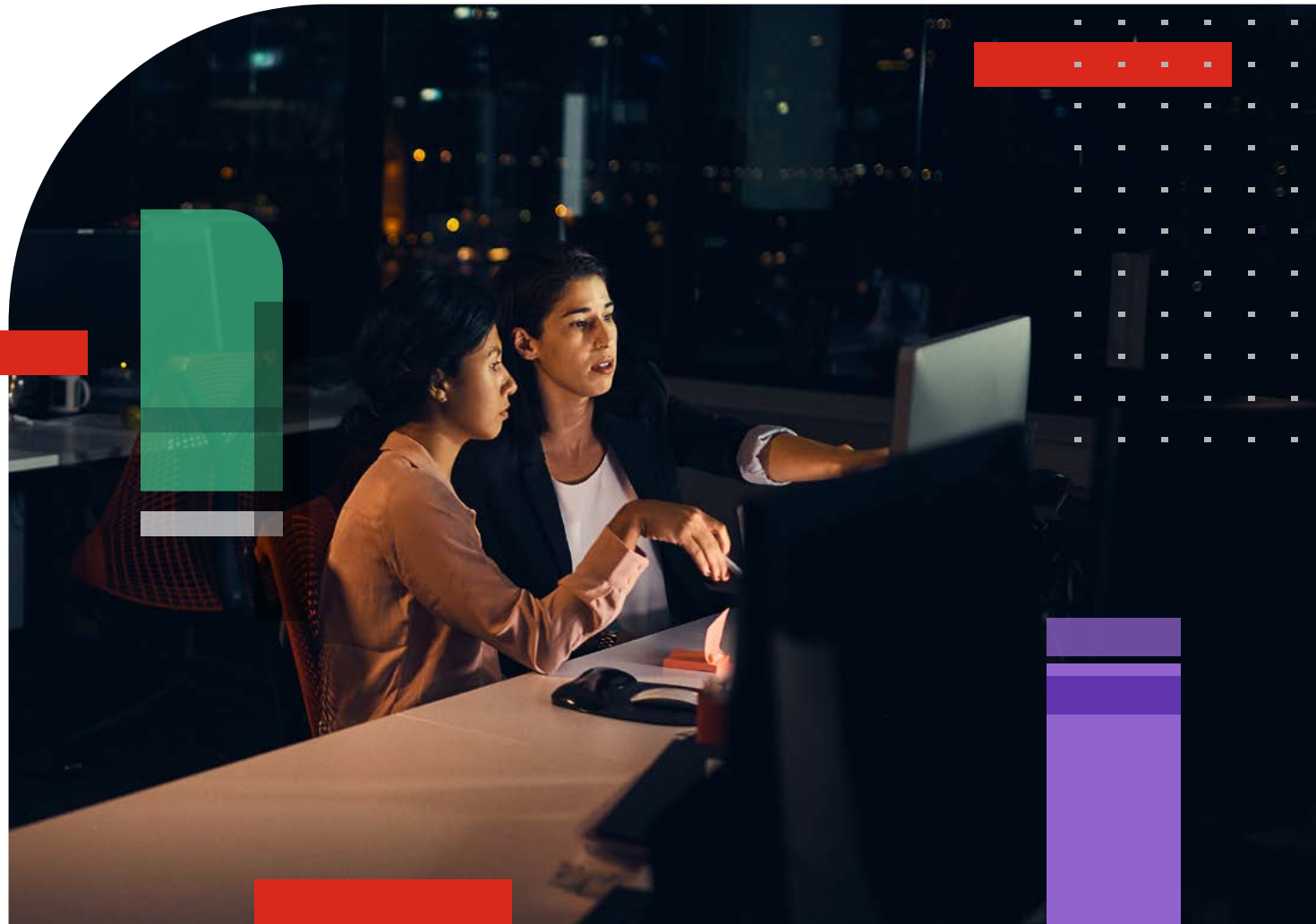
FORTINET
Training Institute

Capacitación y concientización en ciberseguridad de 2023

Resumen de investigación global



Contenido

Metodología

Los hallazgos en este reporte se basan en una entrevista en línea y una encuesta por correo electrónico a 1,855 responsables de la toma de decisiones en materia de TI y ciberseguridad, llevadas a cabo por Sapio Research en noviembre de 2022. Se recopilaron las respuestas de 29 países: Argentina, Australia, Brasil, Canadá, Colombia, Francia, Alemania, Hong Kong, India, Indonesia, Israel, Italia, Japón, Malasia, México, Países Bajos, Nueva Zelanda, República Popular de China, Filipinas, Singapur, Sudáfrica, Corea del Sur, España, Suecia, Taiwán, Tailandia, Emiratos Árabes Unidos, Reino Unido y los Estados Unidos.

Los resultados totales tienen una precisión de ± 2.3 % con límites de confianza del 95 %.

Tamaño de la empresa

De 100 a 499 empleados – **25 %**
De 500 a 999 empleados – **23 %**
De 1,000 a 2,499 empleados – **23 %**
De 2,500 a 4,999 empleados – **15 %**
Más de 5,000 empleados – **14 %**

Género

El **68 %** de los encuestados eran hombres
32 % de los encuestados eran mujeres

Total de encuestados: 1,855

APAC **30 %**
EMEA **27 %**
América del Norte **22 %**
LATAM **22 %**

Tipo de función

El **13 %** de los encuestados ocupaba puestos de propietario
El **34 %** de los encuestados eran ejecutivos de nivel C
El **7 %** de los encuestados eran vicepresidentes
El **12 %** de los encuestados eran presidentes
El **34 %** de los encuestados eran directores

Sector empresarial

Sectores de empresa: los 3 primeros

21 % Tecnología
16 % Manufactura
13 % Servicios financieros

INTRODUCCIÓN

Enfoque en el elemento humano de la ciberseguridad

