MANDIANT®

NOW PART OF Google Cloud

Perspectivas globales sobre la inteligencia de amenazas

Como señala nuestro informe "Perspectivas globales sobre la inteligencia de amenazas", a los equipos de seguridad les preocupa que líderes sénior no logren comprender del todo la naturaleza de la amenaza. Esto significa que se están tomando decisiones críticas de ciberseguridad sin una perspectiva clara del adversario ni sus tácticas.

Sandra Joyce
Vicepresidenta de Mandiant Intelligence
Google Cloud

Este informe único en su tipo ofrece una visión de cómo las organizaciones navegan por el panorama mundial de las amenazas de ciberseguridad. Las conclusiones se han obtenido a partir de entrevistas exhaustivas a 1350 directivos de empresas y TI que toman decisiones sobre seguridad en organizaciones con al menos 1000 empleados. Los encuentados procedían de 13 países en tres distintas regiones y de organizaciones pertenecientes a 18 sectores de la industria, incluidos los servicios financieros, la atención médica y gobierno.

La calidad y el alcance global de las respuestas proporcionan una idea de cómo las personas responsables de tomar decisiones con relación a la ciberseguridad en grandes organizaciones ven y ponen en práctica la inteligencia de amenazas.

Hallazagos

Las respuestas confirman la suposición inicial de que, aunque los equipos valoran la inteligencia de amenazas y la reciben de múltiples fuentes, a menudo tienen dificultades para aplicar la información de forma eficaz a lo largo de sus organizaciones.

Los equipos de seguridad de las empresas más grandes del mundo enfrentan no sólo enormes presiones, sino también desafíos en las comunicaciones a lo largo de su organización. Además, si bien los equipos de seguridad comprenden claramente la necesidad de disponer de una mejor inteligencia sobre los actores de amenaza, muchos de estos toman decisiones sin tener una comprensión total de quién está atacando su organización y por qué. Esta falta de visibilidad ocasiona que las defensas tal vez no cumplan los objetivos esperados.

El 96 % de los encuestados están satisfechos con la calidad de la inteligencia de amenazas que utiliza su organización

El 47 % de los encuestados considera que uno de sus mayores retos es aplicar eficazmente la inteligencia de amenazas en toda la organización de seguridad

El 67 % de los encuestados cree que el equipo de liderazgo sénior subestima la ciberamenaza contra la organización

El 96 % de los responsables de tomar decisiones en materia de seguridad cree que es importante comprender qué qué actores de amenaza cibernéticos podrían estar atacando a su organización

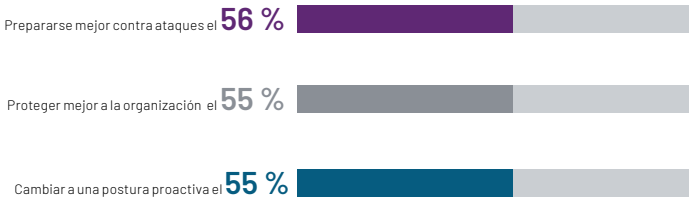
El 79 % de los encuestados afirma que, al menos la mayoría de las veces, toman decisiones sin conocimiento profundo del adversario

Conciencia de las amenazas de las amenazas y sentimiento de seguridad por parte de los profesionales

El informe revela una discrepancia global entre el alto nivel de confianza que tienen las organizaciones a la hora de hacer frente a los ciberataques y la tendencia de los equipos de seguridad a tomar decisiones sin disponer de una información exhaustiva sobre los actores de amenaza y sus tácticas, técnicas y procedimientos (TTPs).

También muestra que una mayoría importante (96 %) de los responsables de tomar decisiones de seguridad cree que es importante comprender qué actores de amenaza podrían estar atacando a su organización.

Como responsable de tomar decisiones de seguridad, ¿por qué cree que es importante comprender qué actores de amenaza cibernéticos podrían estar atacando a su organización?

