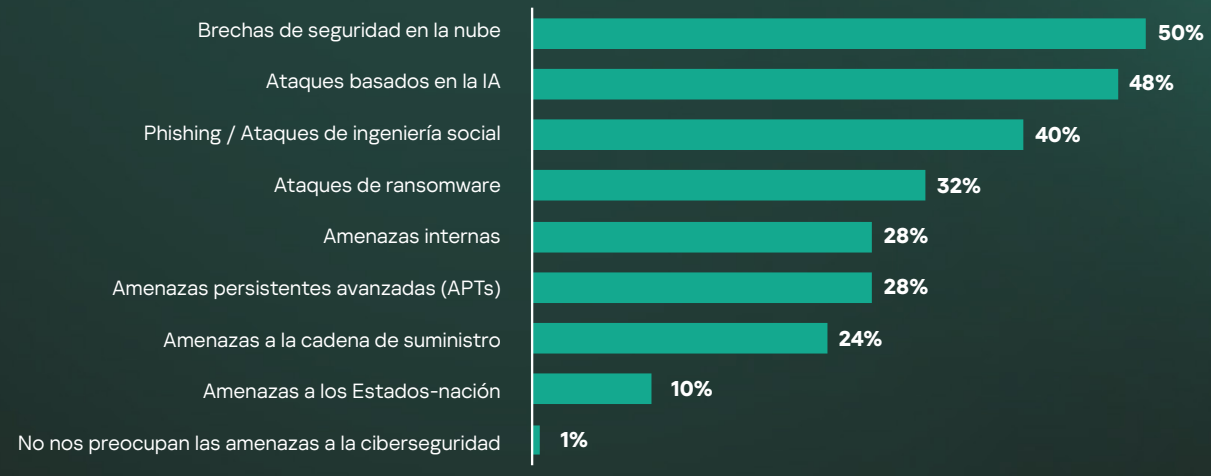
Para la mayoría, es difícil establecer prioridades en sus iniciativas de mejora, pero los planes de inversión concretos para los próximos 12 a 18 meses se alinean con las necesidades actuales: más de la mitad (51%) planea invertir en herramientas de software

para mejorar la detección de amenazas y casi la misma cantidad (49%) en capacitación específica para profesionales de la ciberseguridad. El 41% invertirá en la educación de empleados no informáticos, lo que señala la importancia de defenderse contra una marea creciente de ataques de ingeniería social (una gran preocupación para el 40%).



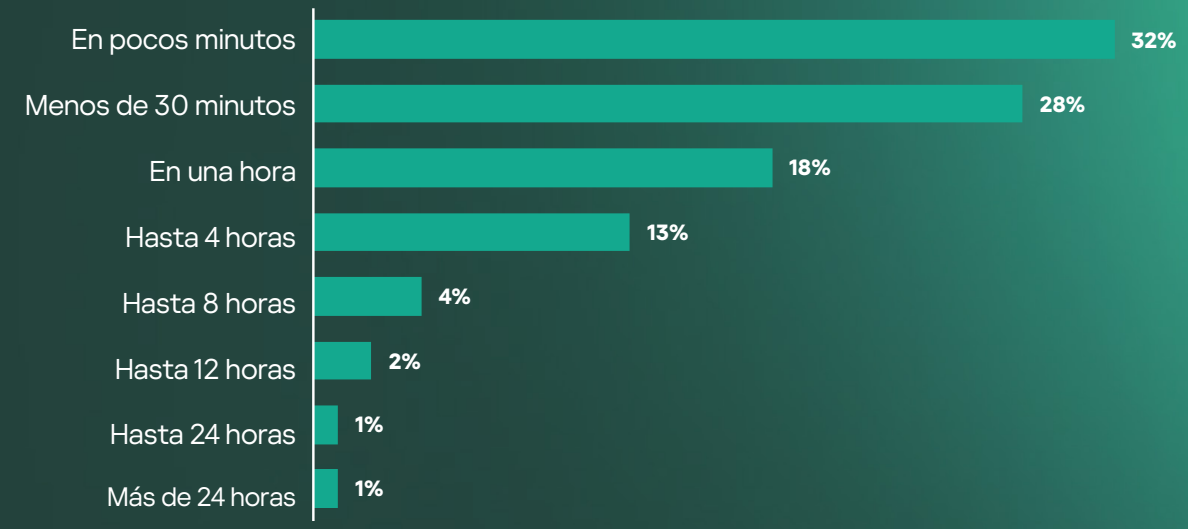
¿Dónde es más probable que su empresa realice inversiones en ciberseguridad en los próximos 12 a 18 meses?