A medida que se intensifican los ciberataques, más y más organizaciones reconocen la necesidad de tener una cultura sólida de seguridad para todos los empleados. La fuerza laboral con ciberconciencia es una adición necesaria a un equipo de seguridad competente y bien informado, además del uso de soluciones avanzadas de ciberseguridad. Los empleados que saben cómo practicar una buena ciberhigiene se consideran cada vez más como una línea de defensa crucial.

Reforzar las ciberdefensas será importante en 2023, dado que las organizaciones se enfrentan a un panorama de amenazas en constante evolución. FortiGuard Labs de Fortinet predice un crecimiento "desmedido" del cibercrimen como servicio (CaaS); el uso del aprendizaje automático para lavar dinero; vulnerabilidades de seguridad del cibercrimen en entornos de realidad aumentada, virtual y mixta; y el malware de wiper (borrado) de datos.

Esta predicción resalta la naturaleza crítica de la capacitación y concientización en ciberseguridad de los empleados, razón por la que Fortinet da a estos temas su propio enfoque en este *Resumen de investigación global sobre capacitación y concientización en ciberseguridad de 2023*. Las siguientes páginas destacan algunas de las principales preocupaciones y acciones que están tomando los líderes de todo el mundo, según los hallazgos del Reporte de la investigación global anual de la brecha de competencias de ciberseguridad de Fortinet.

Resumen ejecutivo

Los empleados pueden ser su punto más débil o su defensa más poderosa.

El 81 % de las organizaciones encuestadas enfrentaron **ataques de malware**, **suplantación de identidad y contraseña** el año pasado, muchos de los cuales se dirigieron directamente a los usuarios.

Los empleados carecen de concientización en ciberseguridad, incluso con la capacitación actual.

El 56 % de los líderes creen que sus **empleados carecen de conocimientos** con respecto a la concientización en ciberseguridad.

La ciberseguridad es una prioridad creciente para las juntas corporativas.

