FORTINET
Training Institute

Brecha de Competencias en Ciberseguridad 2024

Informe de Investigación Global

Contenido

Metodología

Los hallazgos de este informe se basan en las respuestas obtenidas de las entrevistas en línea y una encuesta por correo electrónico a 1850 responsables de la toma de decisiones de TI y ciberseguridad realizada por Sapio Research en enero de 2024. La encuesta y las entrevistas se realizaron en las siguientes 29 ubicaciones:

- Argentina
- Australia
- Brazil
- Canada
- Colombia
- France
- Germany
- Hong Kong
- India
- Indonesia
- Israel
- Italy
- Japan
- Mainland China
- Malaysia
- Mexico
- Netherlands
- New Zealand
- Philippines
- Singapore
- South Africa
- South Korea
- Spain
- Sweden
- Taiwan
- Thailand
- United Arab Emirates
- United Kingdom
- United States of America

Los resultados generales son precisos para ± 2.3 % a un límite de confianza del 95 %.

Tamaño de la empresa

100 a 499 empleados **24%**
500 a 999 empleados **23%**
1,000 a 2,499 empleados **21%**
2,500-4,999 empleados **17%**
5,000+ empleados **14%**

Gender

68% de los encuestados eran hombres

32% de los encuestados eran mujeres

Total de encuestados: 1,850

Asia Pacífico **30%**
Europa, Medio Oriente y África **27%**
Norteamérica **22%**
Latinoamérica **22%**

Tipo de función

El **13 %** de los encuestados ocupó puestos de propietario

El **34 %** de los encuestados ocupó puestos ejecutivos de nivel C

El **9 %** de los encuestados ocupó puestos de vicepresidente

El **11 %** de los encuestados ocupaba puestos principales

El **33 %** de los encuestados ocupó puestos de director

Los tres principales sectores empresariales:

Tecnología **21%**
Fabricación **15%**
Servicios financieros **13%**

Resumen ejecutivo

Con respecto a la ciberseguridad en 2024, los riesgos son altos para Organizaciones de resumen ejecutivo. Las violaciones continúan afectando las finanzas y los líderes sénior son sancionados cuando ocurren. En respuesta, las organizaciones se enfocan en un enfoque triple de ciberseguridad que combina capacitación, concientización y tecnología.

Los líderes corporativos son responsables

El **51%** de los encuestados dice que los directores o ejecutivos han enfrentado multas, tiempo en la cárcel, pérdida de puesto o pérdida de empleo después de un ciberataque.

Para mejorar la ciberseguridad, las juntas han analizado o implementado las siguientes medidas:

- Capacitación o certificaciones obligatorias para el personal de TI/seguridad **(64%)**
- Capacitación sobre concientización en ciberseguridad para todo el personal **(61%)**
- Compra de soluciones de seguridad **(59%)**

El **72%** de los encuestados afirma que sus juntas directivas se centraron más en la ciberseguridad en 2023 que el año anterior.

Las violaciones consumen tiempo y dinero valiosos

El **87%** de los encuestados informa que experimentó una o más violaciones de seguridad en 2023.

El **63%** de los encuestados dice que le llevó más de un mes recuperarse de un ciberataque.

El **53%** de los encuestados dice que las violaciones les cuestan más de USD 1 millón en pérdidas de ingresos, multas y otros gastos. Esto es superior al 48 % en 2022 y al 38 % en 2021.

Ciberseguridad depende de tres factores clave

Los líderes de TI dicen que las tres principales causas de violaciones son:

- Un personal de TI/seguridad que carece de las habilidades y la capacitación necesarias **(58%)**
- Falta de concientización sobre la seguridad de la organización o de los empleados **(56%)**
- Falta de productos de ciberseguridad **(54%)**

El **70%** de los encuestados está de acuerdo en que la escasez de competencias en ciberseguridad crea riesgos adicionales para sus organizaciones.

El **62%** de los responsables de la toma de decisiones de TI dicen que el mayor desafío es encontrar candidatos con experiencia específica en ingeniería y seguridad de redes.

Candidatos con certificaciones sobresalen

El **91%** de los encuestados prefiere contratar candidatos con certificaciones.

El **89%** de los encuestados pagaría para que un empleado obtuviera una certificación de ciberseguridad.

El **72%** de los encuestados dice que es difícil encontrar candidatos con certificaciones centradas en la tecnología, un poco menos que en 2022 (73%) y un poco menos que el 78% en 2021.

Las organizaciones pueden pasar por alto a los candidatos de orígenes subrepresentados

El **83%** de las empresas ha establecido objetivos de contratación de diversidad para los próximos años.