La mayor preocupación proviene de las brechas de seguridad en la nube, un problema que preocupa a la mitad (50%) de las organizaciones. Los ataques basados en IA le siguen de cerca, con un 48% que los considera uno de los tres principales problemas de seguridad. El phishing y otros ataques de ingeniería social ocupan el tercer lugar con un 40%. La sensación general de amenaza se ve reforzada por el escaso número de organizaciones que no tienen inquietudes por la ciberseguridad (sólo el 1%).



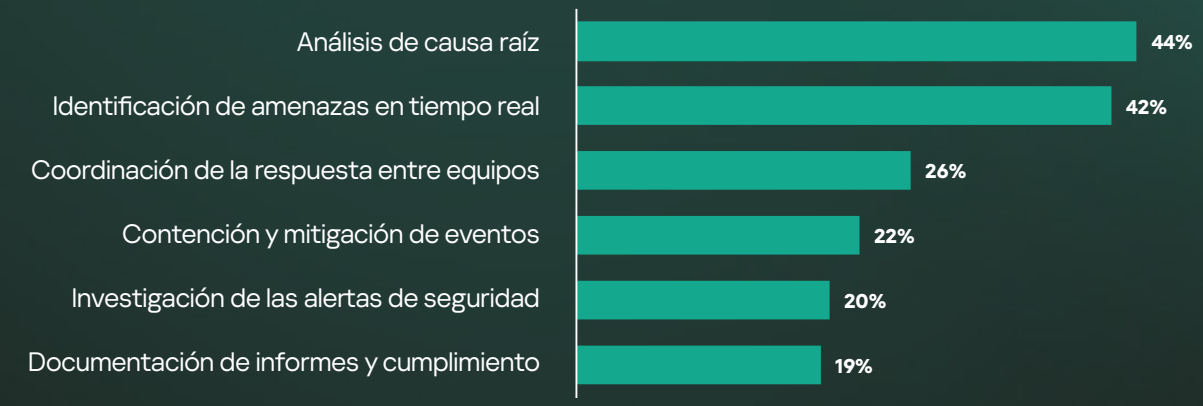
¿Qué amenazas de ciberseguridad preocupan más a su organización? (elija hasta tres respuestas)

Si bien la detección de amenazas cibernéticas claramente necesita mejoras (el 50% planea invertir en herramientas de software para mejorarla), cuando se les pregunta por su tiempo de respuesta típico, casi un tercio (32%) afirma que normalmente lo logra en unos pocos minutos después de tener conocimiento de un ataque, más de una cuarta parte (28%) cita un tiempo de respuesta de menos de 30 minutos.



¿Cuánto tiempo suele tardar su empresa en responder a un incidente una vez que se da cuenta de que está en curso un ataque?

Sin embargo, al analizar los factores que retrasan el proceso de respuesta, estos indican algunas deficiencias fundamentales en la capacidad: la identificación de amenazas en tiempo real es un problema común (42%), sólo superado por el tiempo que lleva realizar el análisis de causa raíz (44%). La coordinación de la respuesta entre equipos retrasa el proceso en un 26%, y para un 22%, la contención y mitigación de eventos supone un problema. Hasta uno de cada cinco (20%) tiene dificultades para investigar las alertas de seguridad de forma eficiente. Todo esto pone de relieve la necesidad de comprender mejor el potencial de automatizar partes clave del proceso.