El 93 % de las juntas directivas se están cuestionando sobre **las ciberdefensas de sus organizaciones**.

El 81 % de los ciberataques fueron del tipo de ataques de suplantación de identidad, contraseña y malware.

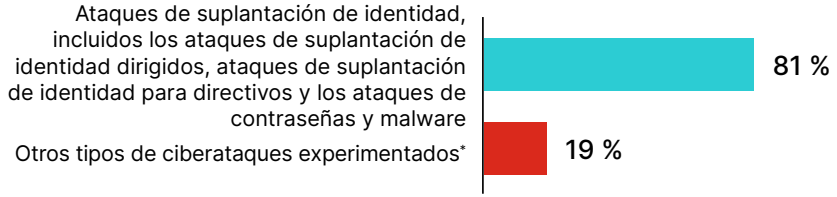
Los empleados pueden ser su punto más débil o su defensa más poderosa

Casi todas las organizaciones encuestadas experimentaron al menos una violación de datos de ciberseguridad en los últimos 12 meses. Casi un tercio experimentó cinco o más. Una característica común de muchos de los ciberataques que se produjeron en 2022 fue que se dirigieron directamente a los usuarios, como esquemas de suplantación de identidad, o aprovecharon una ciberhigiene débil para comprometer contraseñas y credenciales.

Aunque el malware fue el tipo de ataque más común usado en los últimos 12 meses, la suplantación de identidad podría ser la más insidiosa y, por lo general, aloja otros tipos de ataques con apariencia de correos electrónicos, mensajes de texto y enlaces web amistosos. Otros tipos de ataques reportados dirigidos a los empleados incluyeron ataques de contraseña, suplantación de identidad dirigida y suplantación de identidad para directivos (también conocido como Whaling).

Dado que el costo de las violaciones de datos supera USD 1 millón para casi la mitad de las organizaciones que respondieron, parece clave equipar a los empleados para que reconozcan, eviten y reporten las ciberamenazas.

Ataques más comunes que reportaron las organizaciones



*Se refiere a ataques web, ataques de caballo de Troya, ataques de ransomware, ataques DoS y DDoS, ataques de suplantación de DNS, amenazas internas, interpretación de URL, ataques de inyección SQL, ataques de fuerza bruta, ataques Drive-by, ataques de escucha clandestina, ataques de secuestro de sesión, ataques de scripting entre sitios (XSS), ataques Man-in-the-Middle (MITM), ataques de cumpleaños.

