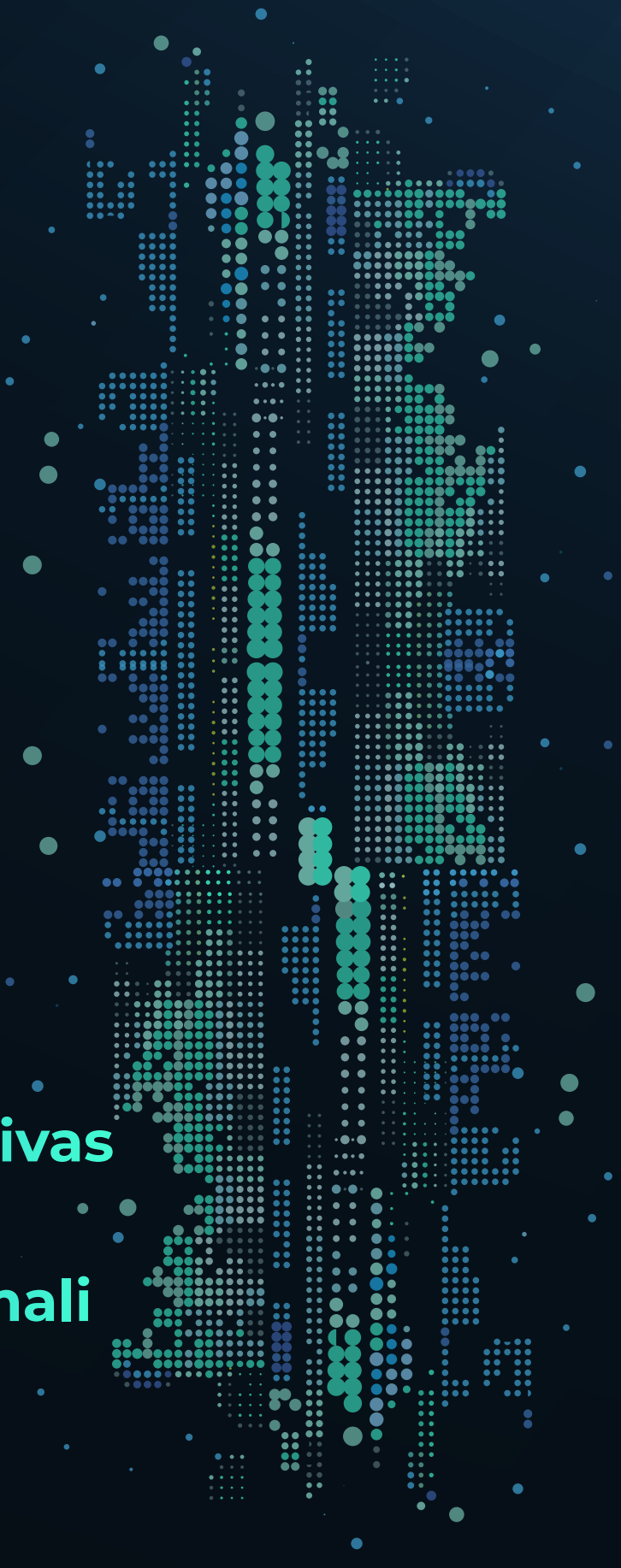
ANOMALI



2022

Informe de perspectivas sobre seguridad informática de Anomali

El estado de resiliencia informática empresarial

Índice

	PÁGINA
INTRODUCCIÓN	3
RESUMEN EJECUTIVO	4
PRINCIPALES DESAFÍOS PARA LOGRAR LA RESILIENCIA INFORMÁTICA	5
EL PANORAMA DE AMENAZAS MODERNO	10
EL IMPACTO DE LOS ATAQUES INFORMÁTICOS	16
RESPONDER A LOS ATAQUES INFORMÁTICOS	18
CONCLUSIÓN: EL NIVEL DE RESILIENCIA INFORMÁTICA QUE HAN LOGRADO LAS ORGANIZACIONES	21
CÓMO AYUDA ANOMALI	22

Introducción

Bienvenido al Informe de perspectivas sobre seguridad informática de Anomali del 2022. En esta investigación inaugural, identificamos y exploramos los desafíos que enfrentan las empresas para establecer y mantener posturas de seguridad informática resilientes, necesarias para proteger y responder a las amenazas informáticas avanzadas de hoy y mañana.

A fin de recopilar y desarrollar datos fundamentales para este informe, el equipo de investigación de amenazas de Anomali contrató a The Harris Poll para realizar encuestas a 800 encargados de la toma de decisiones de seguridad en 11 países de empresas con 5000 o más empleados. Debido a que el COVID-19 ha tenido un impacto tan profundo en los negocios y la seguridad informática, consultamos a estos encargados de tomar decisiones para comprender sus posturas y desafíos de seguridad informática que se remontan al 2019, a fin de proporcionar una mejor comprensión de cómo la pandemia ha afectado a los negocios. Los analistas de inteligencia contra amenazas del equipo de investigación de amenazas de Anomali reforzaron los hallazgos con el análisis de tendencias de amenazas, lo que les dio a los lectores información útil que pueden utilizar para mejorar su capacidad de detectar y responder a las filtraciones y a los atacantes.

Entre las principales conclusiones se encuentra que, incluso con importantes inversiones en seguridad informática, **muchas organizaciones enfrentan obstáculos para alcanzar el nivel de resiliencia informática necesaria para protegerse contra los atacantes, detectarlos y responder a ellos**. Es probable que este hallazgo no sea una sorpresa para la mayoría de los lectores, dado el aumento de las filtraciones y los ataques informáticos que el mundo ha experimentado en los últimos años.

DEFINICIÓN DE RESILIENCIA INFORMÁTICA

La capacidad de proteger de forma proactiva y reactiva a su organización contra amenazas y atacantes, adaptarse a circunstancias cambiantes durante un ataque y recuperarse después de que se haya producido un ataque informático.

Resumen ejecutivo

Nuestra investigación reveló muchas razones por las que es difícil lograr la resiliencia informática. En la parte superior de la lista, se encuentran las organizaciones que luchan con las brechas de desempeño y capacidad en el nivel de detección, respuesta y recuperación necesarios para abordar ataques y filtraciones inmediatos y futuros.

Esta investigación reveló que los ataques informáticos están aumentando (en hasta un **15 %** en comparación con los niveles del 2019 previos a la pandemia). Por lo tanto, no nos sorprendió que alrededor de 3 de 4 organizaciones (un **74 %**) hayan aumentado sus presupuestos de seguridad informática y estén reevaluando sus estrategias de seguridad informática (un **78 %**).

Incluso con el aumento de la inversión, la mayoría de las empresas (un **87 %**) han sido víctimas de ataques informáticos exitosos en los últimos tres años, lo que ha provocado daños, interrupciones o una filtración a sus empresas. A pesar de sus esfuerzos, alrededor de dos tercios (un **67 %**) informan que los ataques informáticos más exitosos han afectado a su organización desde el inicio de la pandemia. Solo en el 2020, uno de cada siete ataques informáticos (un **14 %**) en promedio fue exitoso, lo que dio causó una filtración, un daño o una interrupción operativa. Los encargados de la toma de decisiones de seguridad esperan que este número aumente, ya que sus superficies de ataque se expanden junto con la escala sin precedentes de proyectos de transformación digital. Incluso con este panorama de amenazas cada vez más peligroso, solo el 44 % ha identificado las prácticas recomendadas de respuesta ante incidentes que pueden emplear cuando son atacados.

Los incidentes informáticos están afectando a casi todas las organizaciones, con pérdidas por ataques informáticos dirigidos, campañas de malware, fraude electrónico, amenazas internas y filtraciones de datos asociadas que se acercan a cientos de miles de dólares por organización. Casi 3 de cada 10 (un **28 %**) empresas de todo el mundo informaron pérdidas de $500 000 dólares o más en el 2020, casi dos veces más (un **193 %**) en comparación con el 2019, y casi la mitad (un **47 %**) informó pérdidas de $100 000 dólares o más. Además de las pérdidas importantes, los ataques en sí están aumentando a una velocidad impresionante.

Además de factores como el rápido ritmo de la transformación digital y el aumento de los ataques, muchos encargados de la toma de decisiones de seguridad empresarial citaron la falta de soluciones de seguridad informática integradas como barrera para detectar ataques informáticos y filtraciones de datos, responder a ellos y recuperarse luego de sufrir uno.

Muchos encuestados afirman que sus organizaciones han comenzado a utilizar o están planificando invertir en innovaciones tecnológicas recientes asociadas con la detección y respuesta extendidas (XDR) y la inteligencia contra amenazas avanzada para contrarrestar los obstáculos.

Lo que está claro es que existe un apetito por soluciones de seguridad informática que estén bien respaldadas (un **48 %**), sean fáciles de usar (un **46 %**) y que se integren mejor en marcos de trabajo y arquitecturas existentes (un **44 %**), con más de 4 de cada 10 encargados de la toma de decisiones que consideran que estos atributos son esenciales.

Un 87 %

de los encargados de la toma de decisiones de seguridad empresarial afirman que su organización ha experimentado un ataque informático exitoso en los últimos tres años, lo que ha inducido daños, interrupciones o una filtración a su empresa.

