FORTINET
Training Institute

Brecha de competencias en ciberseguridad 2023

Informe de Investigación Global

Contenido

Metodología

Los hallazgos de este informe están basados en las respuestas de las entrevistas 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 obtuvo 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 **22 %**
De 500 a 999 empleados **24 %**
De 1,000 a 2,499 empleados **23 %**
De 2,500 a 4,999 empleados **16 %**
Más de 5,000 empleados **15 %**

Género

El **68 %** de los encuestados eran hombres
El **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 ocupaban puestos ejecutivos de nivel C
El **7 %** de los encuestados ocupaban puestos de vicepresidente
El **12 %** de los encuestados ocupaba puestos de jefe
El **34 %** de los encuestados ocupaban puestos de director

Sector empresarial

Sectores de empresa: los 3 primeros

Tecnología **21 %**
Manufactura **16 %**
Servicios financieros **13 %**

Resumen ejecutivo

Las conclusiones de este informe sobre la brecha de competencias en ciberseguridad 2023 muestran claramente que las organizaciones están librando una ardua batalla contra las ciberamenazas: sufren más violaciones de seguridad, necesitan profesionales cualificados y siguen luchando por cubrir puestos clave.

Las violaciones de seguridad son más frecuentes y costosas

El **84 %** de las organizaciones experimentaron **una o más violaciones de seguridad** en los últimos 12 meses, frente al 80 % en 2021.

El **29 %** experimentó **cinco o más intrusiones**, frente al 19 % del año anterior.

El **48 %** experimentó violaciones de seguridad en los últimos 12 meses cuya **reparación costó más de USD 1 millón,** frente al 38 % en 2021.

Puestos de TI vacantes: un riesgo para la ciberseguridad

El **68 %** de las organizaciones indican que se **enfrentan a riesgos** adicionales debido a la escasez de competencias en ciberseguridad, en consonancia con el 67 % en 2021.

El **56 % tiene dificultades para reclutar** y el **54 % para retener el** talento, frente al 60 % y el 52 % en 2021.

La seguridad en la nube y las operaciones de seguridad son los puestos más difíciles de cubrir.

Las juntas directivas se centran en la ciberseguridad

El **93 %** de los encuestados indica que su **junta directiva se interesa por la ciberseguridad,** frente al 88 % en 2021.

En 2022, **el 83 % de las juntas sugirió aumentar el personal de seguridad de TI,** en comparación con el 76 % en 2021.

Certificaciones como prueba de conocimientos y competencias en ciberseguridad

El **90%** de los líderes **prefiere contratar a personas con certificaciones centradas en la tecnología,** frente al 81 % en 2021. **El 90 % también pagaría** para que un empleado obtuviera una certificación en ciberseguridad.

El **72 %** de los líderes indican que la contratación de personas certificadas **aumentó la concientización** y los conocimientos sobre seguridad dentro de su organización.

La diversidad puede ayudar a cubrir las necesidades de competencias, pero no siempre es fácil de encontrar

Aproximadamente el **40 %** tiene **dificultades para encontrar candidatos calificados** que sean mujeres, veteranos militares o pertenezcan a minorías.

El **83 %** de las organizaciones **tienen objetivos de contratación de diversidad a corto plazo,** frente al 89 % en 2021.

El número de organizaciones que confirman cinco o más violaciones de seguridad saltó un 53 % entre 2021 y 2022.

INTRODUCCIÓN

Las personas calificadas son clave en la ciberseguridad

En 2022, los retos de ciberseguridad se intensificaron a nivel mundial en todos los sectores, desde el crecimiento exponencial de nuevas variantes de ransomware hasta el aumento de los ataques a la tecnología operativa (TO) y el incremento del malware como servicio (MaaS). Para muchas organizaciones, estos desarrollos hacen que cerrar la brecha de competencias en ciberseguridad dentro de sus propios equipos de TI sea una prioridad más alta que nunca.

Mientras que las soluciones avanzadas de ciberseguridad siguen siendo esenciales para satisfacer las demandas de un panorama de amenazas en rápida evolución, el Informe de Investigación Global sobre la Brecha de competencias en ciberseguridad 2023 de Fortinet revela que los líderes también se fijan en el lado humano de la ecuación, tratando de entender qué competencias necesitan y dónde encontrarlas.

La atención a la creación de capacidades en ciberseguridad comienza en la cúpula, con más juntas directivas que plantean preguntas sobre ciberdefensa y recomiendan un aumento de personal de seguridad de TI. Es probable que esto se deba al reconocimiento de su responsabilidad de salvaguardar la empresa, y por extensión, a los clientes, socios, empleados y la marca corporativa.

Como muestra este informe 2023, las organizaciones buscan reclutar y retener talento para satisfacer sus necesidades de ciberseguridad, en concreto, personas con certificaciones centradas en la tecnología, así como de grupos subrepresentados, como mujeres, personas de poblaciones minoritarias y veteranos militares.

Las novedades de 2023

Esta edición del Informe de Investigación Global sobre la Brecha de competencias en ciberseguridad presenta comparaciones de un año a otro y análisis de tendencias basados en los comentarios de los líderes de seguridad de todo el mundo. Aunque muchos resultados se mantuvieron constantes entre los dos últimos años, se identifican algunas diferencias notables en el informe.

Para más información sobre la concientización de los empleados en ciberseguridad, lea nuestro informe complementario: **Resumen de investigación global de capacitación y concientización en ciberseguridad 2023**, que se publicará esta primavera.

El número de organizaciones que confirman **cinco o más violaciones de seguridad saltó un 53 %** entre 2021 y 2022.

Las violaciones de seguridad son más frecuentes y costosas

Como predijo FortiGuard Labs de Fortinet, las ciberamenazas de todo tipo se hicieron cada vez más ubicuas en 2022. Esta omnipresencia dio lugar a más violaciones de seguridad que el año anterior, y a un mayor costo total de las violaciones de seguridad para muchas organizaciones.

Un elevado número de líderes también atribuye estas violaciones de seguridad, hasta cierto punto, a la falta de competencias en ciberseguridad entre los profesionales de TI

La opinión mayoritaria parece ser que el panorama de amenazas no hará más que empeorar. En los próximos 12 meses, el 65 % de los encuestados espera que aumente el número de ciberataques. Esta predicción se alinea con las proyecciones de FortiGuard Lab, que anticipan el crecimiento de muchos tipos de ataques y modelos de negocio de cibercrimen, incluyendo el mercado de crimen como servicio (CaaS).

A pesar del aumento de las violaciones de seguridad, el 93 % de los líderes cree que su organización está haciendo todo lo posible para hacer frente al creciente volumen de ataques. Esto puede sugerir incertidumbre sobre las medidas adicionales que pueden tomar las organizaciones y se contradice en cierta medida con otras conclusiones sobre el aumento de las preocupaciones de las juntas, como la necesidad de certificaciones para validar las competencias, los conocimientos y las brechas en la concientización en ciberseguridad de los empleados.