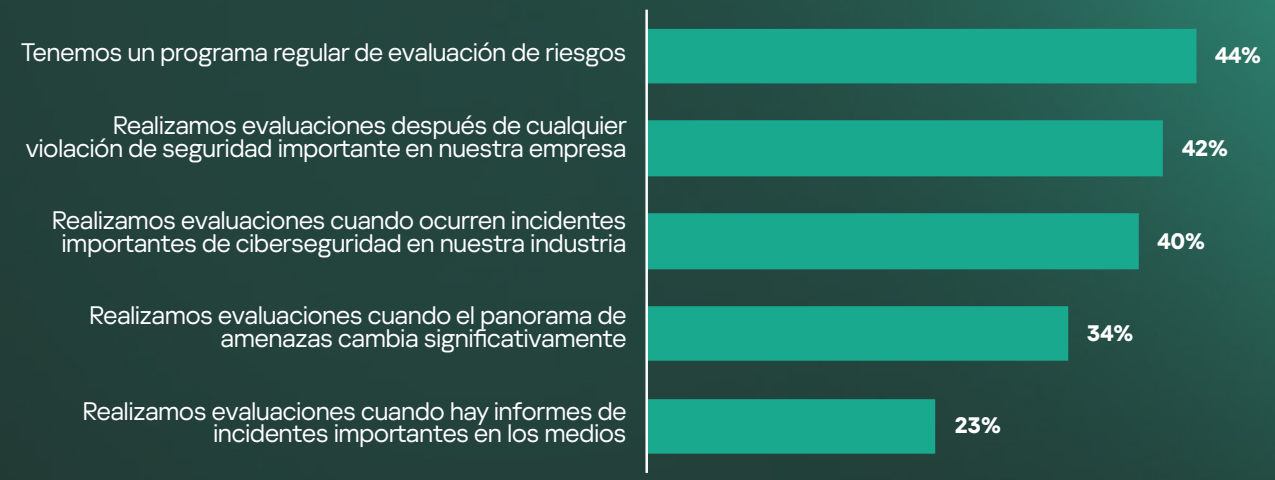


¿Cuál es la parte del proceso de respuesta a incidentes que consume más tiempo en su organización? (Escoja hasta dos respuestas)

Evaluación y mitigación de riesgos

La eficacia de la evaluación de riesgos, la priorización de amenazas y la preparación ante posibles incidentes es clave para una ciberprotección eficaz, especialmente cuando la tecnología transforma el nivel y la complejidad de estas amenazas a una velocidad sin precedentes. Sorprendentemente, más de la mitad (56%) de las organizaciones no cuenta con un calendario regular de evaluación de riesgos, sino que reacciona a eventos internos o externos.

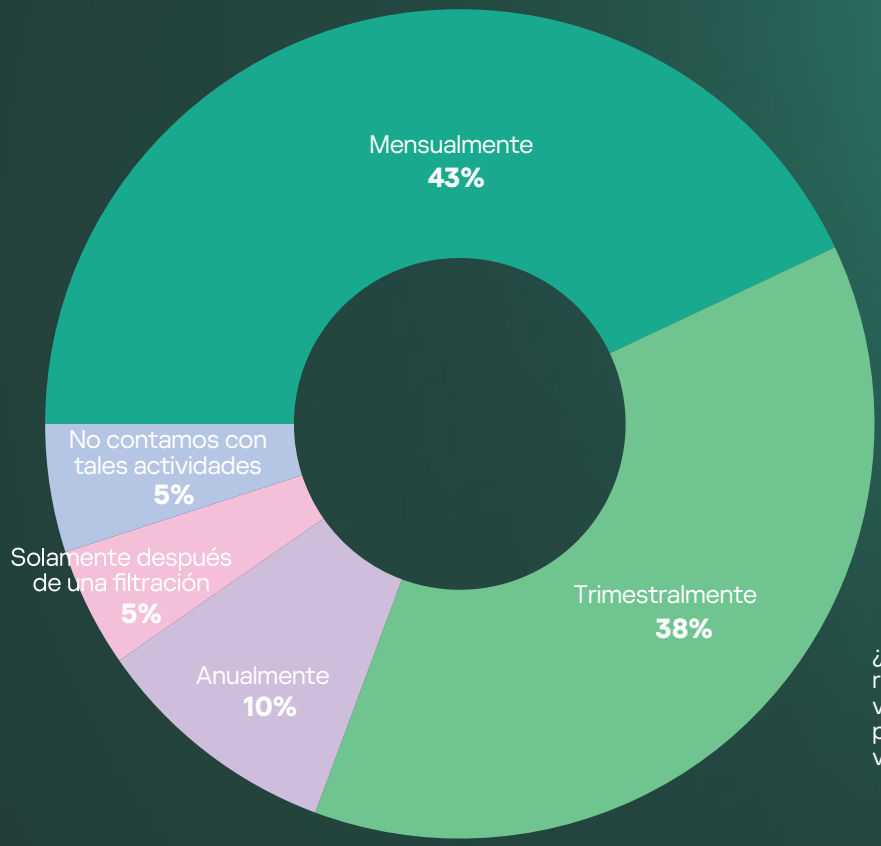
Esto aplica particularmente a las empresas más pequeñas (menos de 500 empleados), donde el 62% no cuenta con un programa regular de evaluación de riesgos, en comparación con el 45% de las que tienen más de 500 empleados. La mayoría reacciona con una evaluación ante brechas de seguridad dentro de su propia organización (42%) o un incidente cibernético significativo en su sector (40%). El desencadenante menos frecuente para una revisión son los informes de los medios de comunicación sobre incidentes importantes.



¿Qué desencadena una evaluación de riesgos de ciberseguridad en su empresa?

Las evaluaciones de riesgos programadas regularmente suelen realizarse mensualmente (por el 67% de quienes tienen un horario establecido, cifra que aumenta al 83% en organizaciones con 1000 o más empleados) y trimestralmente por un tercio, (30%). Como es de esperar, quienes realizan evaluaciones de riesgos como reacción a eventos externos las realizan con menos frecuencia: sólo el 54% las realiza mensualmente, frente al 36% que las lleva a cabo trimestralmente.