Hallazgo 1

Las organizaciones solo son moderadamente eficaces en la detección, respuesta y recuperación de amenazas informáticas

El 42 % de los encargados de la toma de decisiones de seguridad cree que no ha logrado el nivel de resistencia necesario para defender a sus organizaciones de las filtraciones y los ataques. Menos de 6 de cada 10 (un 58 %) encargados de la toma de decisiones están totalmente de acuerdo con que sus organizaciones tienen resistencia informática; sin embargo, este hallazgo contrasta con el hecho de que el 87 % de las organizaciones ha sido filtrado en los últimos tres años.

Hallazgo 2

Solo menos de la mitad de los encargados de la toma de decisiones de seguridad está totalmente de acuerdo en que sus equipos de seguridad informática pueden priorizar rápidamente las amenazas según las tendencias, la gravedad y el posible impacto

Un tercio admite que sus equipos tienen dificultades para actualizar los controles de seguridad a fin de abordar nuevos ataques (un 31 %). Menos de la mitad (un 49 %) de los encargados de la toma de decisiones de seguridad empresarial está totalmente de acuerdo en que sus equipos de seguridad informática pueden priorizar rápidamente las amenazas en función de las tendencias, la gravedad y el posible impacto. Incluso menos (un 46 %) están muy seguros de que sus tecnologías de protección informática pueden evolucionar para detectar nuevas amenazas identificadas a nivel mundial. Un tercio (un 32 %) admite que sus equipos tienen dificultades para mantenerse al día con el cambiante panorama de amenazas de seguridad informática. Las organizaciones más pequeñas están aún más en riesgo. Aquellos con menos de 10 000 empleados son menos propensos a estar armados con un conjunto de prácticas recomendadas al que pueden referirse para responder a los ataques informáticos (un 40 %).

Figura 1.0

RESILIENCIA INFORMÁTICA DE LAS ORGANIZACIONES (% TOTALMENTE DE ACUERDO)

49 %
TOTALMENTE DE ACUERDO

Mi equipo puede priorizar rápidamente las amenazas en función de las tendencias, la gravedad y el posible impacto en nuestra organización

46 %
TOTALMENTE DE ACUERDO

Mis tecnologías de seguridad informática pueden evolucionar para detectar nuevas amenazas identificadas a nivel mundial

32 %
TOTALMENTE DE ACUERDO

Mi equipo lucha por mantenerse al día con el cambiante panorama de amenazas de seguridad informática

PRINCIPALES DESAFÍOS PARA LOGRAR LA RESILIENCIA INFORMÁTICA

Hallazgo 3

Las organizaciones no alcanzan los objetivos de detección y respuesta de amenazas informáticas

El tiempo de espera es el período entre el momento en que un adversario obtiene acceso a una red, se detecta y, luego, se detiene. El tiempo de espera es directamente proporcional a la cantidad de daños que puede causar un atacante. Mientras más tiempo estén dentro de la red, más información obtienen, más datos e IP roban, y se pueden mover a más sistemas e infectarlos con secuestro de datos y otras amenazas. Se estima que los atacantes pueden evadir la detección, en promedio, por hasta 140 días. Sin embargo, esta métrica es específica para la primera vez que se detecta una amenaza y, luego, se divulga.

Otro aspecto del tiempo de espera, que es igualmente precario, es la cantidad de tiempo que se tarda en determinar si una amenaza recién divulgada también está presente en su entorno. Como parte de la encuesta, preguntamos a las organizaciones cuánto tiempo tardaban en detectar y responder a los ataques que se habían divulgado anteriormente. Los resultados fueron alarmantes, ya que, en promedio, todos los encargados de la toma de decisiones de seguridad admitieron que, en general, no cumplen con sus objetivos de detección y respuesta, y que también se atrasan cuando se trata de tipos de amenazas específicos.

Figura 1.1

TIEMPO MEDIO PARA DETECTAR Y RESPONDER FRENTE AL OBJETIVO

(en días)

	Filtración de datos		Vulneración de red		Ataque informático	
	Tiempo medio	Objetivo prom.	Tiempo medio	Objetivo prom.	Tiempo medio	Objetivo prom.
DETECTAR	3,1	2,1	2,8	2,1	2,7	2,5
RESPONDER	2,5	2,2	2,5	2,1	2,4	2,1

Los equipos de operaciones de seguridad eficaces prestarán mucha atención a sus métricas de MTTR y MTTD cuando se trate de resolver incidentes. Es crucial ser fanático en la reducción de estas métricas dentro de las organizaciones, ya que los tiempos de espera más cortos reducen el riesgo general de daño y alteración. La reducción de los tiempos de espera (MTTD y MTTR) comienza con la comprensión de los ataques y su impacto. Las organizaciones también deben desglosar sistemas aislados y colaborar de manera interfuncional para garantizar procesos eficaces de detección y respuesta.

MTTD

El tiempo promedio para detectar, o MTTD, del inglés Mean Time to Detect, refleja la cantidad de tiempo que le toma a su equipo descubrir un potencial.

MTTR

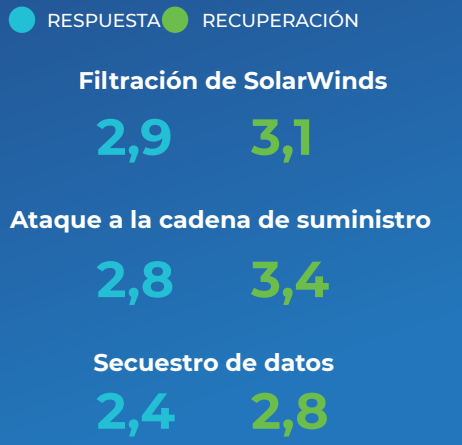
El tiempo promedio para responder, o MTTR, del inglés Mean Time to Respond, es el tiempo que se tarda en controlar, reparar o erradicar una amenaza después de que se haya descubierto.

Figura 1.2

DÍAS PROMEDIO PARA DETECTAR ATAQUES INFORMÁTICOS CONOCIDOS

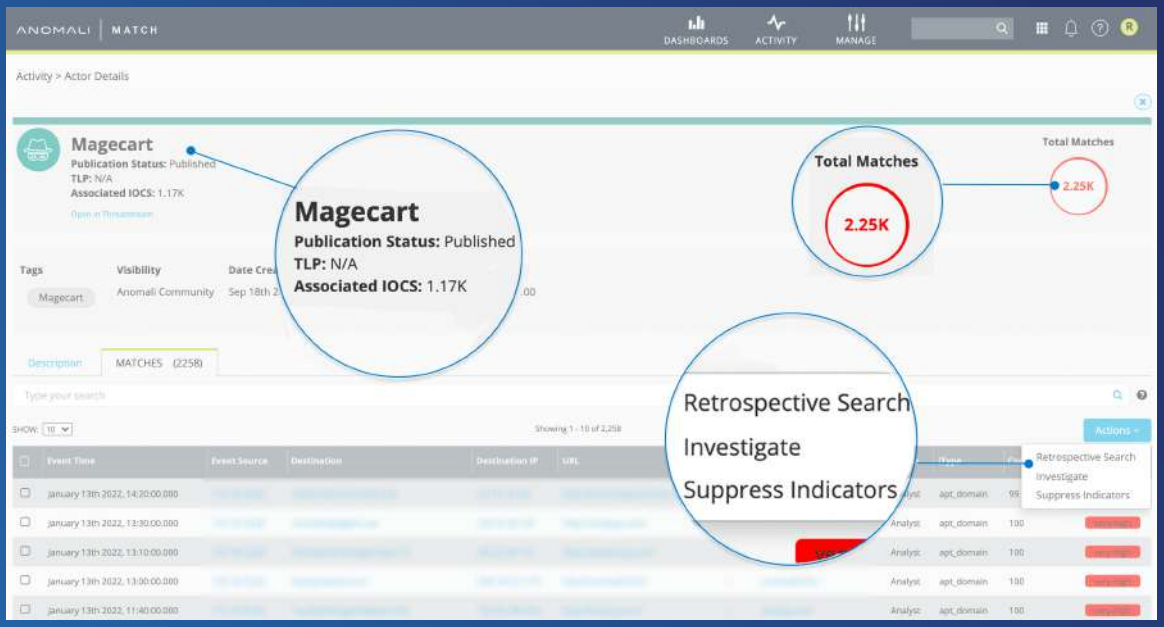
Figura 1.3

DÍAS PROMEDIO PARA RESPONDER A LOS ATAQUES INFORMÁTICOS Y RECUPERARSE DE ELLOS



Anatomía de la detección de amenazas

MAGECART: un grupo criminal informático malicioso dirigido a sitios web de comercio electrónico a fin de robar información de tarjetas de pago para venderla en foros criminales.



Existen muchos tipos de amenazas diferentes y, por lo general, la detección de estos es un solo aspecto de la mitigación y la respuesta. Recopilar más información es fundamental para tomar decisiones basadas en datos sobre las amenazas.

Los profesionales de la seguridad informática ahora utilizan análisis de datos a gran escala (grandes cantidades de información recopilada de varias fuentes) para identificar las amenazas antes de que ocurran. Con las tecnologías adecuadas, estos datos se pueden analizar para obtener información sobre el comportamiento humano, predecir tendencias futuras o prevenir filtraciones de seguridad.