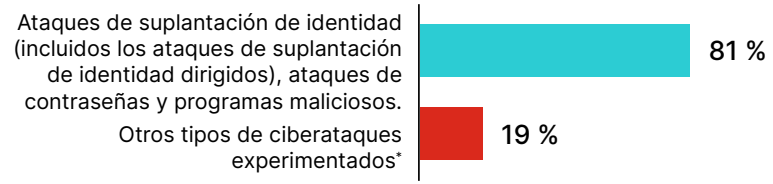
El 81 % de los ciberataques fueron en forma de suplantación de identidad, contraseñas y ataques de malware.

La suplantación de identidad es el método de ataque más común

En 2022, los encuestados informaron que la suplantación de identidad, el malware y los ataques a las contraseñas constituían en conjunto la mayor parte (81 %) de los tipos de ataques que sufrían las organizaciones encuestadas en 2022. En particular, estos tres ataques se pueden dirigir no solo a sistemas, sino también directamente a usuarios individuales. Los esquemas de suplantación de identidad son especialmente insidiosos, ya que a menudo transmiten los otros tipos de ataque: malware e ingeniería social que pueden conducir a ataques de contraseñas y web.

Las organizaciones de América del Norte experimentaron muchos más ataques de suplantación de identidad que sus homólogas de Latinoamérica, mientras que estas experimentaron muchos más ataques de contraseñas que sus homólogas de Europa, Oriente Medio y África.

¿Qué tipos de ciberataques experimentó su organización?



*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 año pasado más organizaciones sufrieron violaciones de seguridad que en 2021 a

El 84 % de los encuestados indica que su organización experimentó una o más violaciones de seguridad en los últimos 12 meses, frente al 80 % del año anterior.

- El 55 % sufrió entre una y cuatro violaciones de seguridad.
- El 29 % sufrió cinco o más violaciones de seguridad.
- El 7 % tenía nueve o más, más del doble que el año anterior (3 %).

Aumentó notablemente el costo de las violaciones de seguridad superiores a USD 1 millón

Casi la mitad (48 %) de las organizaciones que sufrieron al menos una violación de seguridad en los últimos 12 meses indican que costó más de USD 1 millón remediarla, frente al 38 % en 2021.

- El 64 % de las organizaciones norteamericanas informaron que el costo total de las violaciones de seguridad supera el USD 1 millón, la cifra más alta de todas las regiones.
- El 31 % de las organizaciones latinoamericanas informan de un costo total de las violaciones de seguridad superior al USD 1 millón, el menor de todas las regiones.

El 64 % de las organizaciones norteamericanas informaron que el costo total de las violaciones de seguridad supera el USD 1 millón, la cifra más alta de todas las regiones.

La mayoría de los líderes cree que los ataques aumentarán en el futuro

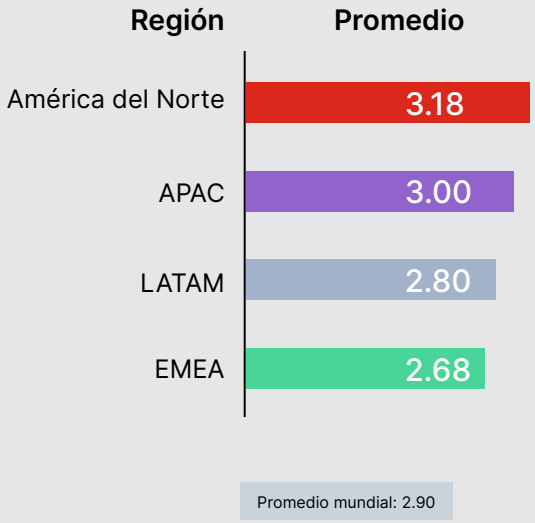
Aunque la mayoría de los encuestados (65 %) espera que los ciberataques aumenten en los próximos 12 meses, un sorprendente 19 % indica que no espera ningún aumento. Teniendo en cuenta las predicciones de los analistas en sentido contrario, estas organizaciones podrían ser vulnerables, ya que probablemente no priorizarán la preparación de sus redes en materia de seguridad, el reclutamiento de personal de TI o el desarrollo de las competencias cibernéticas del personal.

- Los encuestados norteamericanos prevén un aumento del 25 % de los ataques durante el próximo año.
- Los encuestados de Europa, Medio Oriente y África esperan un aumento ligeramente inferior, del 17 %.

Hechos destacados regionales

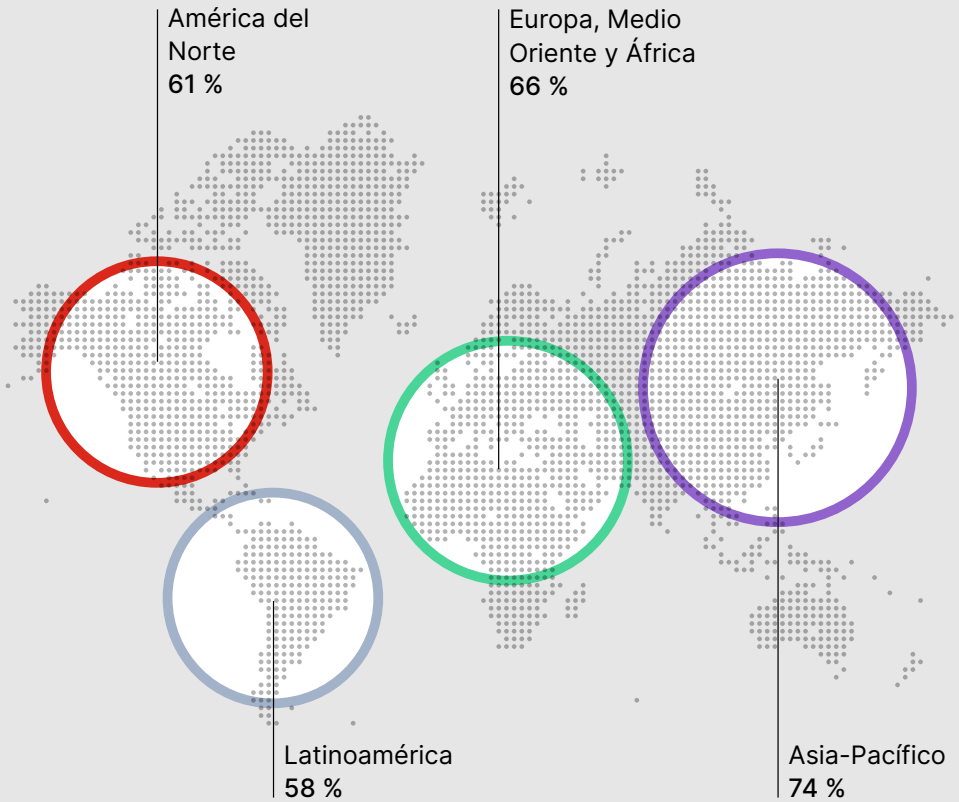
Las organizaciones norteamericanas registran el mayor número de violaciones de seguridad

En promedio, los encuestados de América del Norte indican que sufrieron el mayor número de violaciones de seguridad, mientras que los de Europa, Medio Oriente y África son los que menos.