Una preparación aún menos activa es evidente cuando se trata de preparar una ciberdefensa efectiva mediante simulacros y ejercicios de respuesta a amenazas: en todas las organizaciones, sólo el 43% los realiza mensualmente, el 38% lo hace trimestralmente, el 10% realiza simulacros y ejercicios de respuesta a amenazas sólo una vez al año, el 5% sólo después de una violación en su organización y otro 5% nunca lo hace.



¿Con qué frecuencia su empresa realiza entrenamientos y simulacros vde respuesta a amenazas para prepararse ante posibles violaciones de ciberseguridad?

Las políticas de ciberseguridad se revisan con una frecuencia similar: el 46% las reevalúa mensualmente (el 51% de las empresas más grandes con más de 1000 empleados), el 36% las revisa trimestralmente. Hasta un 12% sólo lo hace anualmente, y el 5% no cuenta con un proceso para revisar sus políticas de ciberprotección.

Recopilación de inteligencia

Más de la mitad (51%) obtiene información sobre los avances tecnológicos más recientes para la seguridad de la información y los sistemas de los proveedores de seguridad a través de seminarios web, talleres, reuniones o materiales como informes y libros blancos. Esto aplica especialmente a las organizaciones más grandes: dos tercios (65%) recurren a proveedores de seguridad para acceder a esta información.

Otras fuentes importantes de información son los cursos y formaciones especializados (39%), las organizaciones profesionales o industriales (35%) y las redes sociales y foros en línea (33%).

¿Dónde obtiene información sobre los avances más recientes en tecnología para apoyar la seguridad de la información y los sistemas?

La mitad de las organizaciones adquiere Inteligencia de Amenazas mediante la gestión manual de sus equipos de seguridad internos (53%), cifra que llega al 60% en el caso de las grandes organizaciones con más de 1000 empleados. El 43% utiliza proveedores comerciales de inteligencia de amenazas (el 46% de las que tienen más de 1000 empleados) y el 39% la obtiene de un proveedor externo de MDR o SOC, que también se encarga de prestar servicios de Inteligencia de Amenazas. Sólo el 3% no utiliza ningún tipo de Inteligencia de Amenazas.

La mitad (50%) utiliza uno o dos proveedores comerciales para su Inteligencia de Amenazas, casi una cuarta parte (23%) utiliza tres proveedores de Inteligencia de Amenazas y el 24% utiliza cuatro o más (hasta el 37% de las organizaciones más grandes con más de 1000 empleados).