**Preguntado solo a aquellos cuya organización experimentó un ciberataque en los últimos 12 meses.

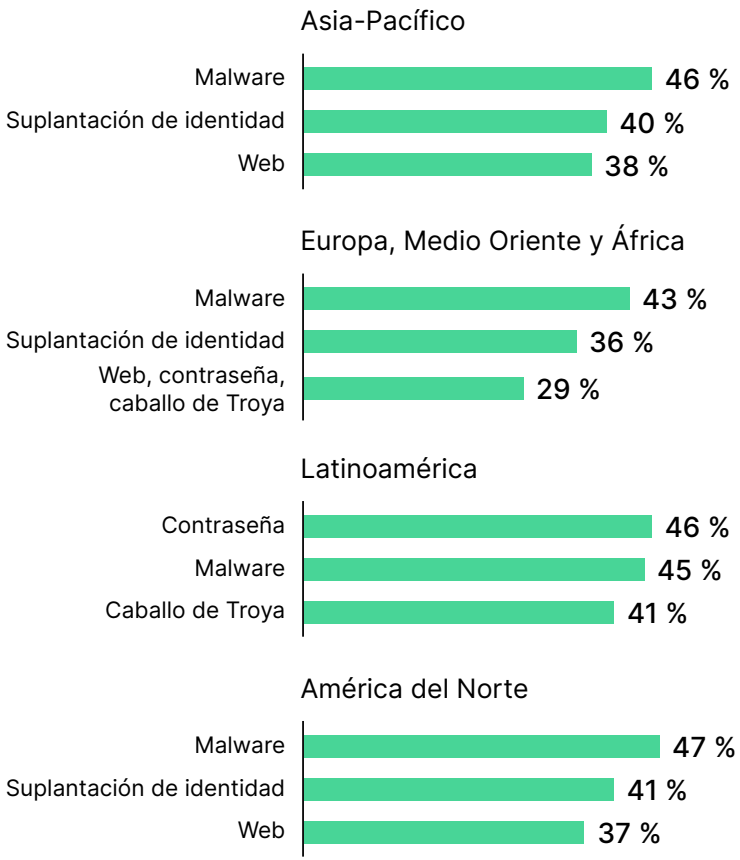
Profundizando

- **El 84 %** de las organizaciones encuestadas experimentaron **al menos una violación de datos de ciberseguridad** en los últimos 12 meses, frente al 80 % del año anterior.
- **El 29 % tuvo cinco o más**, frente al 19 %.
- Y el **7 % tuvo más de 9**, frente al 3 %.
- **El 65 %** de los líderes esperaba un **aumento promedio del 20 % de ciberataques** durante los próximos 12 meses.

Hechos destacados regionales

Los ataques más comunes varían según la región.

Las organizaciones en cada región del mundo tienen un perfil de ataque ligeramente diferente.



Diferentes industrias enfrentan diferentes volúmenes de ataques de malware.

La investigación de FortiGuard Labs 2022 muestra que los volúmenes de ataque varían según la industria y la región. Para esta investigación, FortiGuard Labs separó Europa y Medio Oriente de África.

Industria

Servicios financieros
Regional alta ^ Europa y Medio Oriente (**63.1 %**)
Regional baja v Latinoamérica (**1.8 %**)

Atención médica
Regional alta ^ Asia Pacífico (**62 %**)
Regional baja v África (**2.6 %**)

Servicios de seguridad administrada
Regional alta ^ Europa y Medio Oriente (**46.6 %**)
Regional baja v Asia Pacífico (**1.8 %**)

Minoristas y hostelería
Regional alta ^ Asia Pacífico (**38.8 %**)
Regional baja v África (**8.6 %**)

Petróleo y gas
Regional alta ^ Europa y Medio Oriente (**49.1 %**)
Regional baja v Asia Pacífico (**18.9 %**)

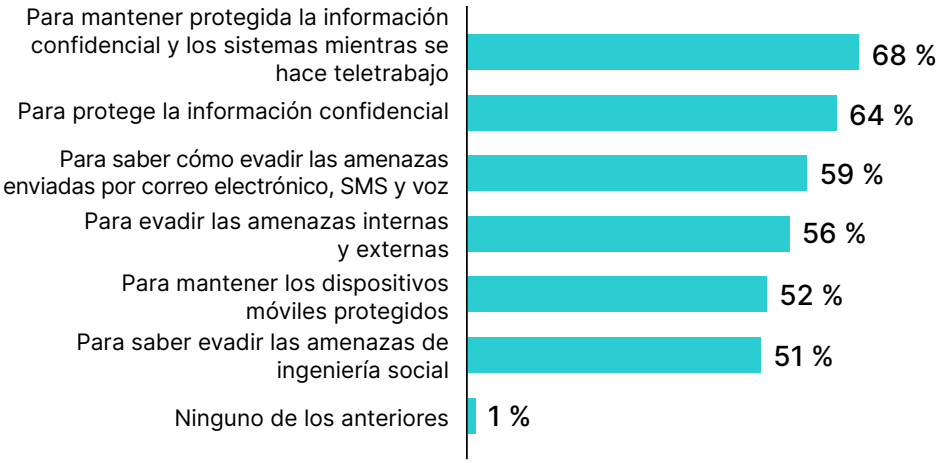
Los empleados carecen de concientización en ciberseguridad, incluso con la capacitación actual

El ochenta y cinco por ciento de los líderes dicen que su organización tiene un programa de capacitación y concientización en ciberseguridad, pero más de la mitad cree que sus empleados aún carecen de conocimientos de ciberseguridad.