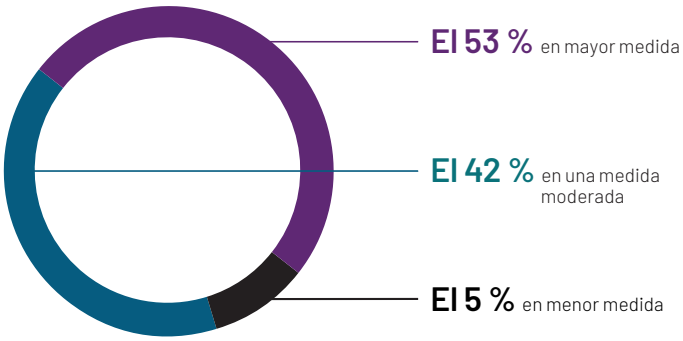


A pesar de la comprensión casi universal de la importancia de adquirir información sobre los actores de amenaza cibernéticos y de que el 96 % de los encuestados afirman estar satisfechos con la calidad de su inteligencia de amenazas, el 79 % de los encuestados sostiene que toman la mayoría de sus decisiones sobre ciberataques sin contar con conocimiento profundo de quién podría estar atacando a su organización. Solo el 35 % afirma que su organización posee un conocimiento exhaustivo de los distintos grupos de amenaza y sus TTPs.

Además, el 67 % de los responsables de tomar decisiones sobre la ciberseguridad cree que los equipos de liderazgo sénior aún subestiman lo que las ciberamenazas representan para las organizaciones, mientras que más de dos tercios (68 %) están de acuerdo en que su organización necesita mejorar su comprensión sobre el panorama de amenaza.

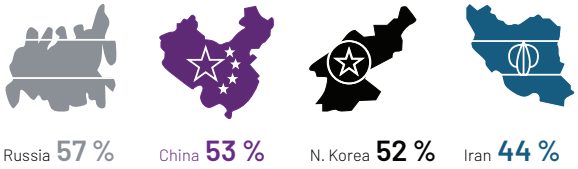
Independientemente de estas preocupaciones, la confianza es alta entre los responsables de tomar decisiones con relación a que sus organizaciones pueden hacer frente a amenazas de seguridad. Casi todos los encuestados (95 %) afirman que creen poder demostrar al equipo de liderazgo sénior que su organización cuenta con un programa de ciberseguridad con una eficacia que va de moderada a alta.

¿Hasta qué punto cree que puede demostrar a su equipo de liderazgo sénior (como la junta de ejecutivos o el cuerpo de directivos) que su organización cuenta con un programa de ciberseguridad eficaz?

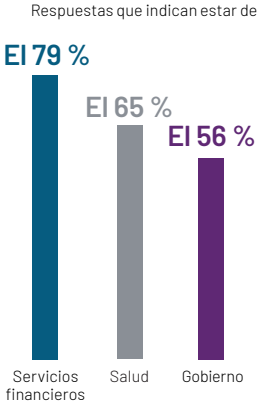


Muchos responsables de la toma de decisiones en materia de seguridad confían en que su organización está totalmente preparada para defenderse de un ataque importante de ciberseguridad causado por un actor con motivaciones financieras (91 %), un hacktivista (89 %) o un Estado-nación (83 %).

En el caso de un ataque de un Estado-nación, ¿contra cuáles de los siguientes países cree que su organización no podría defenderse completamente?

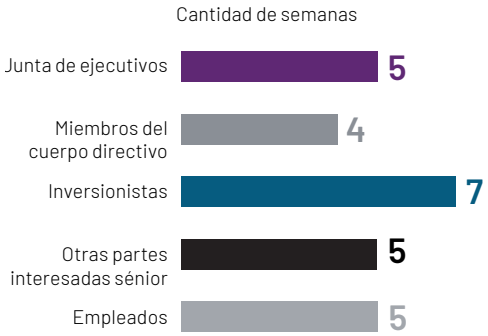


¿Está de acuerdo o no? Mi organización debe mejorar la comprensión del panorama de amenazas.