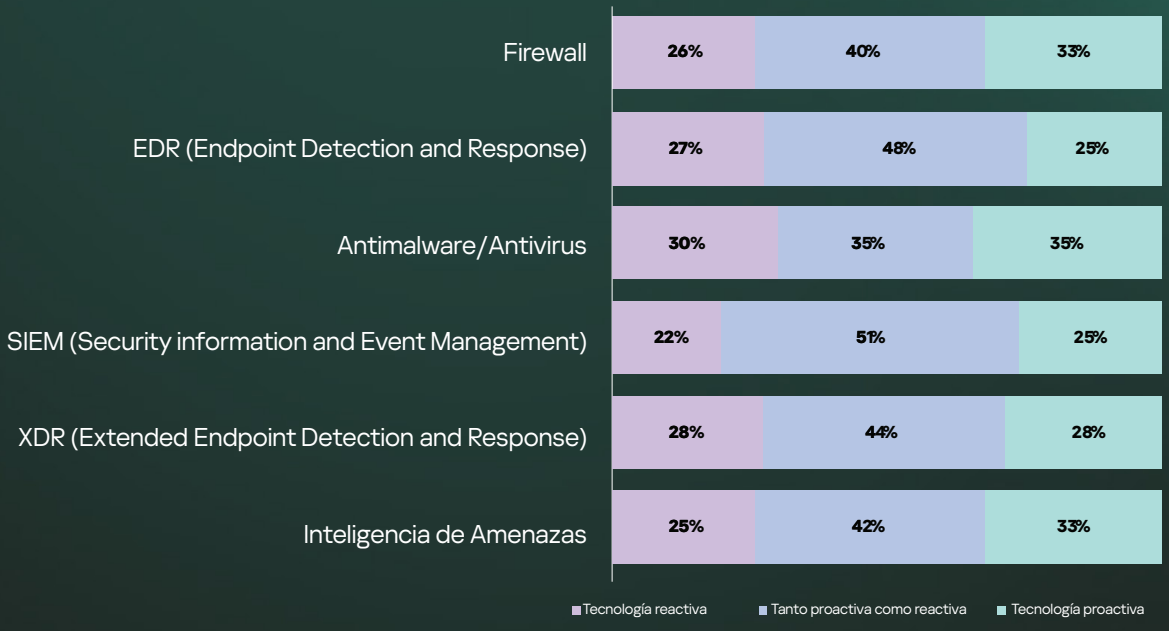
De la reacción a la proactividad

La perspectiva que los profesionales de la ciberseguridad adoptan respecto a su estrategia de defensa influye decisivamente en el diseño y la configuración de las herramientas y tecnologías que utilizan para proteger los datos y sistemas de sus organizaciones. Al preguntarles si su enfoque de la seguridad de la información y los sistemas es más reactivo (respondiendo así a las amenazas y ataques cuando ocurren) o proactivo (centrándose en prevenir los ataques antes de que ocurran), el 69% lo clasificó como proactivo (puntuando del 7 al 10 en una escala de 10 puntos), y sólo el 10% como reactivo (puntuando del 1 al 4). De cara al futuro, el 55% afirmó que adoptaría una estrategia más proactiva en los próximos 12 meses, pero el 27% afirmó que adoptaría un enfoque más reactivo.

Los niveles actuales de inversión no reflejan los niveles reportados de proactividad, ya que sólo el 17% dice que la mitad o más de su inversión en ciberseguridad se destina a XDR e Inteligencia de Amenazas para respaldar la ciberdefensa proactiva. El 47% invierte entre el 25% y el 50% en XDR e Inteligencia de Amenazas, el 37% invierte menos de una cuarta parte de su presupuesto.

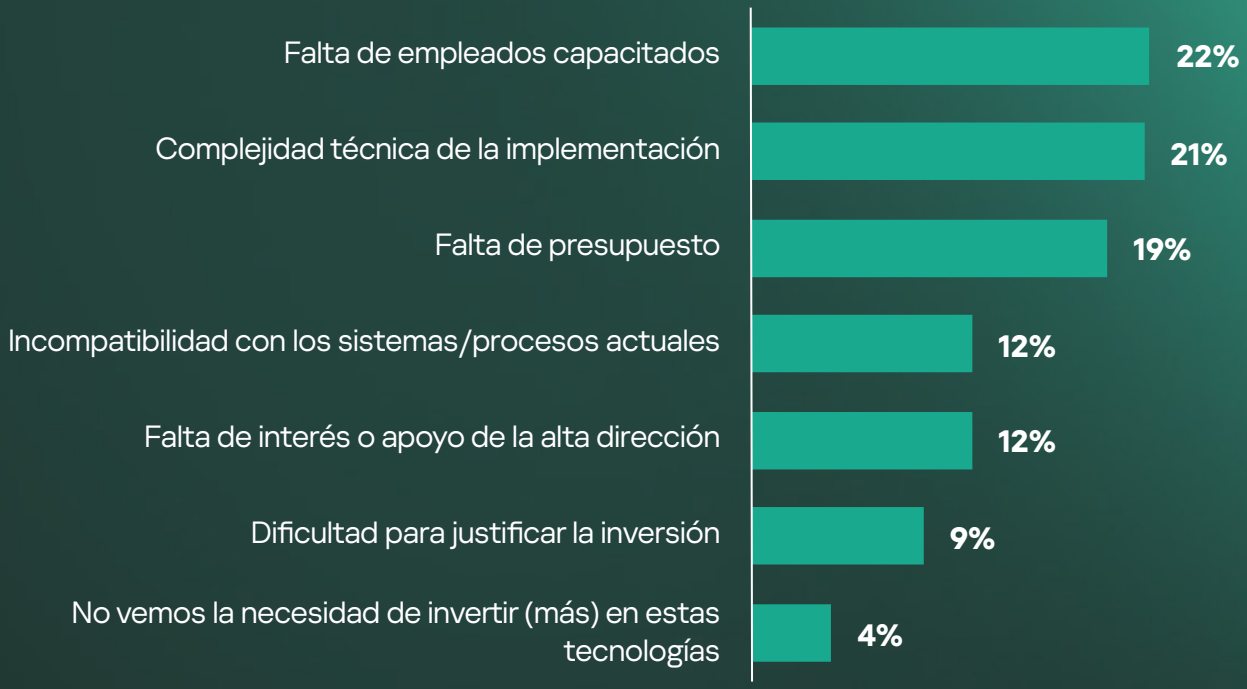
La ciberdefensa proactiva puede definirse, en términos generales, como la capacidad de prevenir ataques antes de que ocurran, creando resiliencia dentro del propio sistema en lugar de responder a los incidentes conforme surgen. Reaccionar a las brechas de seguridad con rapidez y eficacia es importante, pero no se comprende suficientemente el papel y la funcionalidad de las tecnologías proactivas ni cómo optimizar su uso.