El ejemplo anterior muestra cómo las herramientas que integran grandes cantidades de datos a gran escala, incluidos los indicadores de compromiso (IOC, del inglés Indicators of Compromise), los comportamientos observados, el conocimiento de adversarios y los modelos de amenazas pueden ser utilizados por analistas para saber inmediatamente si hay amenazas como Magecart presentes en sus entornos y durante cuánto tiempo han estado presentes. Cuando las organizaciones tienen acceso a dicha inteligencia inmediata, pueden responder de manera rápida y decisiva, lo que es fundamental para establecer una postura de seguridad proactiva y resistente.

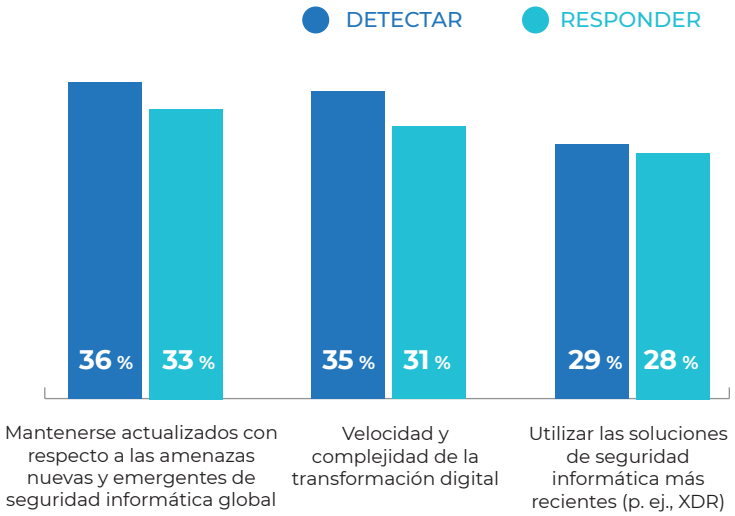
Hallazgo 4

Mantenerse actualizados con respecto a las amenazas nuevas y emergentes de seguridad informática global, y la velocidad y complejidad de la transformación digital son los principales desafíos

Las organizaciones enfrentan muchos desafíos cuando se trata de la detección. Entre los principales se encuentra mantenerse actualizado con respecto a las amenazas nuevas y emergentes de seguridad informática global (un 36 %), la velocidad y la complejidad de la transformación digital (un 35 %) y la adopción de avances en seguridad informática, como XDR (un 29 %). Se observaron desafíos casi idénticos para responder a las amenazas y recuperarse tras sufrir una.

Figura 1.4

DESAFÍOS RELACIONADOS CON LOS ATAQUES INFORMÁTICOS, LA VULNERACIÓN DE RED Y LAS FILTRACIONES DE DATOS



Hallazgo 5

La falta de capacidad para compartir la inteligencia contra amenazas entre los recursos internos dificulta los esfuerzos de mitigación

Mantenerse actualizados con respecto a las amenazas nuevas y emergentes de seguridad informática global, y la velocidad y complejidad de la transformación digital se encuentran entre los desafíos mencionados por los encargados de la toma de decisiones de seguridad empresarial. Pero más que cualquier otra cosa, es posible que la falta de soluciones integradas y la capacidad de compartir inteligencia contra amenazas de manera interfuncional sea lo que más obstaculiza los esfuerzos para detectar los ataques informáticos, responder a ellos y recuperarse luego de sufrirlos. Un poco más de la mitad (un 53 %) de los responsables de la toma de decisiones sienten que sus organizaciones son muy eficaces para compartir información de inteligencia contra amenazas a través de recursos internos.

PRINCIPALES DESAFÍOS PARA LOGRAR LA RESILIENCIA INFORMÁTICA

La inteligencia contra amenazas es compleja y las variables son numerosas, y, a menudo, se describen de manera diferente. Para que los esfuerzos de compartir información sean exitosos, han surgido estándares como MITRE, NIST y STIXX, entre otros, que han mejorado los procesos.

Para comprender cómo compartir, las organizaciones también deben saber lo que están intentando distribuir. Para reducir aún más la complejidad, la inteligencia contra amenazas puede dividirse en dos categorías: IOC y actores de amenazas, lo que puede ayudar a los profesionales de seguridad y riesgo a comprender cómo utilizarla.

Figura 1.5

LA EFICACIA DE COMPARTIR INTELIGENCIA CONTRA AMENAZAS A TRAVÉS DE RECURSOS INTERNOS

IOC

- Las fuentes de OSINT (inteligencia de código abierto) pueden ser fáciles de conseguir si los procesos están implementados para digerir y etiquetar los datos según corresponda.
- Las plataformas de inteligencia contra amenazas (TIP, del inglés Threat Intelligence Platforms) pueden hacer gran parte de este trabajo por usted mediante la unión de las fuentes de inteligencia contra amenazas de sus fuentes de inteligencia (tanto libres como comerciales).
- Bases de datos y repositorios de IOC, como AlienVault (OTX), Hybrid Analysis, MalwareBazaar, PolySwarm, VirusTotal, VirusBay, VirSCAN, URLhaus, y URLScan, entre otros, son excelentes herramientas para recopilar contexto y tomar decisiones basadas en datos.
- Zonas de prueba, como AnyRun, Hatching, Hybrid Analysis, Inquest, Joe y Valkyrie Comodo, entre otros, son útiles para ver las tendencias generales y los TTP a fin de crear firmas para tácticas comunes de malware.
- Los repositorios de idiomas de detección de OSINT para Yara, SIGMA, Snort y otros son una gran manera de cubrir comportamientos maliciosos comunes.

AGENTES DE AMENAZAS

- Las fuentes de OSINT, como ThaiCERT, MITRE Groups, Malpedia y Maltego, son excelentes fuentes de datos de amenazas.
- Las TIP deben tener muchos actores de amenaza documentados y asociaciones de IOC en tiempo real para mantener actualizados los grupos prolíficos.
- Saber qué familias de malware son ejecutadas por diferentes grupos, que se venden “como un servicio”, el commodity malware modificado, las herramientas legítimas o el malware personalizado, permitirá tener una postura proactiva en la creación de mitigaciones para estas amenazas.

La categorización de tipos de inteligencia ayuda a que sea más factible detectar y responder a los atacantes y las filtraciones. Las organizaciones están recurriendo a innovaciones que ayudan a automatizar y poner en funcionamiento la inteligencia contra amenazas en todas las infraestructuras de seguridad para optimizar aún más su valor. Los informes recientes emitidos por los principales analistas de la industria revelan que la demanda de soluciones en el mercado de inteligencia contra amenazas, que incluye plataformas de gestión de amenazas, aumentará hasta un 16 % anualmente en los próximos tres años.

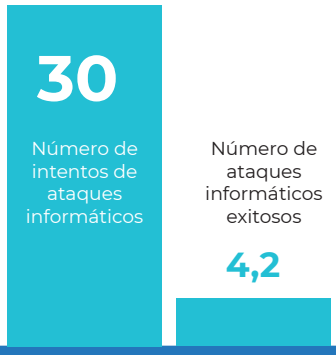
Hallazgo 6

Los incidentes informáticos son generalizados y han aumentado desde el inicio de la pandemia

La mayoría de los encargados de la toma de decisiones de seguridad empresarial coincide en que sus organizaciones han experimentado más intentos de ataques informáticos (un 83 %) y han sufrido más intentos de fraude electrónico (un 86 %) desde el inicio de la pandemia. En particular, estas organizaciones también están experimentando un aumento en el fraude electrónico por correo electrónico con temas relacionados con la pandemia (un 87 %). En el 2020, las empresas con 5000 o más empleados informaron 30 ataques informáticos en promedio, frente al promedio de 26 solo un año antes. Uno de cada siete de estos ataques informáticos (un 14 %) tuvo éxito, lo que dio como resultado daños, interrupciones o una filtración en las redes, la infraestructura y los dispositivos.