Una probable explicación de la falta de información sobre los actores de amenaza es la escasa comunicación entre los responsables de la toma de decisiones en materia de seguridad y su organización en general. Los encuestados señalaron que el tema de la ciberseguridad sólo se aborda, en promedio, una vez cada 4 o 5 semanas con grupos ajenos al equipo de seguridad, que incluye la junta directiva, el cuerpo de directivos y otras partes interesadas sénior. Las conversaciones son incluso aún menos frecuentes con los inversionistas, con los que el promedio baja a una vez cada siete semanas.

¿Con qué frecuencia su departamento aborda el tema de la ciberseguridad con los siguientes grupos? (Promedio de todas las regiones)

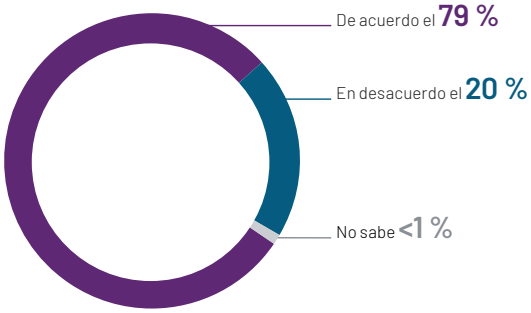


Desafíos de la puesta en práctica de la inteligencia y riesgos relacionados

La importancia de la inteligencia de amenazas fue bien comprendida. Una gran mayoría de los encuestados considera importante identificar al atacante (85 %); las herramientas y técnicas utilizadas por el atacante (88 %); y la motivación del atacante (87 %). A pesar de valorar la información detallada sobre amenazas, los equipos de seguridad revelan que no pueden seguirles el ritmo. Solo el 34 % afirma tener siempre en cuenta el origen de un posible ataque a la hora de probar las defensas y operaciones de ciberseguridad.

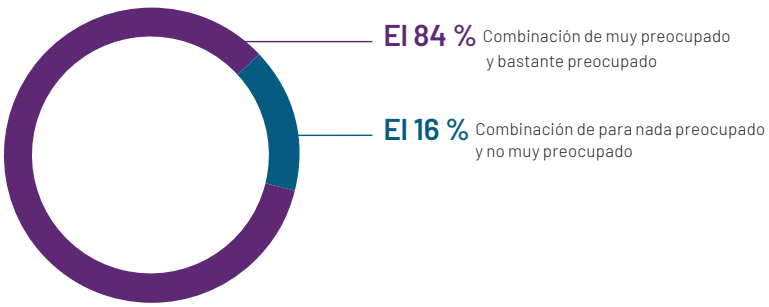
Los equipos de seguridad tampoco invierten el tiempo necesario en identificar las amenazas y actuar en consecuencia. Una gran mayoría de los encuestados (79 %) afirma que su organización podría dedicar más tiempo y energía a identificar tendencias críticas en el ámbito de la ciberseguridad, mientras que casi todos (98 %) afirman que necesitan ser más rápidos a la hora de aplicar cambios en su estrategia de ciberseguridad con base en la inteligencia más reciente sobre amenazas.

¿Está de acuerdo o no? Mi organización podría dedicar más tiempo y energía a las tendencias sobre ciberseguridad que son críticas