Se les preguntó a los profesionales de la ciberseguridad que identificaran una lista de tecnologías conocidas como proactivas, reactivas o ambas; arrojó algunos resultados sorprendentes:



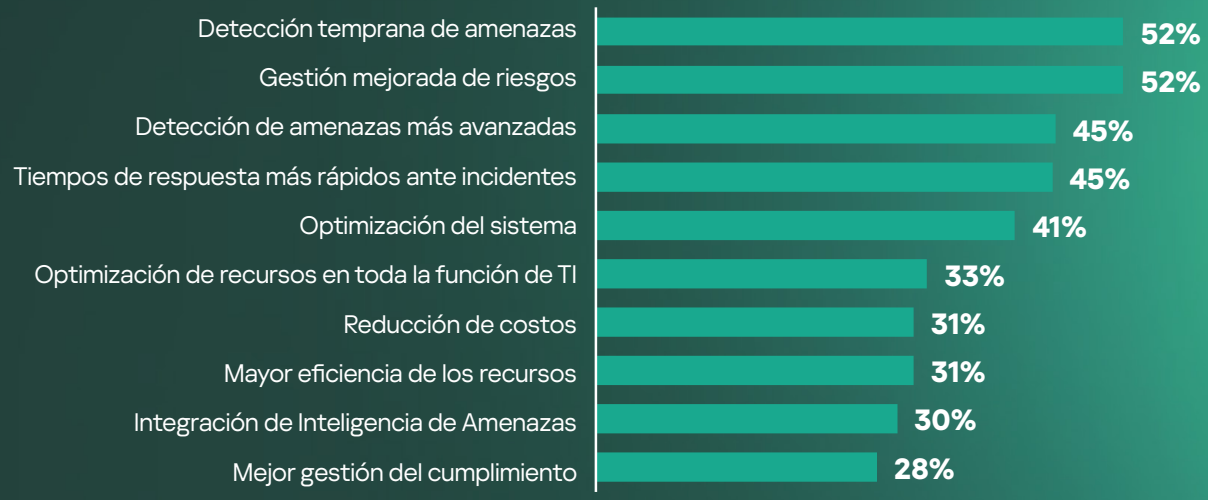
La falta de conocimiento se ilustra por el gran número de profesionales de la ciberseguridad que describen la XDR, la Inteligencia de Amenazas y la EDR como tecnologías reactivas, y los antivirus y antimalware como proactivos. Esto demuestra que la mentalidad preventiva se está expandiendo en la comunidad profesional de la ciberseguridad, pero también que aún no se ha materializado en una estrategia implementada.

El mayor desafío que impide una mayor inversión en estas áreas incluye la falta de personal de TI calificado (22%), la complejidad técnica de la implementación (21%) y la falta de presupuesto (19%). Sólo el 4% afirma no ver motivos para invertir en XDR o Inteligencia de Amenazas.



¿Cuál es el mayor desafío que enfrenta su organización al invertir (más) en tecnologías como XDR e inteligencia de amenazas? (seleccione una respuesta)

La actitud hacia las tecnologías proactivas es positiva y existe un amplio reconocimiento de los beneficios en adoptarlas. Más de la mitad (ambos 52%) mencionan la detección temprana de amenazas y una mejor gestión de riesgos como los principales aspectos positivos, seguidos de la detección de amenazas más avanzadas y tiempos de respuesta más rápidos ante incidentes (ambos 45%).