Figura 2.2

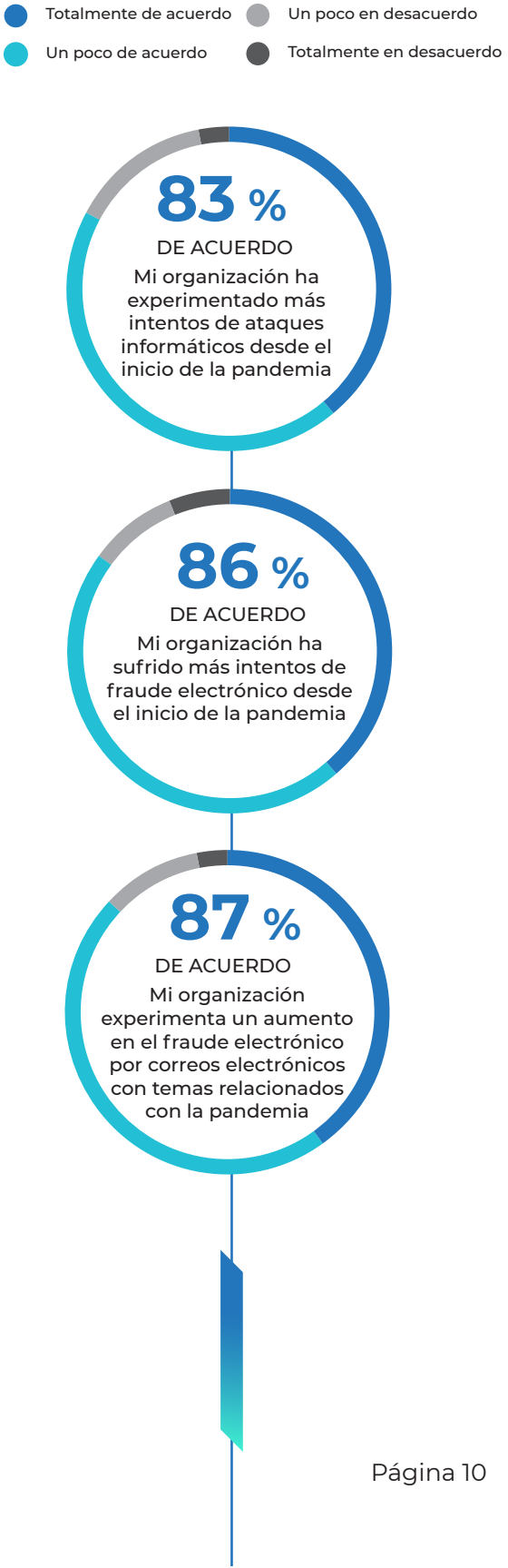
CANTIDAD MEDIA DE ATAQUES INFORMÁTICOS A LA ORGANIZACIÓN



Las organizaciones con 10 000 o más empleados han sufrido más intentos de ataques informáticos tanto en el 2019 como en el 2020, en comparación con las organizaciones de 5000 a 9999 empleados (en el 2019, 29,1 frente a 23,3; en el 2020, 32,4 frente a 27,8)

Figura 2.1

AUMENTO EN TIPOS DE ATAQUES INFORMÁTICOS DESDE LA PANDEMIA



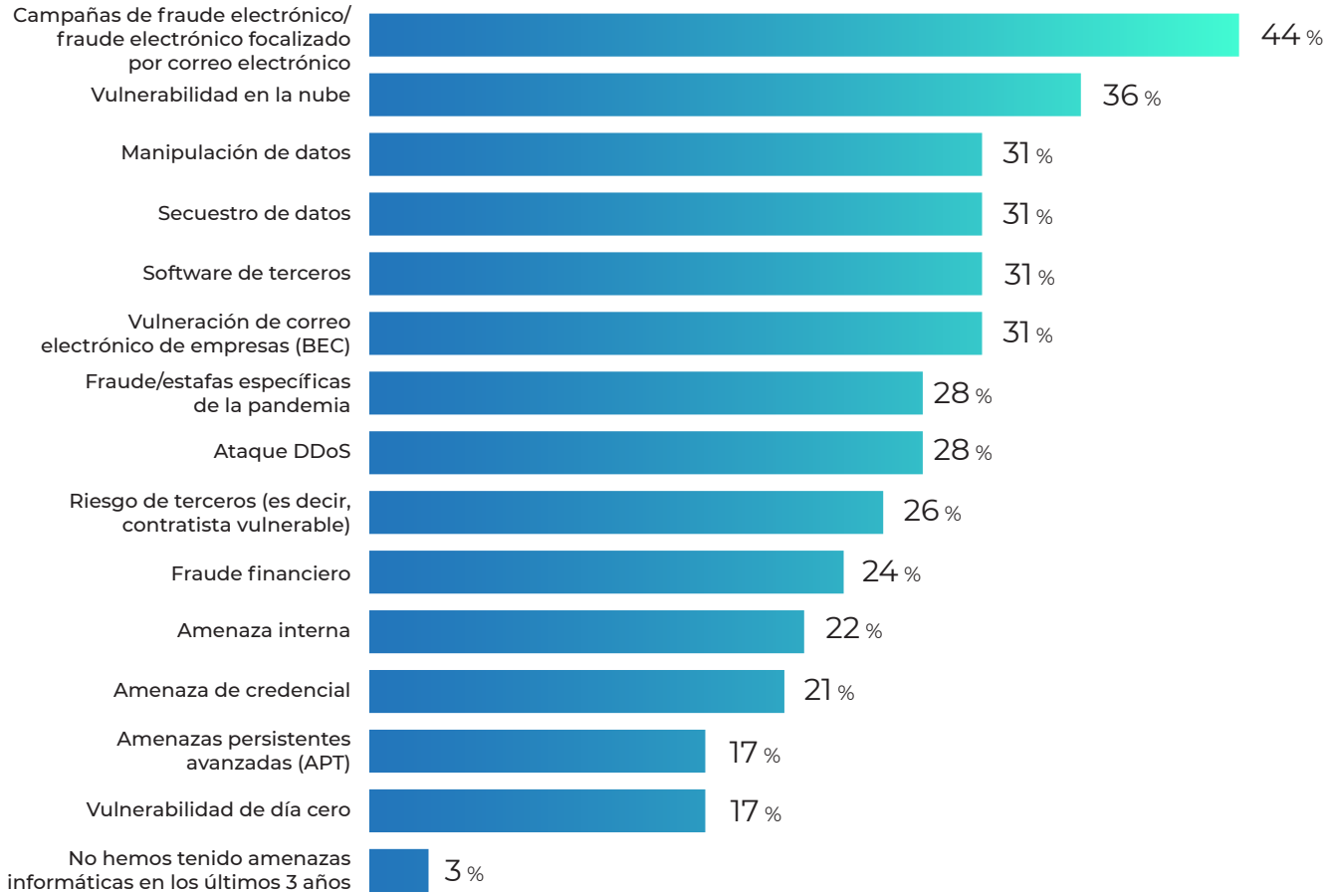
Hallazgo 7

Los intentos de fraude electrónico por correo electrónico son la amenaza que se encuentra con mayor frecuencia

El 44 % de todas las organizaciones sufrió ataques de fraude electrónico en los últimos tres años, el ataque experimentado más común. Los agentes de amenazas de todos los niveles de sofisticación utilizan el fraude electrónico debido a las herramientas disponibles de materias primas y el creciente conjunto de objetivos. Los kits de materias primas de fraudes electrónicos permiten a los agentes de amenazas de baja sofisticación realizar campañas potencialmente dañinas que distribuyan commodity malware. Los documentos maliciosos (maldocs) en sí mismos también son comercializados a través de herramientas como **EtterSilent**. Los agentes y grupos de amenazas también comprometen las cuentas de correo electrónico objetivo para propagar más actividad maliciosa. A menudo incluyen documentos legítimos para que su actividad parezca más auténtica. Nuestra investigación ha observado el uso de documentos legítimos en campañas de **Gamaredon** (Primitive Bear) y **Mustang Panda**, con la probabilidad de que el primero utilice documentos privados antes de publicarlos.

Figura 2.3

AMENAZAS INFORMÁTICAS EXPERIMENTADAS EN LOS ÚLTIMOS 3 AÑOS



Hallazgo 8

Se percibe que las organizaciones criminales informáticas son la mayor amenaza para la seguridad informática (un 44 %), seguida de hackers individuales (un 21 %)

En promedio, la empresa tarda de 3 a 4 días en detectar los ataques de estas entidades después de la divulgación

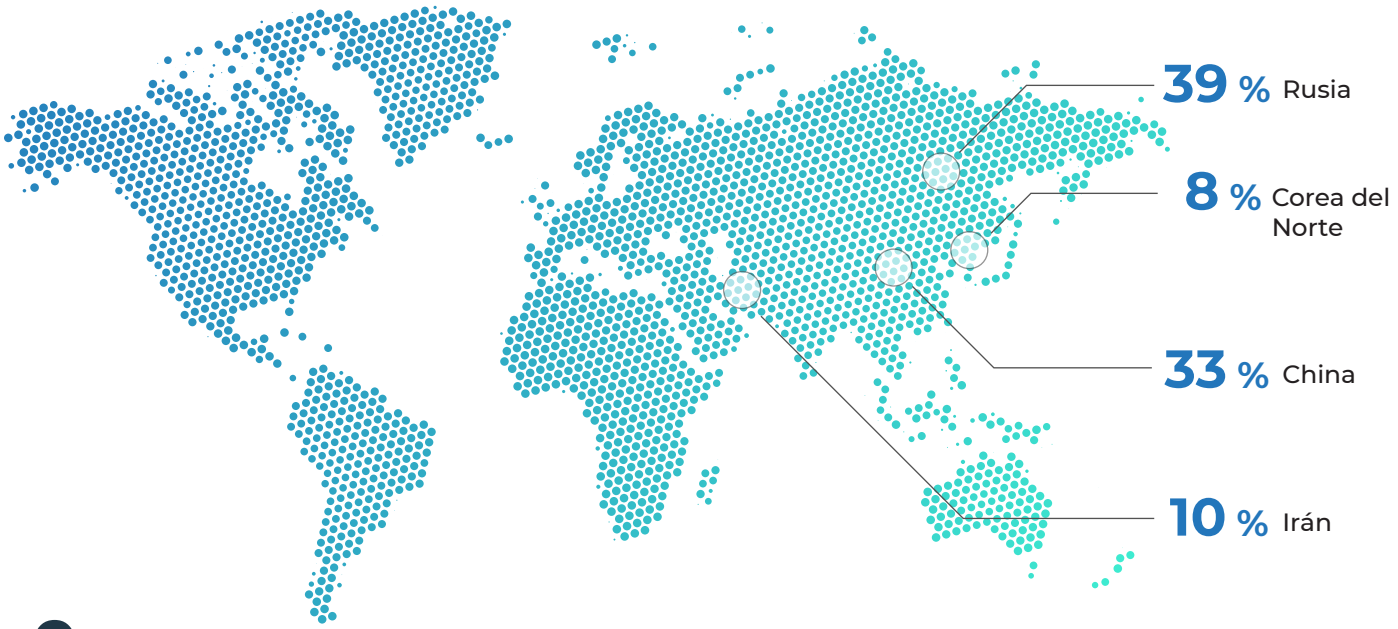
El 44 % de los encargados de la toma de decisiones de seguridad empresarial afirma que los grupos cibercriminales son la mayor amenaza para sus organizaciones. Esto no es sorprendente, ya que los ataques y las filtraciones más perjudiciales que se producen hoy son el resultado de este tipo de actor de amenaza. El 15 % de los encargados de la toma de decisiones de seguridad empresarial cree que los actores respaldados por estados naciones representan la amenaza más significativa a la seguridad informática para sus organizaciones, y Rusia (un 39 %) y China (un 33 %) encabezan la lista. Existe menos preocupación por las amenazas que surgen de Irán (un 10 %) o Corea del Norte (un 8 %). Los encargados de la toma de decisiones de seguridad en organizaciones con menos de 10 000 empleados son menos propensos a comprender completamente los motivos de estos actores en comparación con organizaciones más grandes con 10 000 o más empleados.