El **71%** requiere títulos de cuatro años y el 66 % solo contrata candidatos con formación tradicional.

A pesar de los objetivos continuos, la diversidad de contratación varía de un año a otro:

- Las contrataciones activas de mujeres disminuyeron al 85% frente al 89 % en 2022 y al 88% en 2021.
- Las contrataciones activas de grupos minoritarios no han cambiado en un 68% y subieron ligeramente desde el 67% en 2021.
- Las contrataciones activas de veteranos aumentaron un poco a un 49% frente al 47% en 2022, pero disminuyeron frente al 53% en 2021.

INTRODUCCIÓN

Ciberseguridad requiere un enfoque integral

El Informe de brecha de competencias en Ciberseguridad del año pasado indicó que las juntas directivas se interesaban más en la ciberseguridad. El informe de 2024 incluye nuevas preguntas, diseñadas para profundizar, que revelan por qué este es el caso y destacan el enfoque cada vez más holístico de las empresas para combatir las ciberamenazas.

Al redactar este informe, analizamos los desafíos de las habilidades de ciberseguridad a través de cinco objetivos: las prioridades de los líderes empresariales, el panorama de amenazas, las estrategias de ciberseguridad, el valor de las certificaciones y la contratación de diversos grupos de talento.

Lo que encontramos es que la creciente frecuencia de los costosos ciberataques, combinada con el potencial de graves consecuencias personales para los miembros de la junta directiva y los directores, está dando lugar a un impulso urgente para fortalecer las ciberdefensas que provienen de arriba hacia abajo.

El informe de este año incluye estadísticas comparativas, para algunas preguntas, que se remontan a 2021 y profundiza en los temas clave para crear una imagen más completa del estado de la brecha de habilidades en la actualidad. También incluye detalles adicionales relacionados con la visión a nivel de junta de ciberseguridad y nuevos datos sobre los efectos de las violaciones y detalles sobre cómo las organizaciones planean responder a esos efectos.

Está claro que todavía quedan por resolver algunos desafíos persistentes. La brecha de competencias en ciberseguridad sigue afectando a la industria. Además, el reclutamiento y la retención de empleados con el conjunto de competencias requerido sigue siendo difícil para la mayoría de los encuestados. Esto puede deberse, en parte, a su subutilización continua de grupos de talento no tradicionales y a los requisitos de credenciales "tradicionales".

La conclusión general es que la ciberseguridad efectiva requiere un enfoque triple:

1. **Ayude a los equipos de TI y seguridad** a obtener habilidades vitales de ciberseguridad invirtiendo en la capacitación y las certificaciones necesarias para lograr este objetivo.
2. **Cultive a un personal de primera línea ciberconsciente** que pueda contribuir a la seguridad como primera línea de defensa.
3. **Obtenga y utilice soluciones de ciberseguridad** efectivas para garantizar una **postura de seguridad** sólida.

51% de las organizaciones dicen que los líderes sénior han enfrentado multas, tiempo en la cárcel, pérdida de puesto o pérdida de empleo después de un ciberataque.

Los líderes corporativos son considerados responsables

En la actualidad, las juntas directivas se interesan más en la ciberseguridad y su interés puede estar motivado personalmente. Un poco más de la mitad (51 %) de los encuestados dicen que los directores o ejecutivos han enfrentado multas, tiempo en prisión, pérdida de puesto o pérdida de empleo después de un ciberataque.

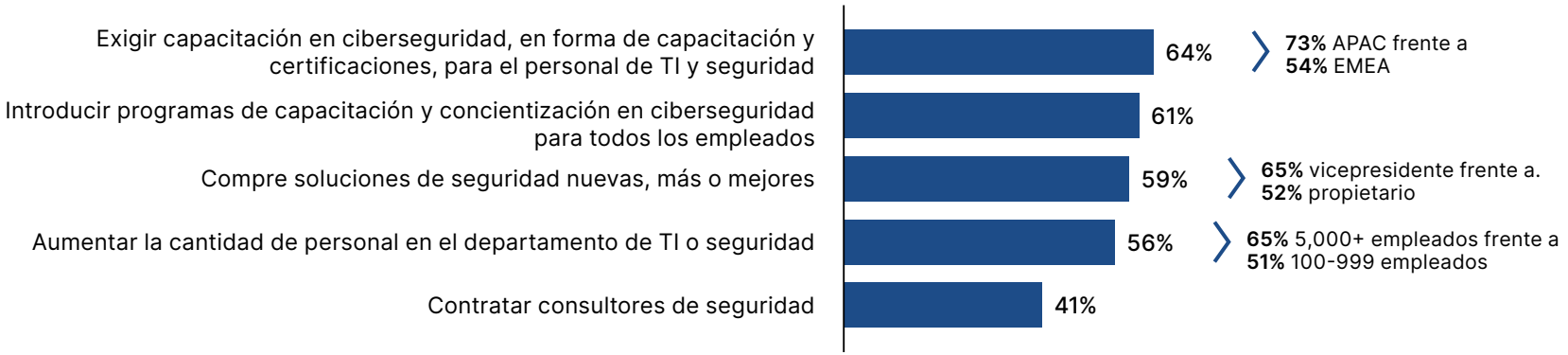
Dados esos riesgos, no es sorprendente que casi tres cuartas partes (72 %) de los encuestados digan que sus juntas directivas se enfocaron más en la ciberseguridad en 2023 que en el año anterior. Las mejoras que las juntas analizaron o implementaron incluyen capacitación o certificaciones obligatorias en ciberseguridad para el personal de TI y seguridad (64 %), capacitación en concientización sobre seguridad para todos los empleados (61 %) y la compra de soluciones de seguridad nuevas, más o mejores (59 %).