Las organizaciones de Asia-Pacífico prevén un aumento de los ataques

Un número considerablemente mayor de encuestados de la región Asia-Pacífico cree que los ciberataques aumentarán en los próximos 12 meses.



Las juntas directivas se centran en la ciberseguridad

A medida que aumentan las ciberamenazas y las violaciones de seguridad, la seguridad de TI sigue ganando importancia en el ámbito de la gobernanza, y las juntas corporativas se plantean preguntas directas sobre cómo se protegen las organizaciones.

En los dos últimos años, analistas como McKinsey y publicaciones como *Harvard Business Review* destacaron la función que pueden desempeñar las juntas directivas para ayudar a las organizaciones a reforzar su postura de seguridad. La creciente superficie de ataque de las empresas y la diversificación de las amenazas convierten este aspecto en algo de vital importancia, dadas las responsabilidades de las juntas directivas a la hora de supervisar el riesgo corporativo y la administración de reputación.

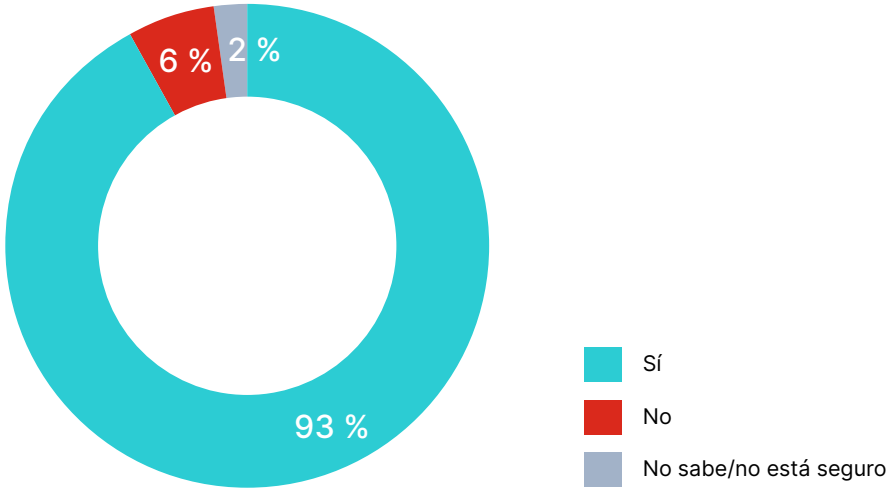
Como resultado, casi todos los líderes encuestados (93 %) indican que sus juntas directivas están planteando preguntas sobre ciberseguridad, y la mayoría de las juntas (83 %) abogan por contratar más personal de seguridad de TI.

El 83 % de las juntas directivas recomiendan aumentar el personal de seguridad de TI.

Las preocupaciones de la junta directiva aumentan con el tamaño de la organización

Aunque la mayoría de las juntas directivas (93 %) se interesan en la ciberseguridad, ese escrutinio es mayor (96 %) en las organizaciones con entre 1,000 y 2,499 empleados.

¿Se pregunta la junta directiva cómo se protege la organización contra el aumento de los ciberataques?



*Se cuestionó solo a aquellos cuya junta depende o tiene una línea directa de comunicación con una junta directiva.

Profundizando

Crece la preocupación de la junta por las ciberamenazas

Casi todos los líderes encuestados (91 %) informan o tienen una línea directa de comunicación con una junta directiva.

- El 93 % indica que su junta pregunta cómo se protege la organización contra los crecientes ciberataques, frente al 88 % en 2021.
- El 96 % de las juntas que gobiernan organizaciones con entre 1,000 y 2,499 empleados preguntan sobre ciberseguridad.

El aumento de personal para reforzar la seguridad es una de las principales prioridades de la junta

La mayoría de las juntas recomiendan contratar personal de TI y ciberseguridad.

- El 83 % de los líderes indica que su junta recomendó aumentar el personal de TI y ciberseguridad en 2022, frente al 76 % en 2021.
- El 85 % de las juntas que gobiernan organizaciones con más de 5,000 empleados recomendaron aumentar el personal de seguridad de TI.

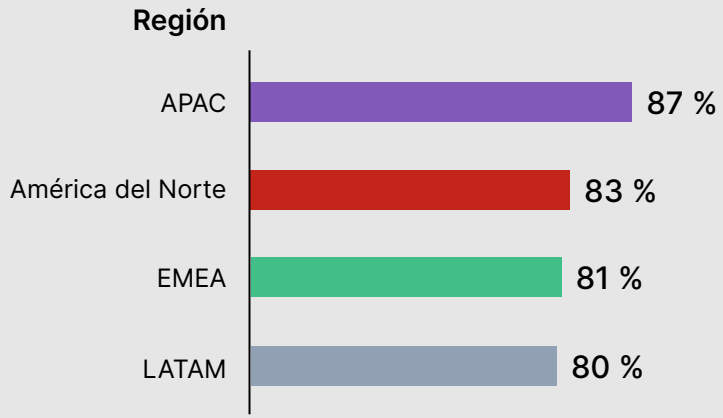
El 93 % de las juntas se pregunta cómo se protege la organización contra los crecientes ataques de la ciberseguridad.