Figura 2.4

MAYOR AMENAZA PARA LA ORGANIZACIÓN

Figura 2.5

PAÍS QUE REPRESENTA LA MAYOR AMENAZA DE SEGURIDAD INFORMÁTICA



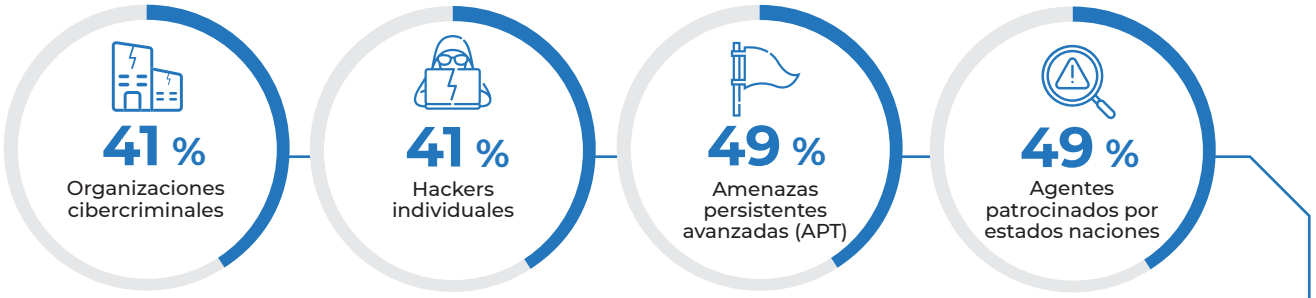
Hallazgo 9

Casi la mitad de los encargados de la toma de decisiones de seguridad empresarial no entienden muy bien los motivos de los adversarios

El ruido persistente de los agentes de amenazas con sofisticación de nivel inferior a medio puede hacer que los indicadores de compromiso (IOC) parezcan como una gota en el océano. En tanto todo esto ocurre, grupos más sofisticados pueden ocultarse en el ruido mientras crean herramientas personalizadas y malware, o abusan de software legítimo, para realizar ataques dirigidos. Por lo tanto, es fundamental comprender los motivos de los actores de amenaza para saber cómo funcionan y cuáles pueden atacar a su organización.

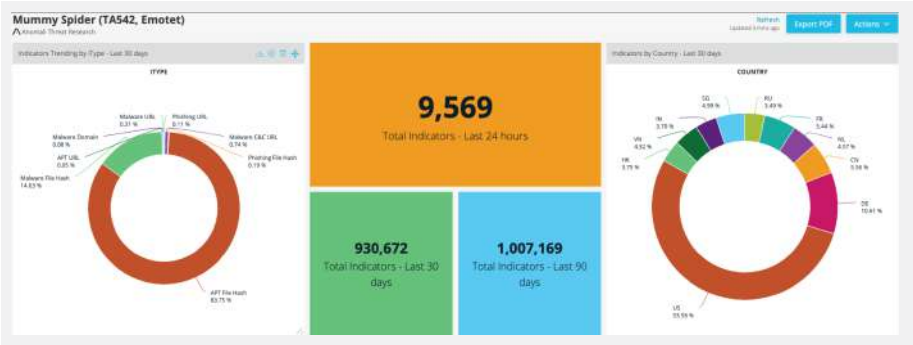
Figura 2.6

PORCENTAJE DE ENCARGADOS DE LA TOMA DE DECISIONES DE SEGURIDAD QUE NO ENTIENDEN COMPLETAMENTE LOS MOTIVOS, LAS TÁCTICAS, LAS TÉCNICAS Y LOS PROCEDIMIENTOS DE LOS ADVERSARIOS



Aquellos en las empresas de servicios financieros y profesionales son los más propensos a creer que comprenden muy bien las motivaciones de los criminales informáticos (un 64 % y un 65 %, respectivamente), mientras que aquellos en las organizaciones de atención médica son los menos propensos a comprender esto (un 45 %).

AGENTES DE AMENAZAS: SER MÁS PRECISO



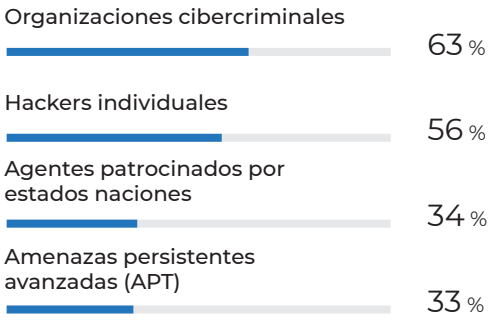
El equipo de investigación de amenazas de Anomali desarrolló este panel para mostrar cómo administrar la inteligencia contra amenazas a fin de proyectar una red inicial amplia y sintetizar los datos. Con este nivel de precisión, es más fácil comprender los motivos y objetivos de los actores de amenazas. En este caso, aplicamos el panel a **Mummy Spider**, un grupo cibercriminal vinculado al desarrollo del malware comúnmente conocido como Emotet o Geodo.

Hallazgo 10

Casi 9 de cada 10 (un 87 %) organizaciones han sido víctimas de algún tipo de ataque informático en los últimos tres años

Entre este grupo, más de la mitad fueron afectados por organizaciones cibercriminales y hackers individuales. Un tercio eran los objetivos de los actores y los ataques respaldados por estados naciones contra amenazas persistentes avanzadas (APT, del inglés Advanced Persistent Threats).

Figura 2.7
ATAQUE INFORMÁTICO LANZADO CON ÉXITO CONTRA LA ORGANIZACIÓN



Hallazgo 11

Alrededor de la mitad de todas las organizaciones (un 52 %) han sido víctimas de ataques de secuestro de datos en los últimos tres años

Aproximadamente el 40 % de las personas que fueron atacadas pagó un rescate (un 39 %), y una de cada cinco (un 19 %) empresas gastó $500 000 dólares o más. A pesar de ser una de las amenazas más comunes y conocidas, el secuestro de datos sigue causando estragos entre todas las organizaciones. Para protegerse de este tipo de ataque, las organizaciones deben saber en qué áreas se encuentran sus vulnerabilidades, segmentar correctamente las redes, restringir y supervisar los permisos de usuario, mantener copias de seguridad y adquirir la capacidad de detectar y responder al secuestro de datos antes de que ingrese a las redes.

Un 39 %

pagó el rescate por un ataque de secuestro de datos en los últimos 3 años

Figura 2.8
MONTO PAGADO EN RESCATES
(EQUIVALENTE EN MONEDA ESTADOUNIDENSE)