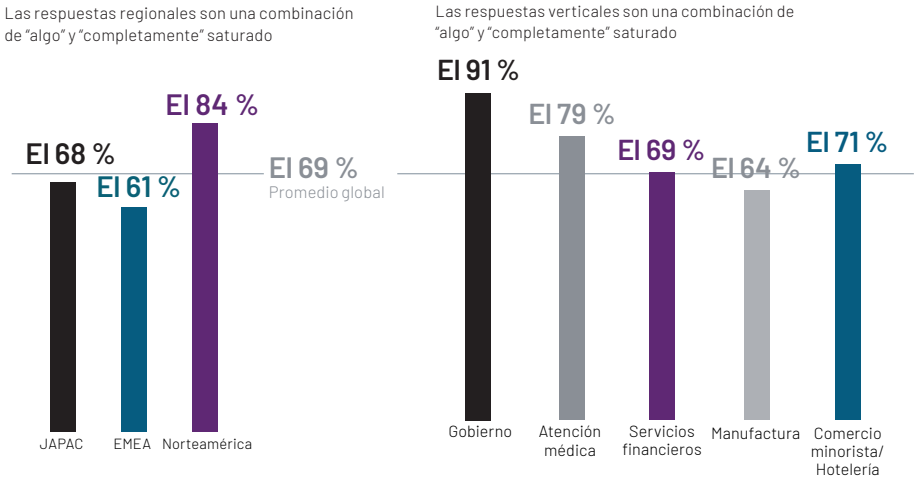
Para obtener inteligencia de amenazas más accionable, los equipos de seguridad deben procesar una gran cantidad de datos todos los días. Una gran mayoría (84 %) de los encuestados afirma estar preocupada de estar pasando por alto amenazas o incidentes debido a la cantidad de alertas y datos a los que se enfrentan. Esta sobrecarga de información también afecta el bienestar del personal: más de dos tercios (69 %) de los equipos de seguridad admite sentirse abrumado.

¿Qué nivel de preocupación tiene de que su organización pueda estar pasando por alto amenazas/ incidentes debido a la cantidad a la cantidad de alertas y datos a los que se enfrenta?



Los encuestados de Norteamérica eran los que corrían más riesgo de agotamiento ante el volumen de datos y alertas relacionados con la inteligencia de amenazas. Entre las verticales de la industria, los encuentados del Gobierno fueron los más propensos a sentirse abrumados.

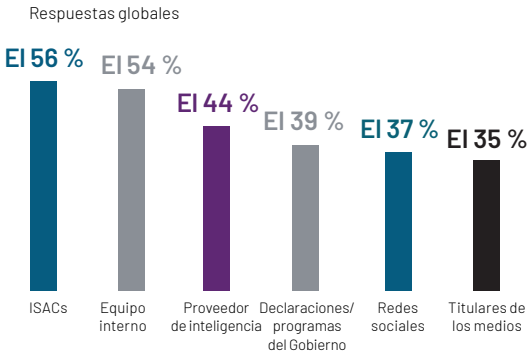
¿Hasta qué punto cree que sus empleados de seguridad informática se sienten abrumados por la cantidad de datos o alertas que tienen que atender?



Si bien la sobrecarga de información se identificó claramente como un desafío para casi todas las organizaciones, casi la mitad (47 %) de los encuestados afirma que aplicar la inteligencia de forma eficaz en toda la organización era uno de los mayores desafíos a los que se enfrentaban al utilizar inteligencia de amenazas y el 38 % afirma que otro desafío era saber qué hacer con la información. Más de la mitad (53 %) afirma que la escasez global de talento en ciberseguridad amenazaba la capacidad de permanecer por delante de de las últimas tendencias, mientras que el 42 % apunta a la naturaleza en constante evolución de las amenazas.

Aunque los equipos se esfuerzan por poner en práctica la inteligencia de amenazas que reciben, siguen recopilando inteligencia desde una amplia gama de fuentes.

¿Qué fuentes utiliza su organización para mantenerse al día sobre el panorama de amenazas?



Con frecuencia, la información recopilada por los equipos de seguridad se mantiene en el ámbito de dichos equipos o no se comparte ampliamente en toda la organización. El 61 % de los encuestados afirma que compartían inteligencia de amenazas con los equipos de TI para abordar las vulnerabilidades de la infraestructura y las aplicaciones o con los responsables de seguridad de TI para priorizar los esfuerzos de seguridad. Un porcentaje mucho menor (38 %) compartió inteligencia con otros empleados para crear conciencia sobre los riesgos.