Estas mejoras se alinean con la opinión de los líderes de TI de que la falta de habilidades y personal capacitado, así como la falta de conocimiento y productos, son las principales causas de las violaciones de seguridad. Consulte la página 17 para obtener más información.

Prioridades de ciberseguridad de las juntas directivas: capacitación, concientización y soluciones

Los miembros de la junta directiva parecen reconocer que el conocimiento, las habilidades y la concientización son las primeras líneas vitales de una ciberdefensa sólida y que la tecnología es esencial para respaldarlos.

Mejoras que se analizan o implementan



PROFUNDIDAD DE LA DIAGRAMA

Las juntas ven Ciberseguridad como un imperativo empresarial

Las juntas están tomando medidas sobre ciberseguridad

El año anterior, el 93 % de los encuestados dijo que los miembros de su junta preguntaban sobre las ciberdefensas. La encuesta de este año profundiza en los aspectos en los que se enfocan las juntas de ciberseguridad.

- El 97 % de los encuestados dice que su junta considera que la ciberseguridad es una prioridad empresarial.
- El 56 % dice que su junta directiva ha discutido o implementado un aumento del personal de TI/seguridad.

Los líderes se enfrentan a sanciones en organizaciones de todos los tamaños

El riesgo de sanciones para los miembros de la junta directiva o los ejecutivos es casi el mismo en todas las organizaciones.

- En el extremo más alto, el 59 % de las organizaciones con entre 2,500 y 4,999 empleados informan que los líderes de sus organizaciones enfrentaron sanciones después de los ciberataques.
- El 48 % de las organizaciones pequeñas (de 100 a 999 empleados) y el 48 % de las organizaciones muy grandes (más de 5,000 empleados) informan que sus líderes también se enfrentaron a sanciones.

Las multas son la sanción más común para los líderes

La mayoría de los miembros de la junta directiva y ejecutivos de la empresa que fueron responsables recibieron sanciones financieras después de un ciberataque, aunque también se cumplieron otras consecuencias graves.

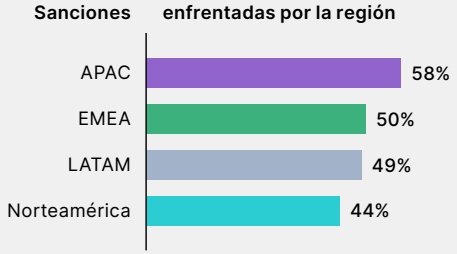
- El 34 % recibió multas.
- El 33 % perdió su puesto o su trabajo.
- El 16 % enfrentó penas de prisión.

EL 97% de los encuestados dicen que su la junta considera la ciberseguridad como prioridad empresarial.

Aspectos destacados regionales

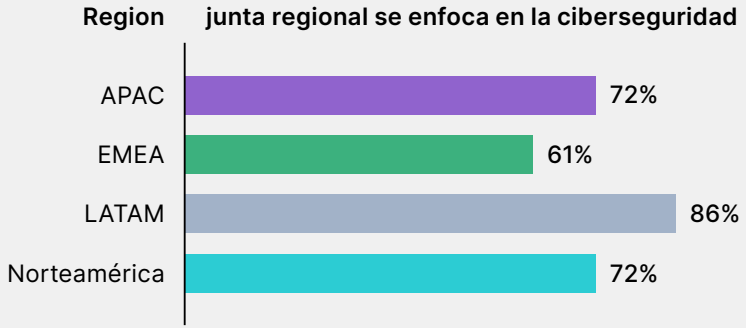
Los líderes de Asia-Pacífico tienen más probabilidades de enfrentar sanciones

Los ejecutivos y miembros de la junta directiva en la región Asia-Pacífico (APAC) tienen más probabilidades de enfrentar multas, tiempo en prisión, pérdida de puesto o pérdida de empleo después de un ciberataque.