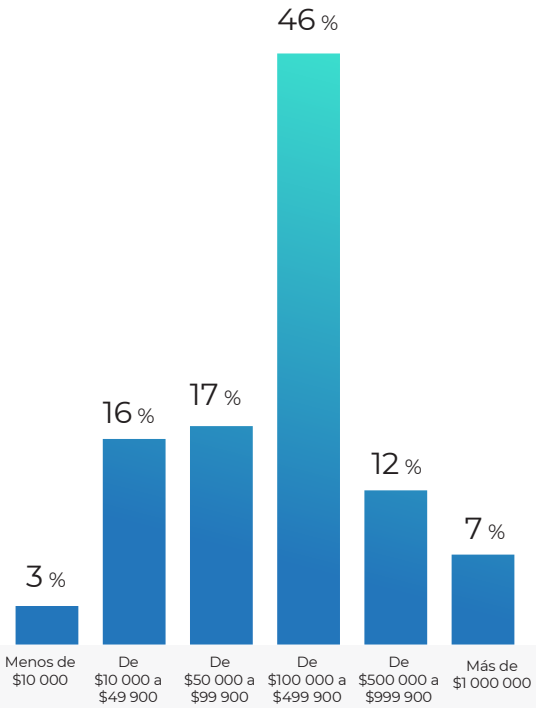
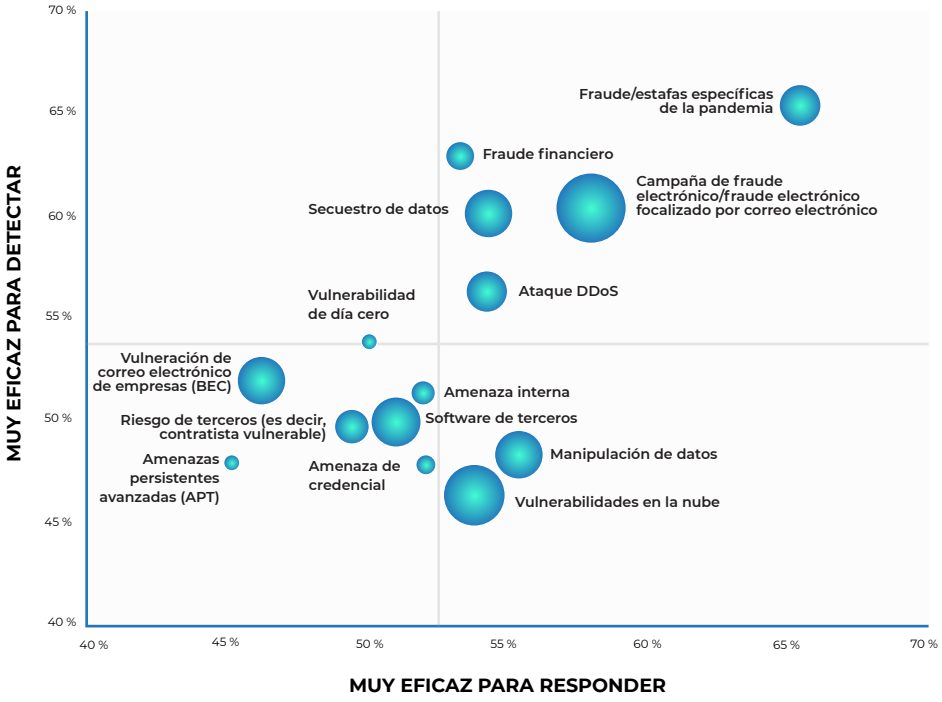


Figura 2.9
POSIBLES ÁREAS DE VULNERABILIDAD



NOTA: el tamaño de la burbuja representa la frecuencia de la amenaza que ocurrió en los últimos 3 años

El 17 % de las organizaciones ha experimentado un ataque de APT en los últimos tres años, y aproximadamente la misma proporción (un 18 %) considera que las APT son la mayor amenaza para la seguridad informática de su organización. Los encargados de la toma de decisiones de seguridad empresarial sienten que están menos equipados para lidiar con estas amenazas que para lidiar con otros tipos de ataques informáticos y, comparativamente, pocos dicen que sus organizaciones son muy eficaces para detectar (un 45 %) y responder (un 48 %) a las APT.

Cuando comenzó la pandemia, los analistas de inteligencia contra amenazas de Anomali detectaron **6200 indicadores de compromiso (IOC) y, al menos, 15 campañas distintas**. Estos se asociaron con 11 agentes de amenazas o grupos que distribuían 39 familias diferentes de malware mediante 80 técnicas variadas de MITRE ATT&CK. Anomali evaluó de manera temprana que la amenaza presentada por las campañas de fraude electrónico relacionadas con el COVID-19 contra empresas públicas y privadas seguiría aumentando, y los Hallazgos 6 y 7 demuestran que dichos ataques se intensifican.

Hallazgo 12

La pandemia ha obligado a las organizaciones a reevaluar las estrategias de seguridad informática

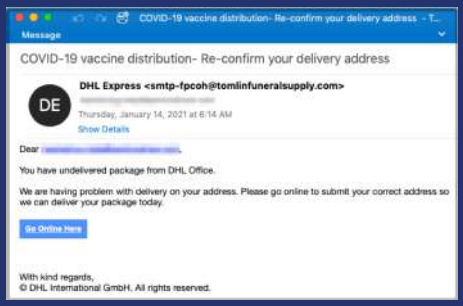
Más de 3 de cada 4 (un 78 %) encargados de la toma de decisiones de seguridad empresarial afirman que la pandemia los ha llevado a reconsiderar sus estrategias de seguridad informática. Desde nuestro punto de vista, esto sucede por varias razones. Los proyectos de transformación digital, el crecimiento de las fuerzas de trabajo remotas y la correspondiente expansión de la infraestructura en la nube han aumentado la superficie de ataque más rápido de lo que estaba creciendo antes de la pandemia. Estos factores han obligado a las organizaciones a aumentar la visibilidad de sus sistemas, lo que ayuda a explicar las inversiones planificadas y el uso existente en cuestiones como XDR, MITRE ATT&CK e inteligencia contra amenazas (Hallazgo 13). Además, el COVID-19 ha dado a los agentes de amenazas un tema reconocible para ejecutar campañas de fraude electrónico y otras actividades maliciosas, ya que la pandemia ha demostrado ser una buena arma para infundir confusión, miedo, curiosidad y otras emociones que tientan a las personas a hacer clic en enlaces maliciosos. Con las nuevas variantes del COVID-19 que aparecen constantemente, las organizaciones deben aumentar su capacidad de adaptarse, especialmente cuando se trata de ataques comunes, como campañas de fraude electrónico de correos electrónicos.

Figura 3.1

IMPACTO DE LA PANDEMIA EN LA ESTRATEGIA DE SEGURIDAD INFORMÁTICA

LA PANDEMIA LE DA UNA VENTAJA A LOS ATACANTES

Desde el comienzo del COVID-19, la investigación de amenazas de Anomali ha observado y detectado muchas campañas maliciosas que aprovechan la pandemia como un gran anzuelo. La imagen de la derecha muestra un ejemplo de una aplicación falsa de dispositivo móvil contra el COVID-19 que circuló a partir de junio del 2020. Para ayudar a la comunidad de seguridad y a los consumidores a permanecer protegidos contra estos intentos fraudulentos de propagar malware, los analistas de inteligencia contra amenazas de Anomali publicaron un blog detallado sobre el tema: **El equipo de investigación de amenazas de Anomali identifica aplicaciones falsas de rastreo de contactos del COVID-19 que se utilizan para descargar malware que monitorea dispositivos y roba datos personales**



Además de las aplicaciones falsas de rastreo de contactos del COVID-19, los analistas de inteligencia contra amenazas de Anomali también han detectado campañas de fraude electrónico por correo electrónico que aprovechan el tema de la pandemia. El siguiente correo electrónico se detectó en febrero del 2021.

Fuente: Los actores de amenazas aprovechan las noticias sobre vacunas contra el COVID-19 para ejecutar campañas, con abuso de AWS para alojar archivos PDF maliciosos, a través del equipo de investigación de amenazas de Anomali

Hallazgo 13

El impacto financiero de las amenazas informáticas se puede medir tanto en términos de aumento de presupuestos en seguridad informática como en pérdidas directas de incidentes cibernéticos y ataques de secuestro de datos

Las organizaciones deben mantener una sólida postura defensiva para protegerse contra una amplia gama de amenazas informáticas, desde campañas de fraude electrónico por correo electrónico, vulnerabilidades en la nube, secuestro de datos y APT. Las empresas ahora están dedicando casi el 40 % de sus presupuestos de TI a la seguridad informática (un 38 %) y tres de cada cuatro (un 74 %) encargados de la toma de decisiones de seguridad empresarial afirman que los presupuestos han aumentado en el último año.

Sin embargo, a pesar de este nivel de gasto, las pérdidas directas de los incidentes informáticos siguen aumentando. En el 2019, solo alrededor de un tercio de las empresas a nivel mundial (un 36 %) informaron pérdidas de $100 000 o más (equivalente en moneda de EE. UU.). En el 2020, ese nivel aumentó a casi la mitad (un 47 %). Pérdidas reportadas de $500 000 o más y de $1 000 000 o más se duplicaron en este mismo período de un año (pérdidas de $500 000 o más: un 15 % en el 2019 frente a un 28 % en el 2020; pérdidas de $1 000 000 o más: un 5 % en el 2019 frente a un 11 % en el 2020). Las cifras del 2021 no estaban disponibles en el momento en que se realizó la encuesta.