Esta desconexión parece sugerir que los programas de capacitación existentes no son tan efectivos como podrían ser, que las prácticas de ciberhigiene se aplican de manera incoherente o que la capacitación no se refuerza lo suficiente, lo que los analistas consideran clave para construir una cultura de ciberseguridad efectiva.

Los líderes dicen que proteger la información confidencial y los sistemas al trabajar de forma remota es el aspecto más importante de la concientización de ciberseguridad para los empleados, seguido de cerca por la protección de la información confidencial en general.

¿Dónde es más importante la concientización en ciberseguridad?



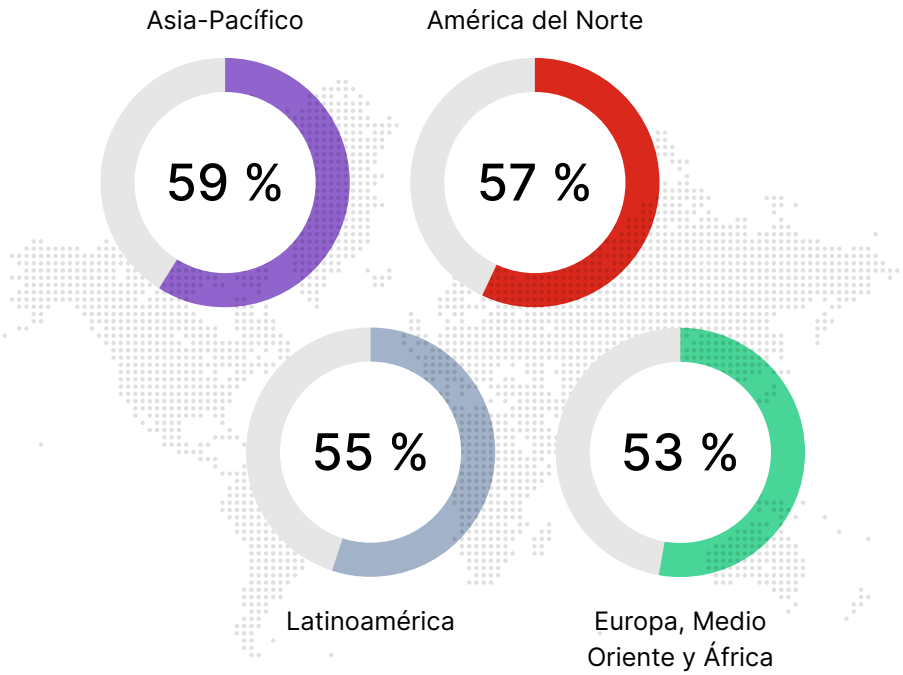
Profundizando

- **El 56 %** de los líderes creen que sus **empleados carecen de conocimientos** con respecto a la concientización en ciberseguridad, frente al 52 % de 2021. Y eso a pesar de que el **85 %** tiene un **programa de capacitación y concientización en ciberseguridad** en marcha.
- **El 73 %** de las organizaciones **sin un programa de capacitación** busca uno, lo que representa un aumento frente al 66 % en 2021.
- **El 93 %** de los líderes creen que una mayor concientización en ciberseguridad de los empleados ayudaría **a reducir los ciberataques**.
- **El 59 %** de los líderes dicen que es razonable que los empleados dediquen **entre una y tres horas al año a la capacitación en ciberseguridad**.
- **El 68 %** de los líderes dicen que es más importante que los empleados sepan **cómo mantener protegida la información confidencial y los sistemas mientras hacen teletrabajo**.