Mayor enfoque de la junta directiva en la ciberseguridad más alta en Latinoamérica

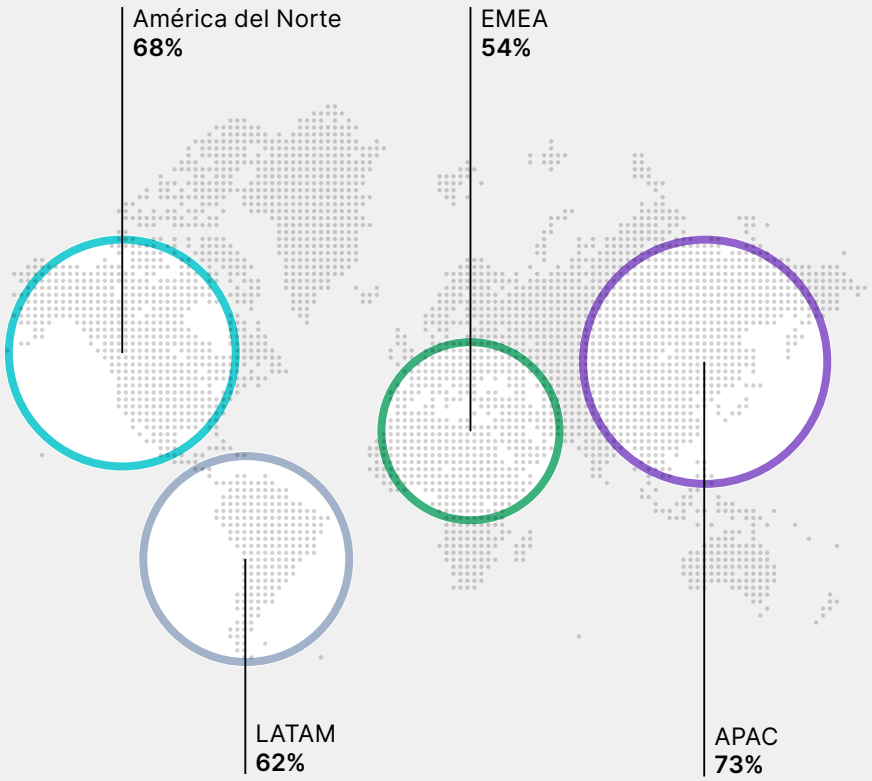
Las juntas directivas de Latinoamérica (LATAM) se centran más en la ciberseguridad en comparación con el año anterior, las juntas directivas de Europa, Medio Oriente y África (EMEA) son las menos.



Las juntas de APAC tienen más probabilidades de apoyar la capacitación obligatoria en ciberseguridad

El soporte de la junta directiva para la capacitación cibernética obligatoria para el personal de TI y seguridad fue más alto en APAC y más bajo en EMEA

Soporte de la junta directiva para la capacitación cibernética obligatoria



53% de los encuestados dice que las violaciones cuestanmás de **USD 1 millón** en 2023.

Las violaciones consumen tiempo y dinero valiosos

La gran mayoría (87 %) de las organizaciones dice que experimentó una o más violaciones de seguridad en 2023, con más de la mitad (53 %) que informó más de USD 1 millón en pérdidas de ingresos, multas y otros gastos, frente al 48 % en 2022 y el 38 % en 2021.

Un porcentaje menor de organizaciones informa que no experimenta ninguna violación de seguridad, solo el 13 % en 2023 en comparación con el 15 % del año anterior y el 20 % en 2021. Al mismo tiempo, las violaciones parecen tener más probabilidades de afectar las finanzas. Solo el 17 % de los encuestados de este año dice que los ciberataques no le han costado dinero a su organización, frente al 21 % en 2022 y al 36 % en 2021.