Hechos destacados regionales

Las juntas de todas las regiones están preocupadas por la ciberseguridad

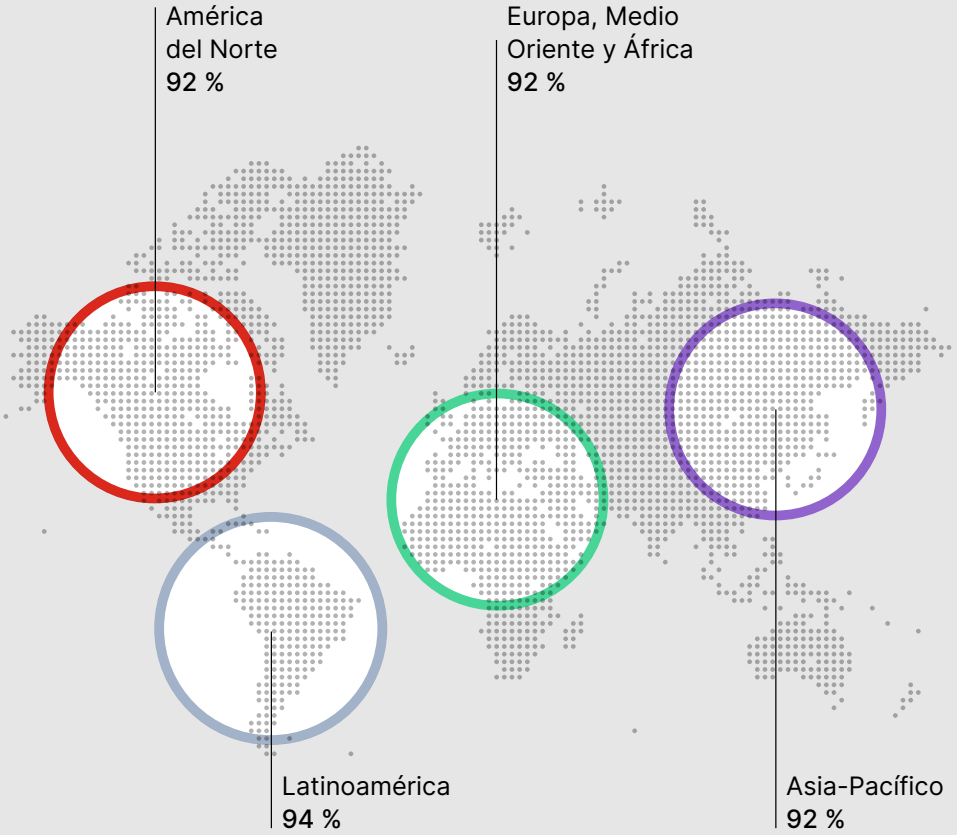
El interés por proteger a las organizaciones de las ciberamenazas es constantemente alto en todo el mundo.

¿Sugiere la junta directiva un aumento de personal para el Departamento de TI o de Seguridad?*



Las juntas de todas las regiones abogan por contratar más personal de seguridad de TI

Los países de la región Asia-Pacífico fueron los que más se inclinaron por aumentar el personal de ciberseguridad en 2022.



*Se cuestionó solo a aquellos cuya junta directiva se interesa en proteger su organización contra el aumento de los ciberataques.

Certificaciones como prueba de conocimientos y competencias en ciberseguridad

La mayoría de los líderes reconocen el valor de los conocimientos y competencias técnicas especializadas. El ochenta y dos por ciento (82 %) de los encuestados indica que su organización se beneficiaría de las certificaciones en ciberseguridad y el 90 % indica que pagaría para que un empleado obtuviera una certificación en ciberseguridad.

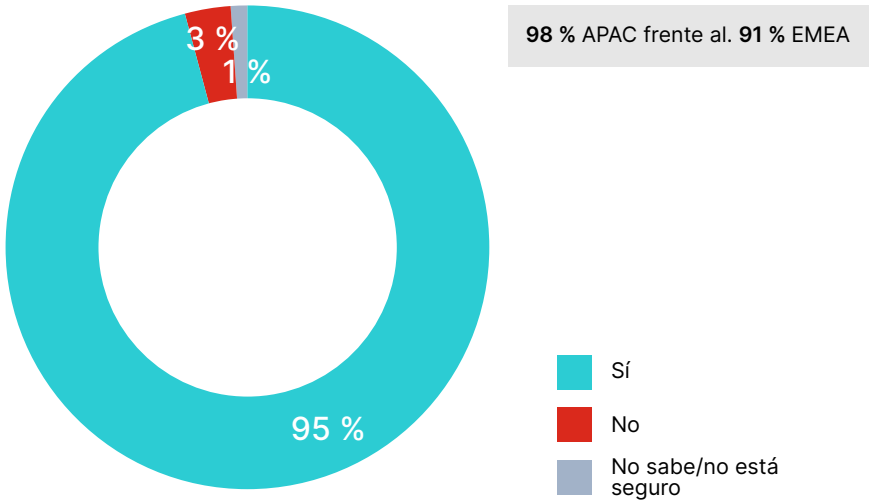
La necesidad de contar con profesionales certificados puede tener su origen en la experiencia del mundo real, ya que la mayoría de los líderes poseen una certificación en tecnología o trabajan con alguien de su equipo que la posee, lo que les permite comprender mejor el valor de obtener certificaciones. Otra hipótesis es que, con el creciente panorama de amenazas, los líderes dejan menos al azar y quieren la validación de que los profesionales que están reteniendo o contratando tienen las competencias en ciberseguridad requeridas.

El 90 % de los líderes prefiere contratar a personas con certificaciones centradas en la tecnología.

Las certificaciones aportan beneficios reales

Los líderes que poseen una certificación en tecnología, o que tienen a alguien en su equipo que la posee, indican que estar certificados tiene un impacto positivo en su función o en la de su equipo.

¿Considera que tener certificaciones centradas en la tecnología tiene un impacto positivo en su función o en la de su equipo?



98 % APAC frente al. **91 %** EMEA

*Solo se cuestionó a aquellos que personalmente tienen una certificación centrada en la tecnología o su equipo la tiene.

Profundizando

Más líderes prefieren contratar empleados con certificaciones centradas en la tecnología

La mayoría de los encuestados (90 %) indica que prefiere contratar a personas con certificaciones, frente al 81 % del año anterior. Del mismo modo, el 90 % estaría dispuesto a pagar para que los empleados obtuvieran la certificación.

- El 84 % tiene una certificación centrada en la tecnología.
- El 86 % tiene a alguien con una certificación en su equipo.
- El 73 % indica que sigue siendo difícil encontrar personas con certificaciones centradas en la tecnología, frente al 78 % de 2021.

Las certificaciones benefician tanto a organizaciones como a individuos

Casi todos los líderes (95 %) que tienen certificaciones o que tienen un empleado certificado en su equipo experimentaron resultados positivos.

- El 72 % indica haber aumentado sus conocimientos en ciberseguridad.
- El 62 % indica un mejor rendimiento de sus tareas.
- El 55 % indica que la certificación aceleró el crecimiento de su carrera, frente al 34 % en 2021.
- El 47 % indica remuneraciones más altas, frente al 29 % en 2021.

Las certificaciones ocupan un lugar destacado junto con la concientización y la capacitación en ciberseguridad, y las soluciones de seguridad

La estrecha clasificación de las tres opciones por parte de los encuestados demuestra que un enfoque triple puede ser la mejor línea de defensa contra los ciberataques.

- El 82 % indica que su organización se beneficiaría de la capacitación en ciberseguridad en forma de certificaciones.
- El 75 % indica que su organización se beneficiaría de la concientización y capacitación en ciberseguridad para todos los empleados.
- El 71 % indica que su organización se beneficiaría de soluciones de seguridad nuevas, mejores o adicionales.