Para poner en práctica la inteligencia de ciberamenazas de forma eficaz y maximizar el valor de sus inversiones:

Evalúe los datos en los que se basa para asegurarse de que sean confiables, oportunos y se puedan poner en práctica

Un programa fiable de inteligencia de amenazas debe construirse sobre bases firmes y estos atributos son un punto de partida esencial.

Comprenda las amenazas activas específicas para su organización y sector

Construya un panorama claro de los adversarios, sus motivaciones y tácticas, técnicas y procedimientos (TTPs) para adaptar mejor sus defensas.

Comuníquese con sus partes interesadas

Desarrolle una cadencia regular de suministro de inteligencia relevante (táctica, operativa o estratégica) al grupo de partes interesadas a fin de impulsar decisiones de negocio y de seguridad óptimas en todo el nivel del liderazgo sénior y la junta directiva.

Priorice los recursos para abordar lo que realmente importa

Aproveche la inteligencia para comprender cuáles son las amenazas realmente importantes para su organización en este momento. Evalúe las vulnerabilidades y exposiciones y califíquelas en cuanto al riesgo según la criticidad. Después, aborde los problemas en el orden adecuado.

Pruebe sus defensas

Pruebe proactivamente la respuesta de la organización a las tácticas de ataque típicas de los adversarios que ha identificado. Valide su protección frente a estos grupos específicos y mida las mejoras en su programa a lo largo del tiempo.

Tome medidas

Aproveche la inteligencia de amenazas de todos sus sistemas y procesos de seguridad para protegerse de forma proactiva frente a posibles amenazas.

Conclusión

En un panorama de amenazas que evoluciona rápidamente, las organizaciones no sólo deben defenderse de delincuentes cibernéticos sin escrúpulos motivados por el beneficio económico, sino también de los Estados-nación que pretenden perturbar la economía, espiar y atacar infraestructuras críticas.

En este contexto, los responsables de la toma de decisiones pueden utilizar la inteligencia de amenazas para anticiparse a las amenazas antes de que se conviertan en un problema y hacerles frente con mayor eficacia. De hecho, la gran mayoría de los responsables de la toma de decisiones en materia de seguridad comprenden la importancia de la inteligencia de amenazas y son capaces de tomar mejores decisiones cuando disponen de ella.

A pesar del reconocimiento casi unánime del valor que puede aportar la inteligencia de amenazas, los equipos de seguridad no la utilizan de forma fiable para combatirlas. Al menos la mitad de las decisiones de seguridad se toman sin disponer de inteligencia de amenazas sobre los posibles atacantes.

Los equipos de seguridad creen que están pasando por alto amenazas reales porque sus equipos tienen dificultades para hacer frente a los datos que deben procesar y, a veces, carecen de personal suficientemente capacitado y no siempre sabe qué hacer con la información de que dispone. Hasta que las organizaciones no empiecen a procesar mejor la inteligencia sobre los actores, permanecerán vulnerables al número cada vez mayor de ciberataques destructivos y perturbadores.

Metodología de la encuesta: Encargada por Mandiant, la encuesta "Perspectivas globales sobre inteligencia contra amenazas" fue realizada por Vanson Bourne, una empresa de investigación de mercado global, entre agosto y septiembre de 2022. La información se obtuvo de 1350 responsables de la toma de decisiones en materia de seguridad informática en EMEA, Norteamérica y JAPAC en organizaciones de más de 1000 empleados.

Más información en www.mandiant.com

Mandiant

11951 Freedom Dr, 6th Fl, Reston,
VA 20190 (703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

Acerca de Mandiant

Mandiant es un líder reconocido en defensa cibernética dinámica, inteligencia de amenazas y servicios de respuesta ante incidentes. Gracias a décadas de experiencia en primera línea, Mandiant ayuda a las organizaciones a confiar en su preparación para defenderse y responder a las ciberamenazas. Mandiant ahora forma parte de Google Cloud.

MANDIANT
NOW PART OF Google Cloud