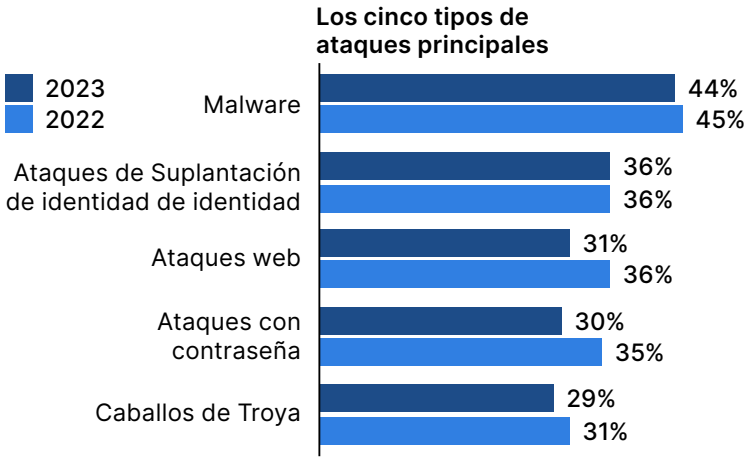
Las violaciones que informaron los encuestados fueron el resultado de muchos tipos diferentes de ataques. El malware, la suplantación de identidad y los ataques web combinados representan el 80 % de todos los ataques durante todo el año. Muchos de los tipos de ataques que se utilizan con más frecuencia se dirigen directamente a usuarios individuales, lo que destaca la importancia de la concientización general sobre seguridad.

Una o más violaciones de ciberseguridad

Cuenta combinada de malware, suplantación de identidad y ataques web para el **80%** de todos los ataques durante todo el año.

Un panorama de amenazas conocido

Los cinco principales ataques experimentados con más frecuencia en 2023 son los mismos que los del año anterior: malware, ataques de suplantación de identidad, ataques web, ataques de contraseñas y ataques de caballos de Troya.



El gráfico de la derecha muestra el resto de los ataques incluidos en la encuesta de este año. Los nuevos tipos de ataques agregados a este informe para el análisis de encuestas fueron: ataques externos a USB o medios físicos (16 %) y coerción y chantaje o soborno del personal interno (12 %).

PROFUNDIDAD DE LA DIAGRAMA

Recuperarse de un ataque es difícil

La recuperación puede llevar mucho tiempo

El tiempo promedio de recuperación de los encuestados fue de casi tres (2.7) meses.

- La mayoría (63 %) de las organizaciones necesitaban más de un mes para recuperarse de un ciberataque.
- El 35 % tardó entre uno y tres meses en recuperarse.
- Casi un tercio (28 %), la recuperación llevó cuatro meses o más.

Las empresas esperan que los ataques aumenten en número y frecuencia

Dada la intensificación y las crecientes consecuencias de los ataques, la mayoría de los encuestados espera que las cosas empeoren antes de mejorar

- El 80 % espera que los ciberataques aumenten durante el próximo año (frente al 65 % en 2022).
- Cuando se les preguntó cuánto pensaban que aumentarían los ataques, en promedio, los encuestados dicen que esperan un aumento del 19.3 % en los próximos 12 meses. Esto está aproximadamente a la par de 2022, cuando el promedio fue del 20 %.

El tamaño y la escala parecen atraer ataques

Las empresas de cierto tamaño y las de ciertas industrias tienden a informar que experimentan múltiples ciberataques.

36 % de las empresas con entre 1,000 y 2,499 empleados informaron cinco o más ataquesen los últimos 12 meses, frente al 35 % en 2022.

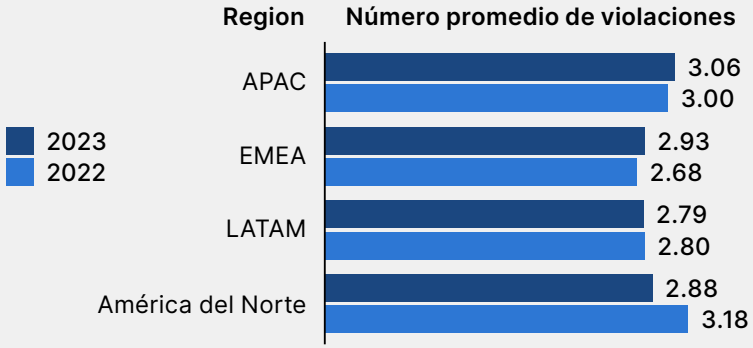
- 34 % de las empresas con entre 2,500 y 4,999 empleados informaron cinco o más ataques: frente al 38 % en 2022.
- Las empresas de petróleo y gas experimentaron la ocurrencia más alta de múltiples ataques de cualquier industria, con el 56 % citando cinco o más del 34 % en 2022.