Figura 3.2

PRESUPUESTO DE SEGURIDAD INFORMÁTICA

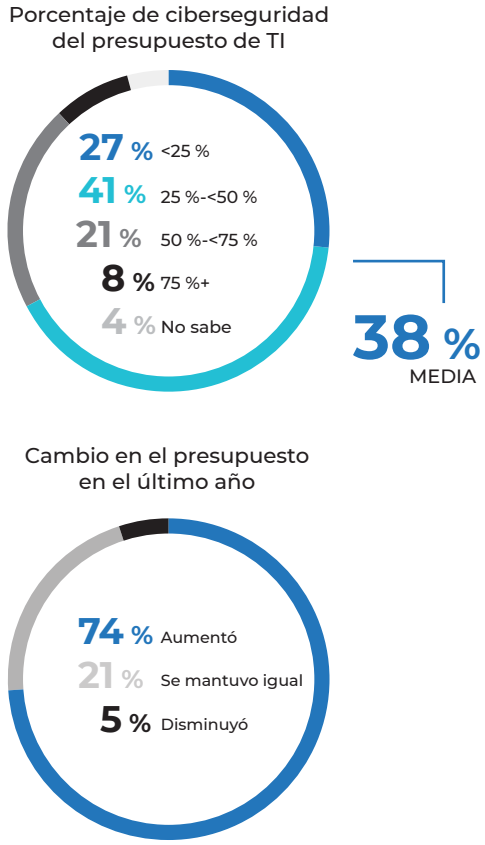
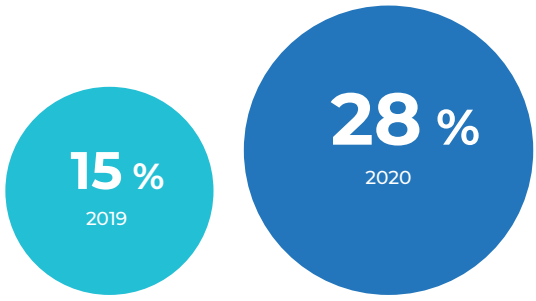


Figura 3.3

PÉRDIDAS DE LAS ORGANIZACIONES SUPERIORES A $500 000 POR ATAQUES INFORMÁTICOS
(EQUIVALENTE EN MONEDA ESTADOUNIDENSE)



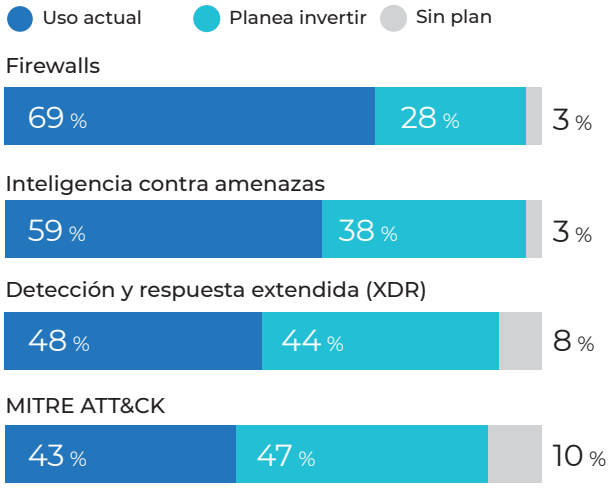
Los ataques de secuestro de datos también se han vuelto bastante costosos. Entre las aproximadamente dos de cada cinco (un 39 %) organizaciones fueron víctimas de un ataque de secuestro de datos y decidieron pagar un rescate, casi dos tercios (un 65 %) pagaron un equivalente a $100 000 dólares de EE. UU. o más.

Hallazgo 14

Las organizaciones siguen utilizando tecnología heredada, pero se inclinan hacia nuevas innovaciones

Un total de 7 de 10 (un 69 %) organizaciones aún utilizan firewalls para detectar amenazas en la red. Sin embargo, el 59 % utiliza inteligencia contra amenazas (el 38 % planea invertir en ella), el 48 % utiliza XDR (el 44 % planea invertir en ellas) y el 43 % utiliza el marco MITRE ATT&CK (el 47 % planea invertir en él). Creemos que este cambio en el uso y la inversión en nuevas herramientas se basa en reconocer que, si bien las soluciones heredadas seguirán desempeñando un papel en las estrategias defensivas, ya no se puede confiar solo en ellas para detectar las amenazas en evolución y responder a ellas.

Figura 4.1
INNOVACIONES ACTUALES UTILIZADAS



Hallazgo 15

Las nuevas soluciones de seguridad informática deben integrarse a los marcos de trabajo y arquitecturas existentes

Para lidiar con las amenazas informáticas que enfrentan a diario, los encargados de la toma de decisiones de seguridad empresarial buscan nuevas soluciones respaldadas, fáciles de usar e integradas con otros sistemas de seguridad informática y diferentes partes de sus organizaciones.

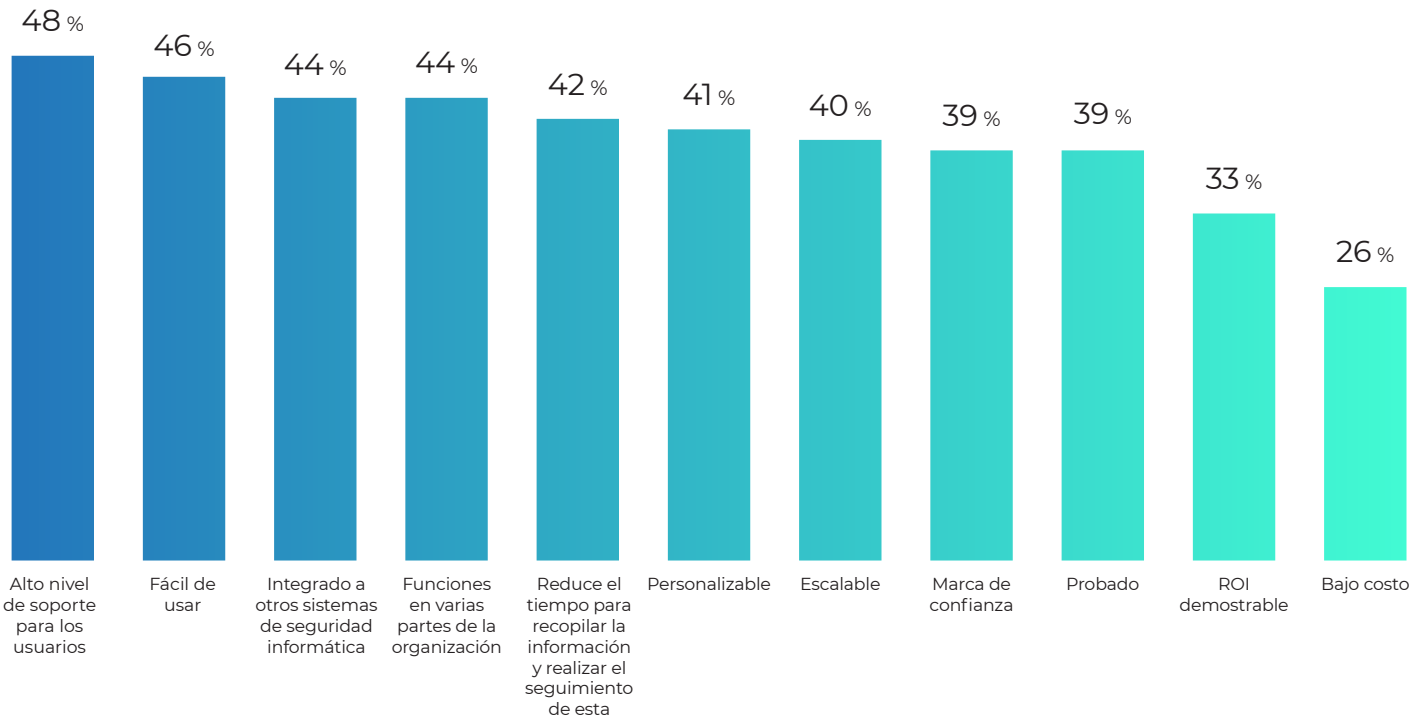
La personalización y escalabilidad también se consideran atributos esenciales cuando se evalúan nuevas herramientas de seguridad informática en, al menos, 4 de cada 10 (un 41 %) encargados de la toma de decisiones. Casi la misma cantidad (un 39 %) desea soluciones de marcas reconocidas que han sido probadas adecuadamente.

Curiosamente, solo un tercio de las organizaciones siente que es esencial que una nueva solución de seguridad informática pruebe el retorno de la inversión (ROI, del inglés Return on Investment) (un 33 %). El bajo costo es la menor de sus preocupaciones, ya que solo un cuarto de los encargados de la toma de decisiones (un 26 %) lo citaron como un requisito esencial.

RESPONDER A LOS ATAQUES INFORMÁTICOS

Figura 4.2

ATRIBUTOS ESENCIALES PARA EVALUAR SOLUCIONES DE SEGURIDAD INFORMÁTICA



A pesar de los hallazgos que demuestran una dependencia excesiva continua de las tecnologías heredadas, fue alentador descubrir que las organizaciones actualmente están utilizando innovaciones que pueden abordar este problema o están planificando invertir en ellas, como el marco de trabajo MITRE ATT&CK, XDR y la inteligencia contra amenazas.

Hallazgo 16

Para mantenerse al día con el panorama de amenazas, la mayoría de las organizaciones utiliza herramientas y tecnologías diseñadas para monitorear amenazas globales

Poner en funcionamiento la inteligencia contra amenazas es cada vez más fundamental para la capacidad de una empresa de administrar el riesgo informático y crear resistencia informática. Los equipos de seguridad a menudo pueden agobiarse por la cantidad de datos que han recopilado, así como las alertas que reciben. Con la capacidad de responder a las amenazas relevantes para su huella digital específica, se vuelven más eficaces y eficientes.

Según la investigación, el 62 % de las organizaciones utiliza herramientas y tecnologías para vigilar las amenazas globales y acelerar su rendimiento de inteligencia contra amenazas. Este hallazgo se alinea con las métricas de la industria que muestran que la demanda está aumentando para las plataformas de gestión de amenazas que utilizan la inteligencia global para detectar amenazas y otras tecnologías que ayudan a automatizar la recopilación y correlación de datos a fin de que sean útiles para los equipos de seguridad.