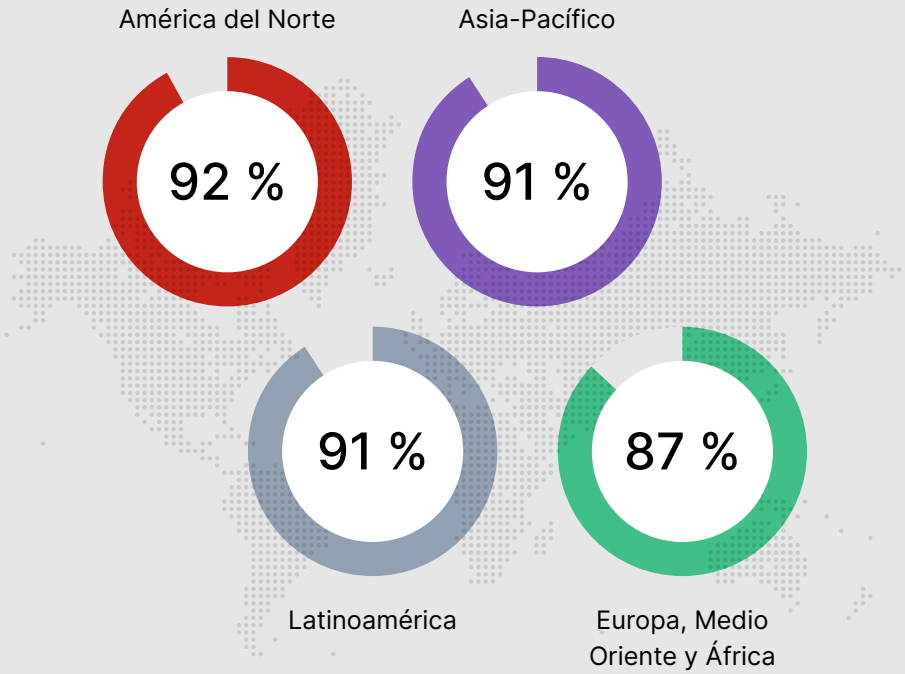
El 90 % de los líderes estaría dispuesto a pagar para que sus empleados obtengan la certificación.

Hechos destacados regionales

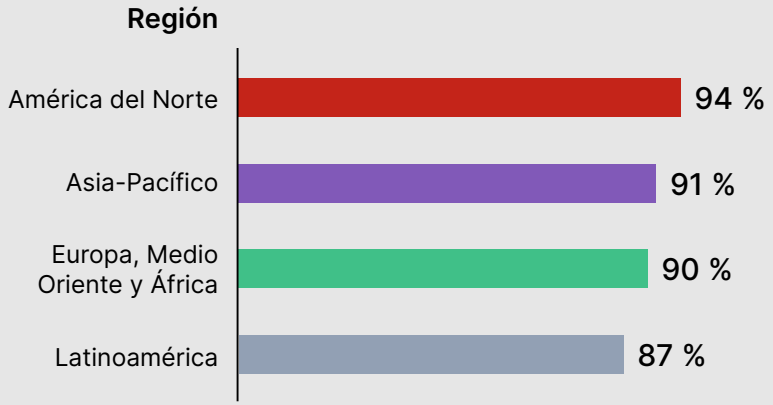
Las organizaciones de todo el mundo valoran la certificación

Las empresas norteamericanas tienen el mayor número de encuestados que prefieren contratar a personas con certificaciones centradas en la tecnología y están dispuestas a pagar por ello.

Prefiere contratar personal certificado



Dispuesto a pagar para que los empleados obtengan la certificación



Puestos de TI vacantes: un riesgo para la ciberseguridad

Más de la mitad de los líderes indican que tienen dificultades para reclutar y retener a los expertos en ciberseguridad, lo que genera una escasez de competencias que plantea riesgos cibernéticos adicionales para sus organizaciones.

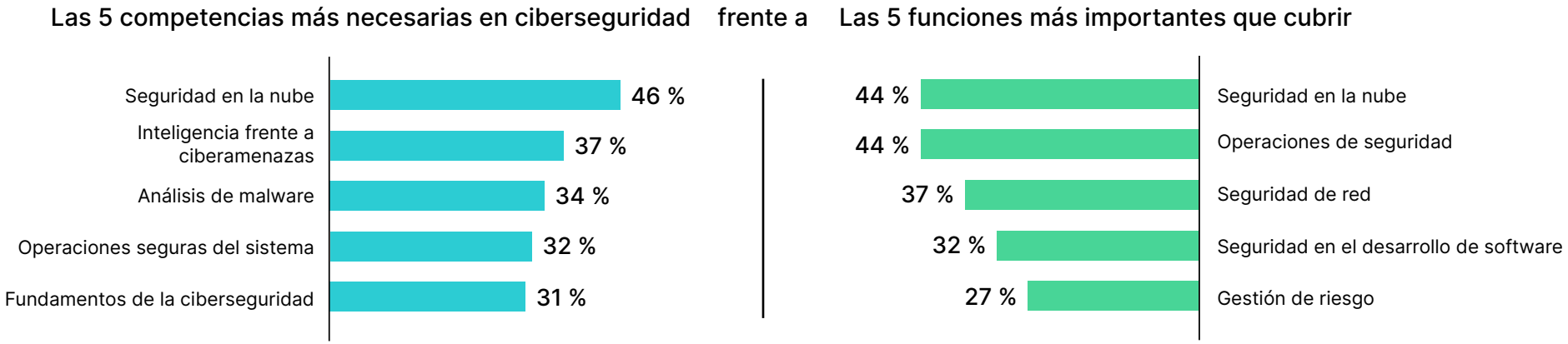
El reclutamiento y la retención son retos esencialmente equivalentes, siendo las competencias más necesarias en las áreas de seguridad en la nube, inteligencia frente a ciberamenazas y análisis de malware. Entre las funciones específicas que están resultando difíciles de cubrir se encuentran la seguridad en la nube, las operaciones de seguridad y la seguridad de red.

Dada la carga a la que se ven sometidos actualmente los equipos de ciberseguridad para hacer frente a miles de alertas diarias, administrar herramientas dispares y proteger un perímetro de red cada vez más disperso debido a las tecnologías en la nube y los modelos de trabajo híbridos, esta escasez de competencias es significativa.

El 68 % de las organizaciones indican que se enfrentan a riesgos adicionales debido a la escasez de competencias en ciberseguridad.

Lo que más se necesita son conocimientos en ciberseguridad en la nube.

La seguridad en la nube encabeza la lista de las competencias en ciberseguridad más necesarias y los puestos más difíciles de cubrir para las organizaciones.



Profundizando

La escasez en ciberseguridad aumenta el riesgo

Sesenta y ocho por ciento (68 %) de los líderes están de acuerdo en que la escasez de competencias en ciberseguridad crea riesgos cibernéticos adicionales para su organización, similar al 67 % en 2021.

- El 28 % está muy de acuerdo con esta declaración.
- Solo el 7 % está totalmente en desacuerdo con esta declaración.

El reclutamiento y la retención son igual de difíciles

Más de la mitad (56 %) de los encuestados indican que sus organizaciones luchan por reclutar personal especializado en ciberseguridad, un poco menos que el 60 % en 2021.

La mayoría (54 %) indica que la retención también es un desafío, un poco más que el 52 % del año pasado.