Hechos destacados regionales

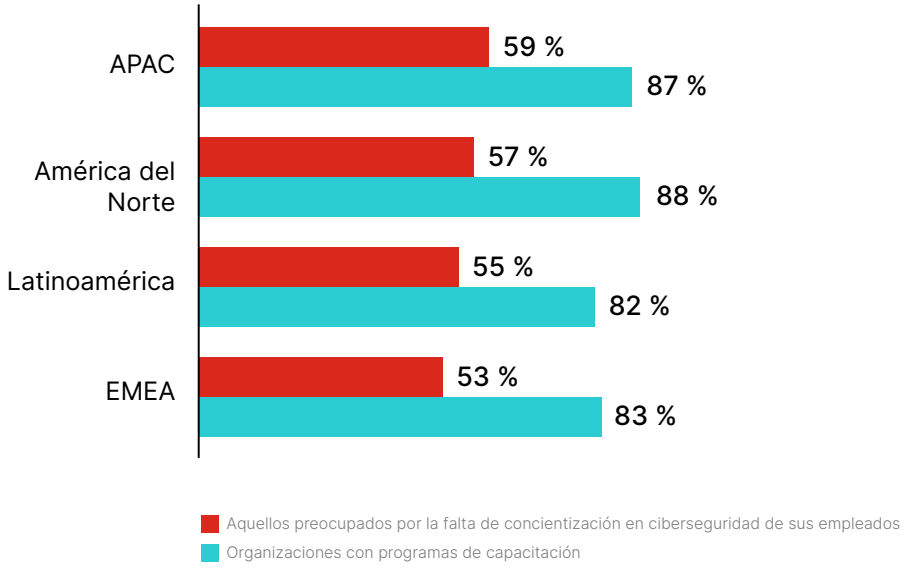
¿Son las preocupaciones sobre la concientización en ciberseguridad similares en todas las regiones?

La preocupación es levemente mayor en la región de Asia Pacífico y menor en Europa, Medio Oriente y África.



La capacitación es frecuente, pero las brechas persisten.

Es interesante ver que, aunque más de la mitad de los líderes de todas las regiones creen que falta concientización en ciberseguridad, la mayoría de las empresas ofrecen programas de capacitación.



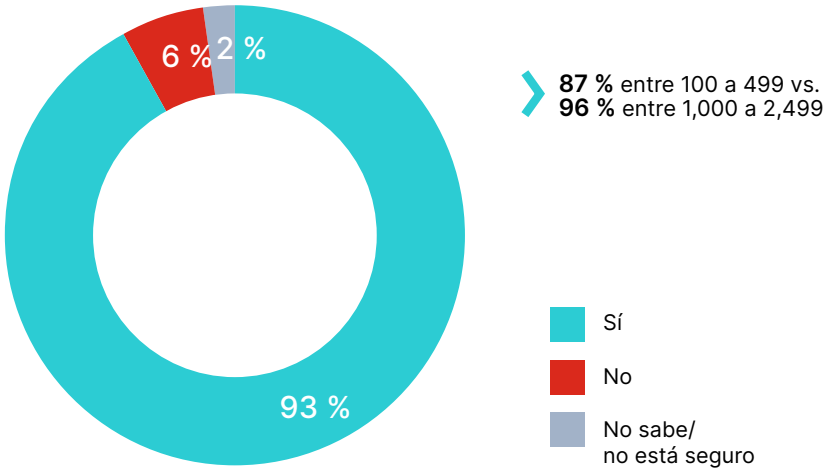
La ciberseguridad es una prioridad creciente para las juntas directivas

Un rotundo 93 % de los líderes con una línea directa a una junta directiva dice que su junta pregunta sobre las ciberdefensas de la organización.

Es razonable considerar esto como una señal de que las juntas se toman en serio sus responsabilidades de gestionar el riesgo corporativo y proteger la marca, además de estar conscientes del aumento de ataques y violaciones de datos.