Estas herramientas también proporcionan procesos para que los profesionales de inteligencia gestionen los requisitos de las partes interesadas, maximicen el análisis de datos mediante la comprensión de la intención y los objetivos de los adversarios, y proyecten y mejoren la toma de decisiones.

La seguridad informática ahora es una estrategia empresarial esencial. Comprender las amenazas de seguridad informática y mitigarlas requiere las herramientas, la experiencia y los conocimientos adecuados. Un programa eficaz de inteligencia contra amenazas ayuda a las organizaciones a detectar amenazas de manera temprana y les permite actuar en su contra rápidamente.

Figura 4.3
MANERAS EN QUE LAS ORGANIZACIONES SE MANTIENEN AL DÍA CON EL CAMBIANTE PANORAMA DE AMENAZAS

CONCLUSIÓN

El nivel de resiliencia informática que han logrado las organizaciones

Para esta encuesta, definimos la resiliencia informática como la capacidad de proteger de manera proactiva y reactiva a su organización contra amenazas y atacantes, adaptarse a circunstancias cambiantes durante un ataque y recuperarse después de que se haya producido un ataque informático. Descubrimos que, aunque las organizaciones están aumentando los presupuestos de seguridad informática, agregando capas de seguridad innovadoras y enfocándose en la eficacia en lugar de los costos, aún tienen mucho trabajo que hacer si esperan prosperar en el futuro.

Después de casi dos años de desafíos e interrupciones sin precedentes en nuestra vida personal y laboral, algunos encargados de la toma de decisiones de seguridad empresarial creen que están progresando, pero no podemos concluir que este es el caso. Aunque 6 de cada 10 (un 58 %) encargados de la toma de decisiones están totalmente de acuerdo con que sus organizaciones tienen resiliencia informática, el 87 % ha sido víctima de un ataque informático exitoso durante los últimos 3 años, lo que ha provocado daños, interrupciones o una filtración a su negocio. El 42 % que cree que no ha logrado el nivel de resiliencia necesario puede estar evaluando sus posturas de seguridad con mayor precisión. Alrededor de la mitad de los encargados de la toma de decisiones de seguridad, incluso aquellos que han logrado la resiliencia, expresaron que ampliar los proyectos de transformación digital y el trabajo remoto continuo aumentarán sus probabilidades de ser víctimas de un ataque.

Figura 5.1
LA RESILIENCIA INFORMÁTICA DE LA ORGANIZACIÓN
(TOTALMENTE DE ACUERDO)

ACERCA DE ANOMALI

Anomali es el líder en soluciones de seguridad informática de detección y respuesta extendida (XDR) impulsadas por inteligencia. La plataforma de Anomali, que cuenta con una gran administración de datos y está perfeccionada por la inteligencia artificial y el aprendizaje automático, ofrece capacidades patentadas que correlacionan un volumen extraordinario de telemetría de soluciones de seguridad implementadas por el cliente con el repositorio más grande de inteligencia global, lo que permite a los equipos de operaciones de seguridad detectar amenazas con precisión, optimizar la respuesta, lograr la resiliencia y detener a los atacantes y las filtraciones. Nuestras soluciones basadas en software como servicio, que son las primeras en la nube, se integran fácilmente en las pilas de tecnología de seguridad existentes y se adaptan a la implementación híbrida. Fundada en el 2013, Anomali presta servicios a organizaciones del sector público y privado, ISAC, MSSP y clientes de Global 1000 en todo el mundo en cada industria importante. Empresas de capital riesgo líderes, incluidas Google Ventures, General Catalyst e IVP back Anomali. Obtenga más información en www.anomali.com.

CÓMO AYUDA ANOMALI

Los criminales informáticos, los actores respaldados por estados naciones y los hacktivistas trabajan tiempo extra para atacar a las organizaciones a fin de explotarlas. Las organizaciones necesitan datos e información de inteligencia contra amenazas para comprender plenamente sus vulnerabilidades, adelantarse a las amenazas y responder a los eventos rápidamente.

La detección y respuesta extendida (XDR, del inglés Extended Detection and Response) impulsada por la inteligencia de Anomali proporciona a los equipos de seguridad el contexto necesario para prevenir y abordar las amenazas de manera más rápida y eficaz. Al automatizar el proceso de recopilación y análisis de datos, información e inteligencia de amenazas internas y externas, los equipos de seguridad pueden comprender rápidamente las amenazas, determinar el impacto y respaldar una respuesta optimizada.

PRODUCTOS DE ANOMALI

Anomali ThreatStream
Gestión de inteligencia contra amenazas que automatiza la recopilación y el procesamiento de datos sin procesar y los transforma en inteligencia contra amenazas útil para acelerar la detección, optimizar las investigaciones y aumentar la productividad de los analistas.

Anomali Match
Detección y respuesta extendidas (XDR) impulsadas por inteligencia que ayuda a las organizaciones a detectar y responder de manera rápida a las amenazas en tiempo real. Match correlaciona automáticamente TODA la telemetría de seguridad con la inteligencia de amenazas activa para entregar más de 190 billones de eventos de amenazas por segundo para

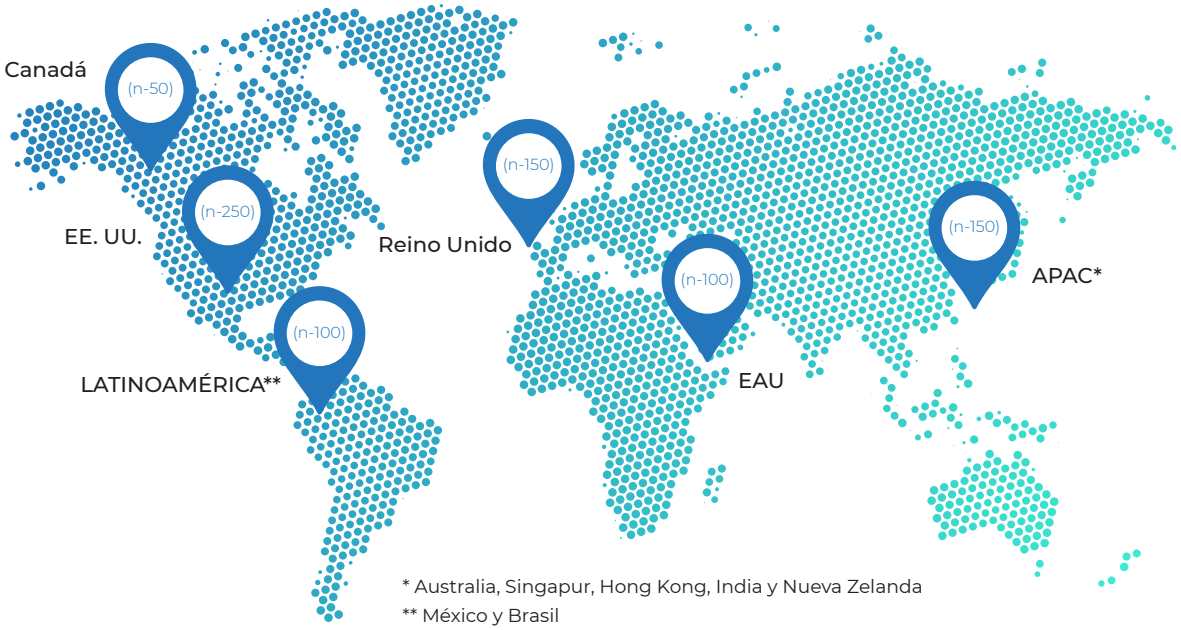
Anomali Lens
Extensión de procesamiento de lenguaje natural (NLP, del inglés Natural Language Processing) que ayuda a poner en funcionamiento la inteligencia contra amenazas mediante el análisis automático del contenido basado en la Web para identificar amenazas relevantes y optimizar el ciclo de vida de la investigación y la generación de informes sobre ellos.

Para averiguar cómo Anomali puede ayudar a su organización a tener resistencia informática, visítenos en **anomali.com.**

ANOMALI

Metodología

Anomali encargó a The Harris Poll realizar encuestas en línea entre los encargados de la toma de decisiones de seguridad empresarial en organizaciones con más de 5000 empleados. La encuesta se realizó entre el 9 de septiembre y el 13 de octubre del 2021 en los siguientes países:



* Australia, Singapur, Hong Kong, India y Nueva Zelanda
** México y Brasil

CRITERIOS DE CALIFICACIÓN

- **Mayor de 18 años**
- **Empleado a tiempo completo**
- En **servicios financieros, farmacéuticos, atención médica, telecomunicaciones, fabricación, servicios profesionales**
- En una **función de TI**
- **Perspectiva tecnológica:** nivel alto de gerente e influencia en las soluciones de seguridad de los datos
- **Perspectiva comercial:** nivel alto de director e influencia en la estrategia de seguridad de los datos

Los datos sin procesar se ponderaron cuando era necesario por la cantidad de negocios dentro de la clase de tamaño de empleados para alinearlos con sus proporciones reales en la población de negocios con más de 5000 empleados en las industrias seleccionadas de fabricación, telecomunicaciones, servicios financieros, atención médica, productos farmacéuticos y servicios profesionales, científicos y técnicos para cada país por separado. Luego, los países se combinaron con un peso posterior para proporcionarlos equitativamente en el total.