En promedio, la recuperación de un ciberataque tarda **2.7 meses.**

Aspectos destacados regionales

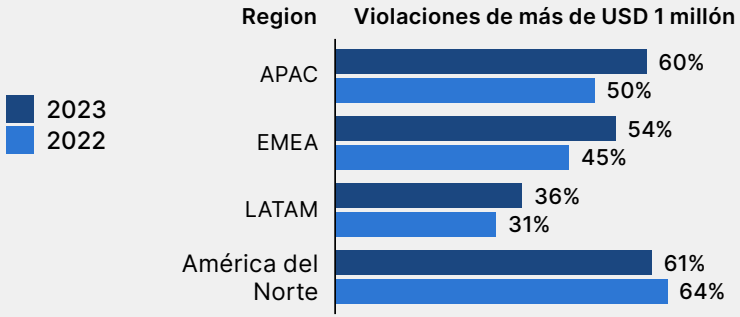
Las violaciones son igualmente comunes en todo el mundo

Si bien el promedio de APAC es ligeramente superior y los de LATAM es ligeramente inferior, todas las regiones informan un número promedio similar de violaciones.



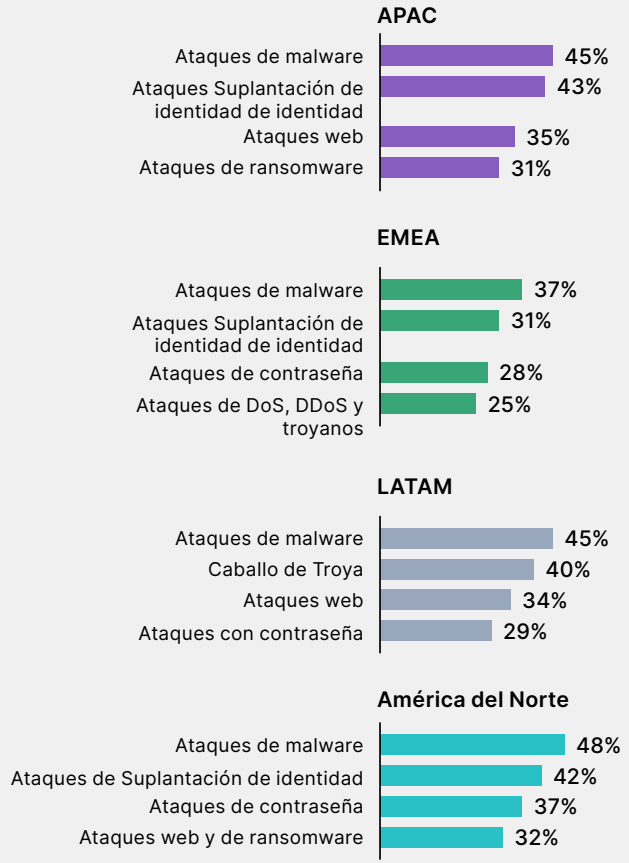
América del Norte y APAC tuvieron ataques más costosos

América del Norte y APAC continuaron informando los ataques más perjudiciales financieramente, con un costo de más de USD 1 millón en 2023. A excepción de América del Norte, todas las regiones observaron un aumento en los ataques más costosos en comparación con 2022.



Los principales tipos de ataque difieren ligeramente por región

Los ataques de malware fueron el tipo de ataque más común en todas las regiones. Los ataques de contraseña fueron más comunes en América del Norte que en cualquier otra región. Los encuestados de APAC experimentaron un mayor porcentaje de suplantación de identidad y ataques web que otras regiones.



58% de los responsables de la toma de decisiones de TI dicen que la principal causa de las violaciones de seguridad es el personal de TI/seguridad con un

Ciberseguridad depende de tres factores clave

Como dice el refrán, el conocimiento es poder. Por el contrario, la falta de conocimiento se consideraría una debilidad o, en el caso de la ciberseguridad, una responsabilidad importante. Mucho más de la mitad (58 %) de los encuestados dicen que las habilidades insuficientes y la falta de personal de TI/seguridad debidamente capacitado son las principales causas de las violaciones. Además, el 56 % señala una falta de concientización en ciberseguridad de la organización o de los empleados y el 54 % culpa a la falta de productos esenciales de ciberseguridad.

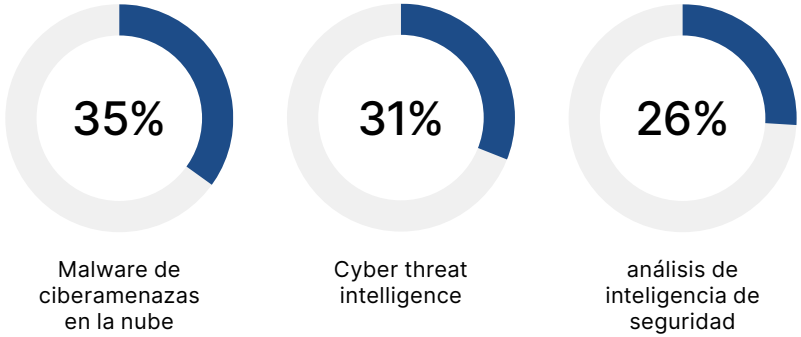
Dado que las habilidades técnicas, el personal y las soluciones de seguridad se consideran factores clave, tiene sentido que el 65 % de los líderes de TI digan que planean hacer crecer sus equipos de TI/seguridad en respuesta a experimentar un ciberataque.