- El 44 % indica que tanto las funciones de seguridad en la nube como las de operaciones de seguridad son los más difíciles de cubrir.
- El 37 % indica que las funciones de seguridad de red son las más difíciles de cubrir.
- El 32 % indica que las funciones de desarrollo de software son las más difíciles de cubrir.

Las competencias de seguridad en la nube son las más necesarias en casi la mitad de las organizaciones

Los líderes identificaron las siguientes competencias como muy necesarias para sus organizaciones.

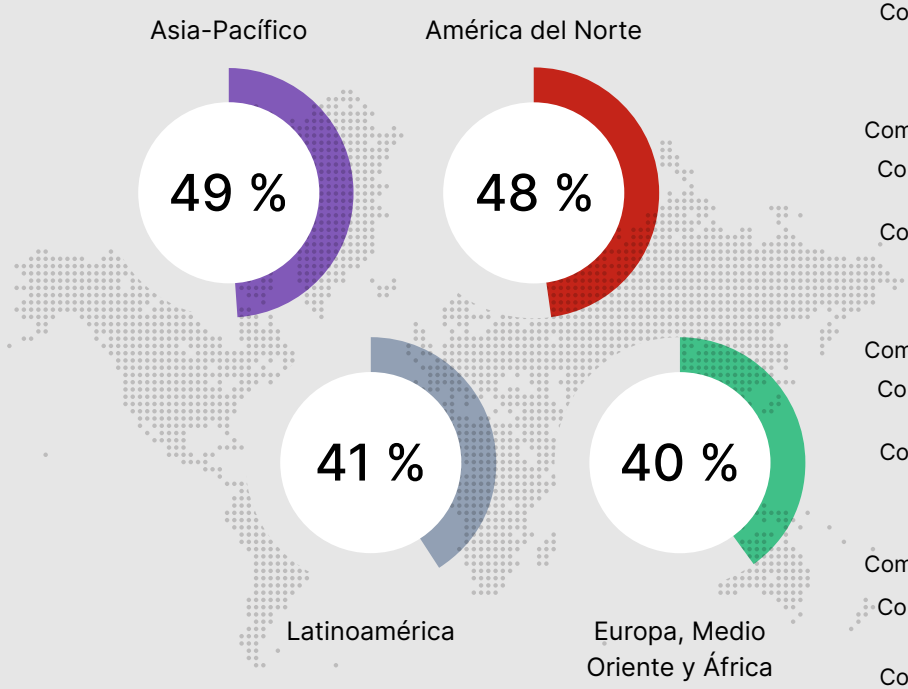
- El 46 % informa la necesidad de competencias de seguridad en la nube.
- El 37 % indica que lo que más necesita son competencias de inteligencia frente a ciberamenazas.
- El 34 % indica que lo que más necesita son competencias de análisis de malware.

El 46 % informa la necesidad de competencias de seguridad en la nube.

Hechos destacados regionales

Algunas regiones tienen más dificultades para cubrir funciones de seguridad en la nube

Las organizaciones de las regiones de Asia-Pacífico y América del Norte se enfrentan a mayores desafíos para cubrir funciones de seguridad en la nube en comparación con sus homólogas de Latinoamérica y Europa, Medio Oriente y África.



Las distintas regiones requieren competencias diferentes

Aunque las organizaciones de todas las regiones indican que necesitan competencias de seguridad en la nube, las de América del Norte son mucho más propensas a necesitar también competencias de inteligencia frente a ciberamenazas mientras que las de Latinoamérica necesitan sobre todo competencias de análisis de malware.

La diversidad de talento puede ayudar a cubrir las necesidades de competencias, pero no siempre es fácil de encontrar

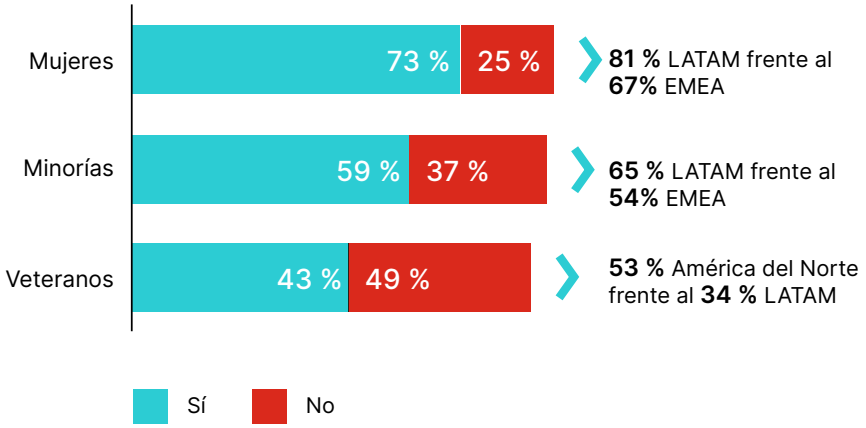
La mayoría de las organizaciones (83 %) tienen objetivos de diversidad para la contratación en los próximos dos o tres años. Recurrir a fuentes de talento históricamente ignoradas puede ayudar a colmar brechas de competencias ampliando el conjunto de candidatos potenciales. Sin embargo, en algunos casos sigue siendo difícil encontrar personas debidamente calificadas.

Las organizaciones constantemente buscan expertos en ciberseguridad procedentes de diversas fuentes, en particular mujeres, grupos minoritarios y veteranos militares. A menudo se considera que este último grupo ya tiene la capacitación, orientación y disciplina adecuadas para trabajar en un contexto de ciberseguridad.

De las tres fuentes de talento, la mayoría de los responsables de la toma de decisiones de TI consideran que encontrar y contratar mujeres calificadas es el principal desafío, considerablemente más difícil que contratar a minorías y veteranos.

Aproximadamente el 40 % de las organizaciones indican que tienen dificultades para encontrar candidatos calificados que sean mujeres, veteranos militares o pertenezcan a minorías.

¿Tiene alguna iniciativa de reclutamiento estructurada o formal que se dirija específicamente a los siguientes grupos de población?



Más iniciativas de reclutamiento dirigidas a las mujeres.

Para atraer diversidad de talento, muchas organizaciones mantienen iniciativas de reclutamiento dirigidas a mujeres (73 %) y candidatos de poblaciones minoritarias (59 %). Sin embargo, entre 2021 y 2022, las iniciativas similares para veteranos cayeron del 51 % al 43 %.

Profundizando

La mayoría de las organizaciones tienen objetivos de diversidad, pero tienen dificultades para contratar

El ochenta y tres por ciento (83 %) de las organizaciones encuestadas tienen objetivos de contratación de diversidad a corto plazo, un poco menos que el 89 % en 2021.

- El 69 % indica que la contratación de mujeres es un desafío importante, manteniéndose en el 70 % en 2021.
- El 56 % indica que la contratación de personas procedentes de minorías es un desafío importante, frente al 61 % en 2021.
- El 43 % indica que la contratación de veteranos es un desafío importante, frente al 53 % en 2021.