Debido a que muchos ataques tienen como objetivo los usuarios, parece probable que las juntas reconozcan, o reconozcan pronto, que la concientización en ciberseguridad de los empleados es una parte fundamental de la "ecuación de la defensa". El noventa y tres por ciento de los líderes cree que una mayor concientización en ciberseguridad de los empleados ayudaría a disminuir la ocurrencia de ciberataques.

Las juntas directivas preguntan sobre la ciberseguridad



*Solo se les preguntó a aquellas organizaciones cuyas juntas directivas se preguntan cómo se protegen sus organizaciones contra el aumento de los ciberataques.

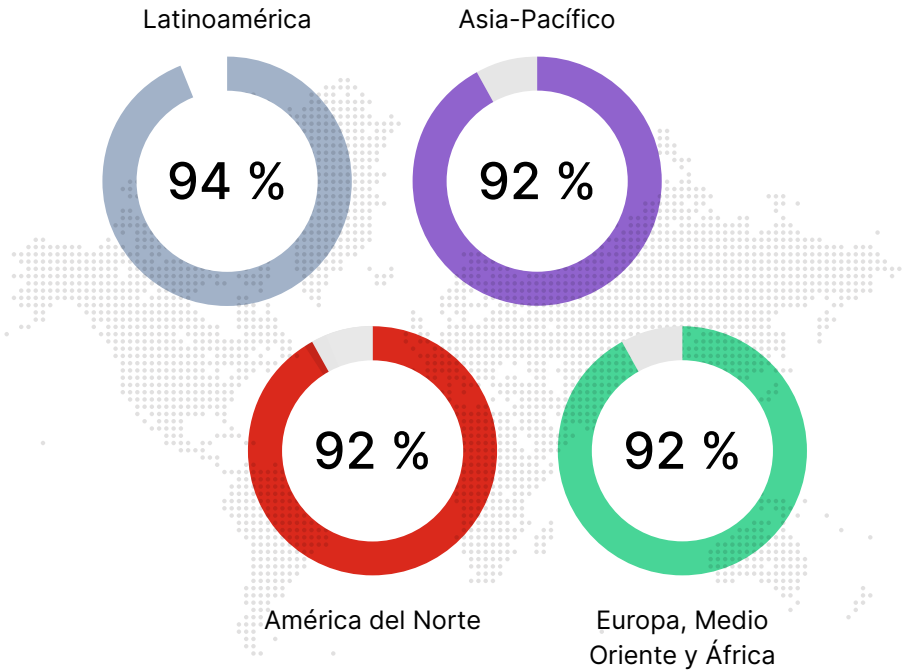
Profundizando

- **El interés de la junta directiva en la ciberseguridad aumentó: hasta un 93 %** en esta encuesta actual de 88 %, según lo que se indica en el *reporte Brecha de competencias en ciberseguridad 2022 de Fortinet*.
- **El interés de la junta en la seguridad es uniforme en gran medida a través de todas las industrias**, aunque es un poco más alto en servicios financieros, atención médica y telecomunicaciones (entre 94 y 95 %) que en educación, medios y entretenimiento (88 %).

Hechos destacados regionales

Las juntas de todas las regiones preguntan sobre la ciberseguridad.

Los resultados de la encuesta muestran niveles similares de preocupación entre las juntas de todo el mundo.



*Solo se les preguntó a aquellas organizaciones cuyas juntas directivas se preguntan cómo se protegen sus organizaciones contra el aumento de los ciberataques.

Conclusión

Con el 84 % de los líderes que reporta al menos una ciberviolación de datos en los últimos 12 meses, y casi la mitad que menciona un costo total de las violaciones de datos superior a USD 1 millón, es importante que las organizaciones continúen fortaleciendo sus ciberdefensas. Las organizaciones deben desarrollar un enfoque integral de la ciberseguridad, que incluya soluciones sofisticadas y automatizadas, equipos de expertos y, como muestran los resultados de esta encuesta, un programa efectivo de capacitación y concientización en ciberseguridad.