Casi tantos (62 %) dicen que exigirán capacitación en ciberseguridad en forma de certificaciones para el personal de TI y seguridad. Casi tantos (61 %) dicen que introducirán programas de concientización y capacitación en ciberseguridad para todos los empleados, y la mayoría (59 %) también dicen que planean comprar más, más nuevas o mejores soluciones de seguridad.

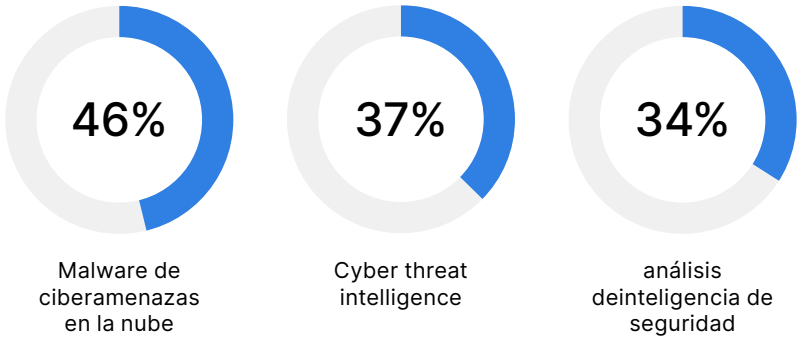
Las habilidades bajo demanda se mantienen relativamente estables

Entre 2022 y 2023, las tres principales habilidades de ciberseguridad en demanda se mantuvieron iguales en todas las organizaciones participantes. Si bien no hay una causa clara para el cambio en porcentajes, tenga en cuenta que se agregaron nuevas habilidades a la lista de 2023, que no estaban presentes en la encuesta anterior.

Las habilidades más necesarias en 2023



Las habilidades más necesarias en 2022



PROFUNDIDAD DE LA DIAGRAMA

Las personas son esenciales a Ciberseguridad

La escasez de competencias es una responsabilidad

El 70 % de los encuestados está de acuerdo en que la escasez de habilidades en ciberseguridad crea riesgos adicionales para sus organizaciones, un poco más que el 68 % en 2022 y el 67 % en 2021.

- El 62 % de los encuestados dice que es difícil encontrar candidatos con experiencia en ingeniería y seguridad de redes.
- Las funciones más difíciles de cubrir continúan siendo las operaciones de seguridad y la seguridad en la nube (43 %), un poco menos que el 44 % para ambos en 2022.

Los desafíos de reclutamiento se ven como un problema de suministro

A las organizaciones les resulta más fácil reclutar, aunque los desafíos persisten.

- El 54 % de las organizaciones dicen que tienen dificultades para reclutar talento en ciberseguridad. Estas cifras disminuyeron ligeramente desde el 56 % en 2022 y el 60 % en 2021, pero el reclutamiento de candidatos con experiencia en ciberseguridad sigue siendo un problema para más de la mitad de los encuestados.
- El 51 % de los encuestados dice que los grupos de talento para los conjuntos de habilidades requeridos son generalmente escasos.

Los empleados quieren aprender y crecer

Las presiones de retención pueden estar disminuyendo ligeramente porque los empleados valoran mucho la capacitación y la mejora de las competencias.

- Un poco menos de organizaciones (50 %) dicen que luchan por retener el talento en ciberseguridad en comparación con 2022 (54 %) y 2021 (52 %).
- El mayor desafío para la retención viene de la incapacidad de las organizaciones para ofrecer suficiente oportunidades de capacitación y mejora de competencias (50 %).
- Salario/beneficios (41 %) y trabajo remoto/híbrido