Parte del desafío consiste en encontrar candidatos calificados y diversos

Los encuestados indican que el reclutamiento de candidatos calificados de los tres grupos subrepresentados es igual de difícil.

La mayoría (54 %) indica que la retención también es un desafío, un poco más que el 52 % del año pasado.

- El 43 % indica dificultades para reclutar veteranos calificados, un ligero descenso respecto al 45 % de 2021.
- El 41 % indica que tiene dificultades para reclutar mujeres candidatas calificadas, una cifra significativamente superior al 30 % del año pasado.
- El 38 % indica que tiene dificultades para reclutar a personas cualificadas procedentes de minorías, porcentaje que no varió desde el año pasado.

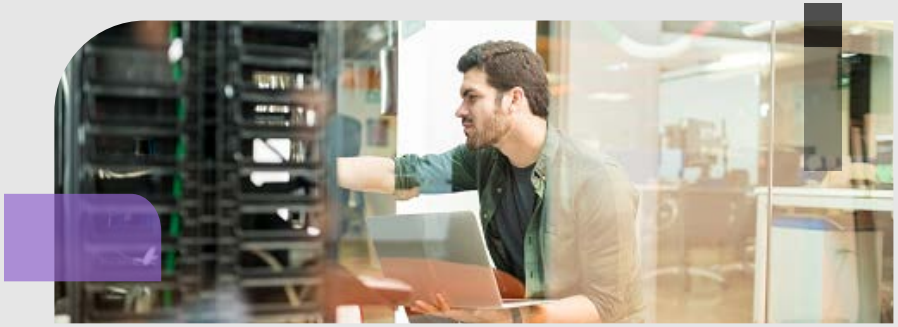
A pesar de los desafíos, la diversidad en la contratación es una realidad

Muchas organizaciones contrataron a personas de los tres grupos, especialmente mujeres.

- El 89 % de los encuestados contrata activamente a mujeres, casi lo mismo que el año pasado (88 %).
- El 68 % contrató a personas pertenecientes a minorías, cifra similar a la de 2021 (67 %).
- El 47 % contrató a veteranos militares, un descenso con respecto al 53 % del año anterior.

El 83 % de las organizaciones encuestadas tienen objetivos de contratación de diversidad a corto plazo, un poco menos que el 89 % en 2021.

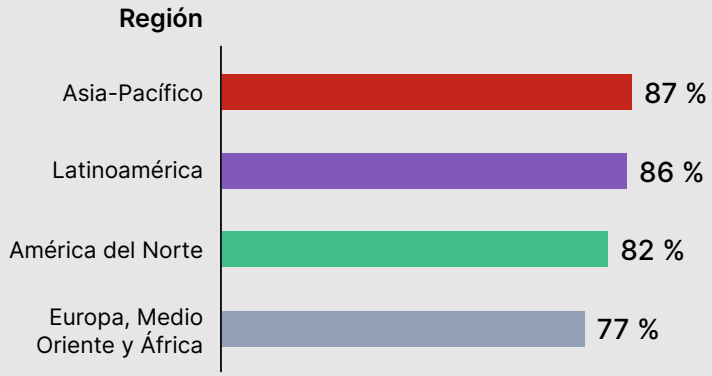
Hechos destacados regionales



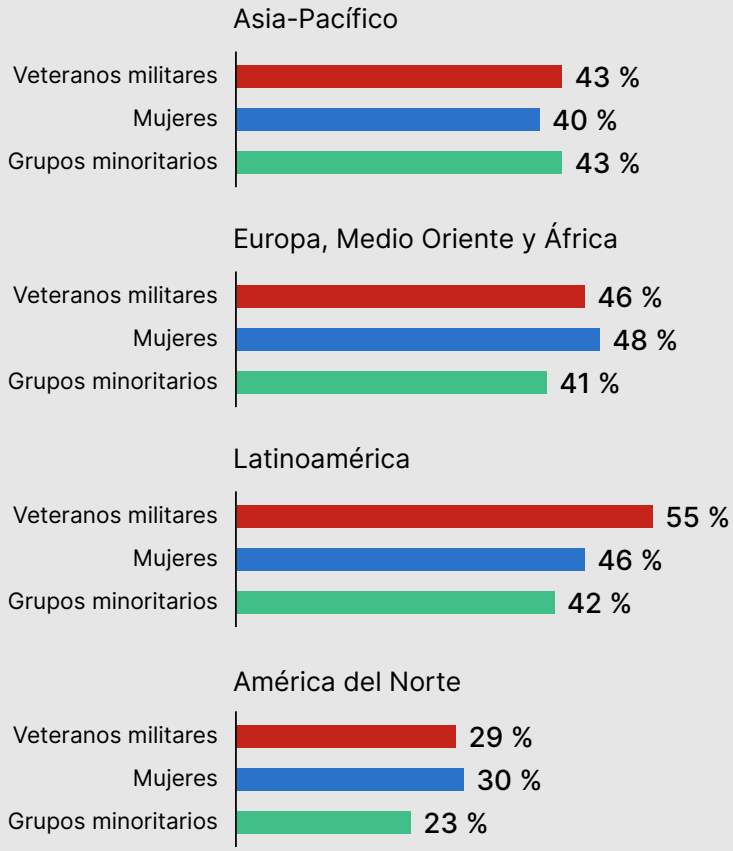
En todas las regiones, las organizaciones se enfrentan a diferentes desafíos en materia de RR. HH.

Las empresas de la región Asia-Pacífico y de Latinoamérica son las más propensas a tener objetivos de contratación de diversidad para los próximos dos o tres años. Región por región, la contratación de grupos subrepresentados es más difícil.

Objetivos de contratación en materia de diversidad por región



Desafíos en la contratación de diferentes grupos



Conclusión

El panorama de las amenazas en evolución y la creciente incidencia de las violaciones de seguridad hacen imperativo que las organizaciones sigan construyendo su defensa de ciberseguridad para proteger sus redes, sistemas, datos, clientes, socios y empleados. Al considerar sus estrategias de ciberseguridad, los líderes deben tener en cuenta tres factores:

- **Soluciones avanzadas** para hacer frente a las amenazas en tiempo real en entornos TI complejos y distribuidos
- **Equipos de expertos** con los conocimientos y competencias necesarios para administrar eficazmente la ciberseguridad
- **Una cultura de ciberconciencia** para cada individuo de su organización

Mayor interés de las juntas corporativas

Las juntas corporativas de las empresas están prestando más atención al riesgo cibernético y a los factores humanos asociados, lo que genera más conversaciones a nivel directivo sobre lo que se está haciendo para mitigar el riesgo. Las conversaciones específicas sobre el aumento del tamaño de los equipos de seguridad de TI están empujando a las organizaciones a prestar más atención. Este aumento de la atención a nivel directivo probablemente impulsará a las organizaciones a redoblar sus esfuerzos para reclutar y retener a empleados calificados y desarrollar una estrategia de contratación para las competencias en ciberseguridad necesarias y difíciles de encontrar, especialmente con el creciente reconocimiento de que las competencias no cubiertas crean un riesgo adicional para muchas organizaciones. Los líderes que necesiten demostrar a sus juntas que son conscientes del estado actual y futuro del panorama de las amenazas querrán adelantarse a estas conversaciones en curso.