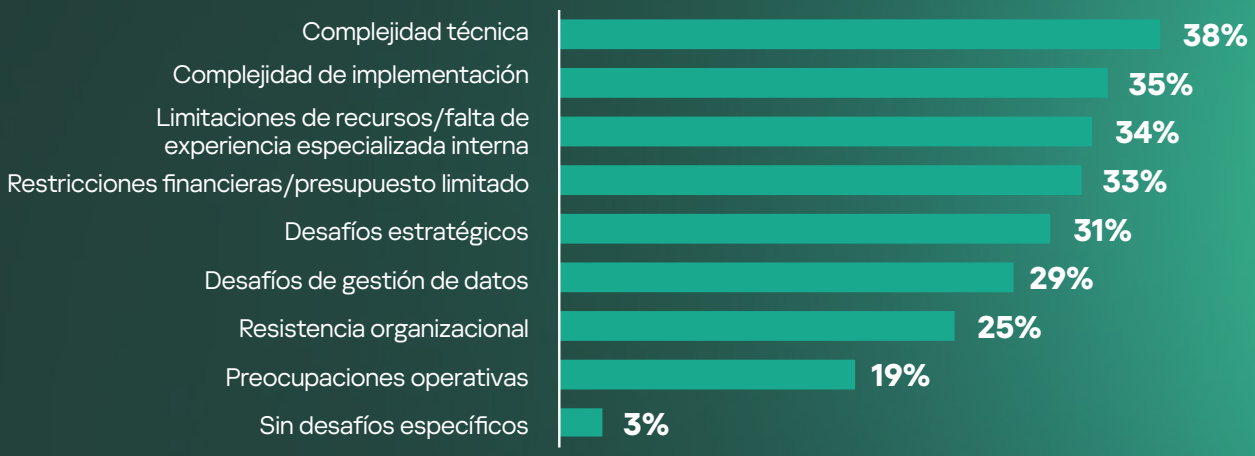


¿Qué beneficios, si los hay, tiene o podría tener la (potencial) adopción de tecnologías proactivas para organizaciones como la suya?

Quienes identifican como un beneficio clave la detección temprana de las amenazas señalan que el beneficio más importante (70%) es la identificación de amenazas potenciales antes de que puedan causar algún daño, seguido de una transición más rápida entre oponerse a la amenaza y detectarla (49%) y el monitoreo del comportamiento de la red para descubrir anomalías (44%).

Una mejor gestión de riesgos se traduce en la evaluación y priorización continua de los riesgos de seguridad como el beneficio clave para el 60%. La visibilidad en tiempo real de la situación de seguridad (46%) y la implementación automática de controles de seguridad (45%) son otros aspectos positivos de una gestión de riesgos mejorada.

Como se mencionó anteriormente, además de los beneficios claramente reconocidos, los profesionales de la ciberseguridad se enfrentan a diversos desafíos al orientar su inversión hacia tecnologías proactivas. Los más comunes son la complejidad técnica (38%), la complejidad de la implementación (35%), las limitaciones de recursos y la falta de experiencia interna especializada (34%). Un tercio menciona las limitaciones financieras (33%), los desafíos estratégicos (31%) y los desafíos de la gestión de datos (29%).



¿Y cuáles son, si los hay, los desafíos que plantea la adopción de tecnologías proactivas?

Los desafíos de complejidad técnica van desde problemas de compatibilidad con la infraestructura heredada (45%), la necesidad de experiencia especializada para implementar y gestionar estas soluciones (44%) y desafíos de integración con la infraestructura existente (39%).

"Dado el esfuerzo general por mejorar la eficacia de la ciberseguridad para proteger eficazmente los datos y sistemas en el futuro, la inteligencia de amenazas desempeñará un papel fundamental para todas las organizaciones comerciales".

La necesidad de una planificación y pruebas cuidadosas (49%) es un obstáculo clave dentro de la complejidad de la implementación; también son difíciles la coordinación entre varios departamentos (41%) y los procesos de implementación que consumen mucho tiempo (40%).

Las limitaciones de recursos también se dividen en varios aspectos: escasez de profesionales capacitados en ciberseguridad (48%), experiencia interna limitada para la implementación (44%) y equipos de seguridad con poco personal (40%).

La limitación financiera más desafiante es el alto costo inicial de las soluciones de seguridad avanzadas (60%). Los gastos continuos de licencias y mantenimiento también representan un problema para más de la mitad (55%).

Dado el impulso general hacia la mejora de la eficacia de la ciberseguridad para proteger los datos y los sistemas de manera efectiva en el futuro, la Inteligencia de Amenazas desempeñará un papel vital para todas las organizaciones comerciales al ayudarlas a comprender a los agentes de amenazas, sus tácticas y posibles vulnerabilidades del sistema, respaldando estrategias de defensa más efectivas y una mejor resolución de incidentes.

Para traducir esta información en soluciones prácticas se necesitará experiencia adicional y el apoyo de proveedores profesionales para desarrollar y seleccionar las soluciones proactivas más adecuadas para cada organización, a fin de superar los desafíos y maximizar los beneficios asociados con el avance hacia una ciberprotección más resiliente.

Recomendaciones de Kaspersky

Las medidas de ciberseguridad de los especialistas de Kaspersky que colaboraron en este estudio tienen como objetivo fortalecer la ciberresiliencia de las organizaciones, reduciendo el tiempo de respuesta ante incidentes, ampliando la capacidad de detección y prevención de amenazas y promoviendo una cultura de seguridad integrada a la estrategia de negocio.

Las sugerencias se agrupan en tres grandes pilares: Gobernanza y Estrategia, Tecnología e Infraestructura y Capacitación y Recursos Humanos.