Los empleados son una línea de defensa esencial.

Dado que muchos de los tipos más comunes de ciberataque (esquemas de suplantación de identidad, ciertas formas de malware y ataques de contraseña) se dirigen directamente a los usuarios, es probable que la poca concientización en ciberseguridad de los empleados debilite significativamente la postura de seguridad general de una organización. Por el contrario, los programas efectivos de capacitación y concientización en ciberseguridad pueden mejorar la postura de seguridad, agregando capas adicionales de protección a una organización. Los líderes parecen reconocer esto, un 93 % respondió que creen que una mayor capacitación y concientización para los empleados ayudaría a disminuir la frecuencia de los ciberataques.

Hay que reforzar la capacitación.

Los programas de capacitación y concientización en ciberseguridad son métodos ampliamente reconocidos para reforzar la cibercultura de los empleados. No es sorprendente que la mayoría de las organizaciones tengan programas existentes. No obstante, más de la mitad de todos los líderes encuestados aún están preocupados por la falta de concientización en ciberseguridad de sus empleados. Una evaluación crítica de los programas de capacitación y concientización en ciberseguridad podrían revelar oportunidades para tratar el elemento humano de la ciberseguridad de manera más efectiva, reduciendo así el riesgo general. Tomar medidas para garantizar que los programas cubran suficientemente una amplia gama de temas de manera práctica, y que el aprendizaje se refuerce con recordatorios y comprobaciones, debería ayudar a mejorar los resultados de la capacitación.

Las juntas directivas se centran en la ciberseguridad.

Con un programa de capacitación sólido, las organizaciones pueden aumentar la concientización de los empleados sobre el riesgo cibernético y empoderarlos para defender la organización, estableciendo las bases para una cultura de ciberseguridad sólida y preparada. Esto puede resonar en las juntas directivas corporativas que, como muestran los resultados de la encuesta de este año, están cada vez más preocupadas por la seguridad cibernética y probablemente se centren en el elemento humano en el futuro, reconociendo que desempeña un papel esencial en la protección de los intereses empresariales y la reputación de la marca corporativa.

Las organizaciones saben que necesitan soluciones de ciberseguridad avanzadas y que las certificaciones de tecnología desarrollan las funcionalidades de ciberseguridad de sus equipos de TI. Hasta la fecha, es posible que la concientización de los empleados no haya recibido toda la atención que merece; no obstante, podría resultar fundamental en la lucha contra los ciberataques en los próximos años.

Puede encontrar una visión más amplia y detallada de las necesidades y desafíos de ciberseguridad de las organizaciones en el Reporte de la investigación global anual de la brecha de competencias de ciberseguridad 2023 de Fortinet.

Acerca de Fortinet

Fortinet (NASDAQ: FTNT) es una fuerza impulsora en la evolución de la ciberseguridad y la convergencia de las redes y la seguridad. Nuestra misión es proteger a las personas, los dispositivos y los datos en todas partes y hoy en día ofrecemos ciberseguridad en todos los lugares donde se necesita con la mayor cartera integrada de más de 50 productos de nivel empresarial.

Más de medio millón de clientes confían en las soluciones de Fortinet, que se encuentran entre las más implementadas, patentadas y validadas del sector.

El Instituto de Capacitación de Fortinet, uno de los programas de capacitación más grandes y amplios de la industria, se dedica a ofrecer capacitación en ciberseguridad y las nuevas oportunidades profesionales y las pone al alcance de todos. FortiGuard Labs, la organización de investigación e inteligencia frente a amenazas de élite de Fortinet, desarrolla y utiliza tecnologías de aprendizaje automático e IA de vanguardia para proporcionar a los clientes protección oportuna y constante de primera categoría e inteligencia práctica frente a amenazas. Obtenga más información en https://www.fortinet.com, el Fortinet Blog y FortiGuard Labs.

FORTINET

Training Institute

www.fortinet.com/lat

Mayo de 2023