El 48 % de las organizaciones que sufrieron al menos una violación de seguridad en los últimos 12 meses indican que costó más de USD 1 millón remediarla, frente al 38 % en 2021.

Las certificaciones cobran protagonismo

Tanto si se trata de contratar a nuevos empleados como de mejorar los conocimientos del personal de seguridad de TI existente, los líderes recurren cada vez más a las certificaciones para validar las competencias individuales. Los programas de certificación bien diseñados tienen como objetivo establecer no solo las competencias técnicas, sino también una comprensión más profunda de cómo aplicar esas competencias en el contexto de una función determinada.

Invertir en las personas suele reforzar el compromiso de los empleados. Fortinet considera que invirtiendo y desarrollando su actual fuerza laboral de seguridad de TI, las organizaciones pueden reducir los problemas de retención de talento. Animando y apoyando a los empleados para que obtengan o renueven sus certificaciones, las organizaciones pueden aumentar la lealtad de los empleados, aumentar la retención y garantizar que las competencias de los individuos se mantengan actualizadas.

Búsqueda de talento en nuevos lugares

La ampliación de la reserva de talento para atraer a grupos más diversos seguirá siendo fundamental para que las organizaciones puedan satisfacer sus necesidades de personal. En 2021, se estimaba que las mujeres representaban solo una cuarta parte de la fuerza laboral mundial en ciberseguridad.[3] Aunque las poblaciones minoritarias varían según el país y la región, parece generalmente cierto que estos grupos están subrepresentados en el campo de la ciberseguridad. En EE. UU., por ejemplo, solo el 9 % de los expertos en ciberseguridad son negros, el 8 % asiáticos y el 4 % hispanos.[4]

Los veteranos militares suelen tener la ventaja única de poseer ya una mentalidad de defensa y están bien formados para aprender nuevas competencias y pasar de una función a otra. El sector tiene mucho que ganar atrayendo a personas de este grupo y aprovechando su formación y competencias, tanto técnicas como interpersonales.

La cultura de la empresa cuenta

Además de las tecnologías y los especialistas en ciberseguridad, los líderes disponen de otra poderosa herramienta para protegerse: una cultura interna de ciberseguridad sólida. Los líderes pueden cultivar una cultura fuerte aumentando la concientización de los empleados sobre la necesidad de una buena higiene de ciberseguridad. Para más información sobre la concientización de los empleados en ciberseguridad, lea nuestro informe complementario: the Resumen de investigación de capacitación y concientización en seguridad de 2023, que se publicará esta primavera.

La buena noticia es que se sigue avanzando en la lucha contra el cibercrimen y las organizaciones que se comprometieron a reforzar su postura de seguridad no están solas. Desde la Asociación contra el Cibercrimen (PAC) del Foro Económico Mundial hasta la Asociación Cibernética de la Industria de la OTAN y el MITRE Engenuity Center for Threat-Informed Defense, muchos organismos gubernamentales están comprometidos con la protección de las empresas frente a las ciberamenazas. En Fortinet estamos orgullosos de contribuir activamente a muchas de estas iniciativas

[3] Tayo Bero, "Cybersecurity is a red-hot career choice – why aren't more women working in this space?" The Globe and Mail, 24 de agosto de 2022.
[4] Ben Allen, "Minorities and the Cybersecurity Skills Gap", Forbes, 30 de septiembre de 2022.

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 hacer que la capacitación en ciberseguridad y las nuevas oportunidades profesionales estén al alcance de todos. FortiGuard Labs, la organización de investigación e inteligencia frente a amenazas de élite de Fortinet desarrolla y usa tecnologías de aprendizaje automático e IA de vanguardia para brindar a los clientes protección oportuna y consistente de primera categoría e inteligencia práctica frente a amenazas. Obtenga más información en www.fortinet.com, el Fortinet Blog y FortiGuard Labs.

FORTINET
Training Institute

www.fortinet.com/lat

Marzo 2023

Resumen ejecutivo

Las conclusiones de este informe sobre la brecha de competencias en ciberseguridad 2023 muestran claramente que las organizaciones están librando una ardua batalla contra las ciberamenazas: sufren más violaciones de seguridad, necesitan profesionales cualificados y siguen luchando por cubrir puestos clave.

Las violaciones de seguridad son más frecuentes y costosas

El **84 %** de las organizaciones experimentaron **una o más violaciones de seguridad** en los últimos 12 meses, frente al 80 % en 2021.

El **29 %** experimentó **cinco o más intrusiones**, frente al 19 % del año anterior.

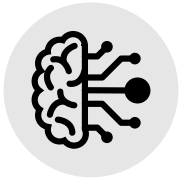
El **48 %** experimentó violaciones de seguridad en los últimos 12 meses cuya **reparación costó más de USD 1 millón,** frente al 38 % en 2021.

Puestos de TI vacantes: un riesgo para la ciberseguridad

El **68 %** de las organizaciones indican que se **enfrentan a riesgos** adicionales debido a la escasez de competencias en ciberseguridad, en consonancia con el 67 % en 2021.

El **56 % tiene dificultades para reclutar** y el **54 % para retener el** talento, frente al 60 % y el 52 % en 2021.

La seguridad en la nube y las operaciones de seguridad son los puestos más difíciles de cubrir.



Las juntas directivas se centran en la ciberseguridad

El **93 %** de los encuestados indica que su **junta directiva se interesa por la ciberseguridad,** frente al 88 % en 2021.

En 2022, **el 83 % de las juntas sugirió aumentar el personal de seguridad de TI,** en comparación con el 76 % en 2021.

Certificaciones como prueba de conocimientos y competencias en ciberseguridad

El **90 %** de los líderes **prefiere contratar a personas con certificaciones centradas en la tecnología,** frente al 81 % en 2021.

El **90 % también pagaría** para que un empleado obtuviera una certificación en ciberseguridad.

El **72 %** de los líderes indican que la contratación de personas certificadas **aumentó la concientización** y los conocimientos sobre seguridad dentro de su organización.

La diversidad puede ayudar a cubrir las necesidades de competencias, pero no siempre es fácil de encontrar

Aproximadamente el **40 %** tiene **dificultades para encontrar candidatos calificados** que sean mujeres, veteranos militares o pertenezcan a minorías.

El **83 %** de las organizaciones **tienen objetivos de contratación de diversidad a corto plazo,** frente al 89 % en 2021.