1. Gobernanza y Estrategia

- Definir roles y responsabilidades formales para la gobernanza de seguridad.
- Realizar evaluaciones de riesgo de manera constante, con una periodicidad definida (al menos trimestral).
- Contar con planes de respuesta a incidentes probados regularmente mediante simulaciones.
- Revisar periódicamente las políticas de seguridad y los controles críticos.
- Implementar indicadores de desempeño y riesgo (KPIs y KRIs) que conecten la ciberseguridad con los resultados del negocio.
- Priorizar medidas fundamentales de protección: gestión de vulnerabilidades, copias de seguridad automatizadas y autenticación multifactor.
- Adoptar frameworks reconocidos de madurez y gobernanza, como el NIST Cybersecurity Framework, ISO/IEC 27001 y CIS Controls, para orientar las políticas y prácticas corporativas.
- Implementar procesos de gestión de riesgos de terceros y de la cadena de suministro (supply chain), evaluando los controles de seguridad de socios y proveedores de servicios críticos.
- Crear comités de seguridad interdepartamentales, integrando TI, seguridad y áreas de negocio para la toma conjunta de decisiones.
- Incorporar métricas de seguridad y resiliencia en los paneles de desempeño ejecutivo.
- Asegurar el cumplimiento de las leyes de protección de datos y privacidad de la región, incluyendo la LGPD (Brasil), la Ley 25.326 (Argentina), la Ley de Protección de Datos Personales (México) y las normas de Habeas Data (Colombia, Perú), o alinear el programa de seguridad con la Estrategia Nacional de Ciberseguridad vigente en cada país.

2. Tecnología e Infraestructura

- Garantizar el uso completo y actualizado de las herramientas básicas: protección de endpoints, firewall, copias de seguridad y control de acceso.
- Integrar nuevas soluciones con sistemas heredados para eliminar brechas de cobertura.
- Adoptar la automatización en los flujos de detección y respuesta, reduciendo el tiempo de reacción ante incidentes.
- Evaluar y priorizar la adopción de soluciones avanzadas (EDR, XDR, SIEM) para ampliar la visibilidad y la capacidad de correlación de eventos, permitiendo detectar incidentes en etapas tempranas.
- Incorporar inteligencia de amenazas integrada en las plataformas de seguridad para detectar comportamientos anómalos.
- Fortalecer las alianzas con proveedores de inteligencia y laboratorios de investigación para mantener la actualización constante sobre TTPs recientes.
- Promover la integración entre SOC, TI y áreas de negocio para una respuesta coordinada.
- Establecer políticas de actualización, pruebas y mantenimiento preventivo en toda la infraestructura crítica.
- Implementar un programa estructurado de gestión de vulnerabilidades, con escaneos periódicos, priorización por criticidad y corrección ágil.
- Reforzar la gestión de identidades y accesos (IAM) con políticas de mínimo privilegio y autenticación multifactor en todos los sistemas.
- Realizar simulaciones regulares de incidentes para validar la eficacia técnica y los flujos de comunicación.
- Adoptar arquitecturas escalables y resilientes, con segmentación de red y modelo Zero Trust.
- Utilizar orquestación y automatización de incidentes (SOAR) para reducir la dependencia de la intervención manual.
- Desarrollar y mantener planes de continuidad del negocio (BCP) y recuperación ante desastres (DRP), probándolos regularmente.
- Realizar análisis de impacto al negocio (BIA) para identificar procesos y activos críticos para la operación.

3. Capacitación y Recursos Humanos

- Realizar campañas de concientización continuas y no puntuales sobre phishing, ingeniería social y buenas prácticas digitales.
- Ofrecer capacitación técnica permanente para los equipos de TI y seguridad en:
- Respuesta a incidentes.
- Análisis de malware.
- Uso de herramientas de Threat Intelligence.
- Fomentar certificaciones profesionales y la participación en foros y comunidades especializadas.
- Crear centros internos de competencia dedicados a threat intelligence, gestión de vulnerabilidades y respuesta a incidentes.
- Desarrollar programas avanzados de formación en threat hunting, análisis forense y gestión de riesgos digitales.
- Establecer alianzas estratégicas con proveedores de inteligencia, universidades y centros de investigación.
- Integrar prácticas de seguridad en el ciclo de desarrollo (DevSecOps), acercando seguridad, TI e innovación.
- Promover entrenamientos de crisis y comunicación en incidentes, preparando a ejecutivos y líderes para la toma de decisiones bajo presión y para emitir mensajes consistentes al público interno y externo.
- Utilizar metodologías prácticas como KIPS (Kaspersky Interactive Protection Simulation) y ejercicios tabletop para probar respuestas en tiempo real.
- Fomentar la creación de una cultura de seguridad continua, en la que las buenas prácticas y la vigilancia digital formen parte del día a día de la organización.

kaspersky