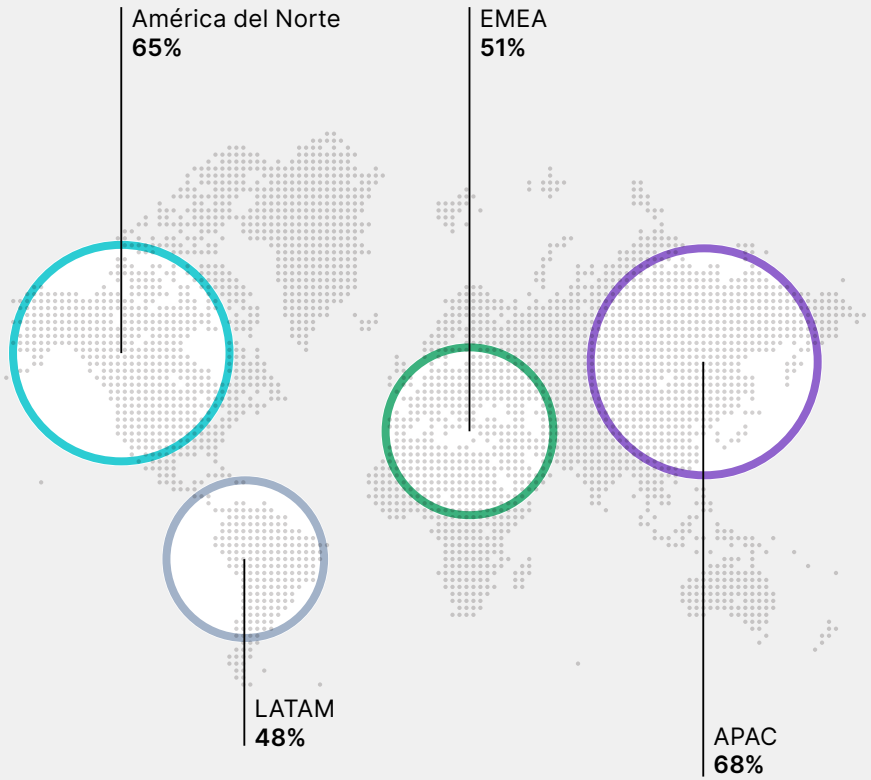
El 50% de los encuestados dice que la falta de capacitación y oportunidades de mejora de competencias es el mayor desafío de retención.

Aspectos destacados regionales

El vínculo entre las violaciones y las habilidades es más fuerte en APAC

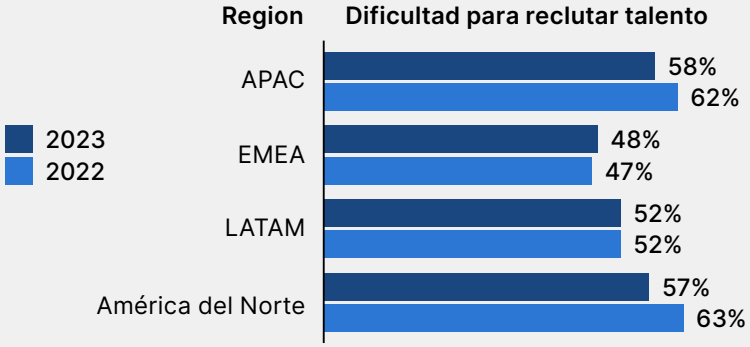
El 68 % de las empresas de APAC atribuyen las violaciones a la falta de habilidades y capacitación en ciberseguridad, en comparación con solo el 48 % de LATAM.

Atribuir las violaciones a la falta de habilidades y capacitación



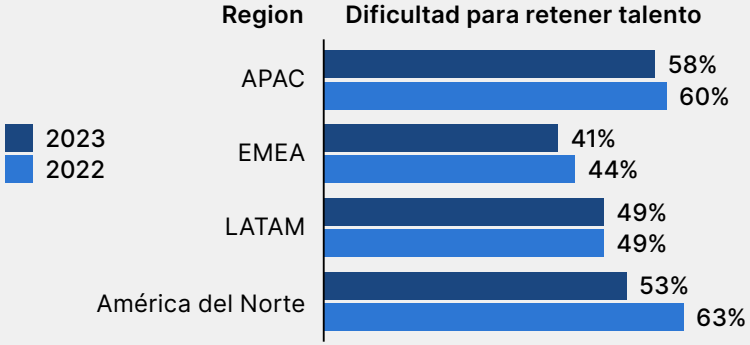
APAC y América del Norte tienen más dificultades con el reclutamiento

Esto sigue siendo el mismo que en 2022, aunque en porcentajes ligeramente más altos.



Las empresas de APAC informan más dificultades con la retención

Las organizaciones en América del Norte indican una disminución significativa en la dificultad para retener el talento en comparación con 2022. EMEA tuvo una leve disminución, mientras que LATAM se mantuvo igual.



EL **91%** de los líderes prefiere contratar candidatos con certificaciones.

Los candidatos con certificaciones se destacan

Los líderes de TI consideran ampliamente las certificaciones como distintivos de conocimientos de ciberseguridad. Casi todos (91 %) prefieren contratar candidatos con certificaciones, una cifra que está en línea con 2022 y un aumento del 10 % con respecto a 2021. La mayoría (67 %) de los encuestados prefiere que los miembros del equipo o los subordinados directos tengan certificaciones porque creen que estas credenciales validan el conocimiento y la concientización en ciberseguridad.

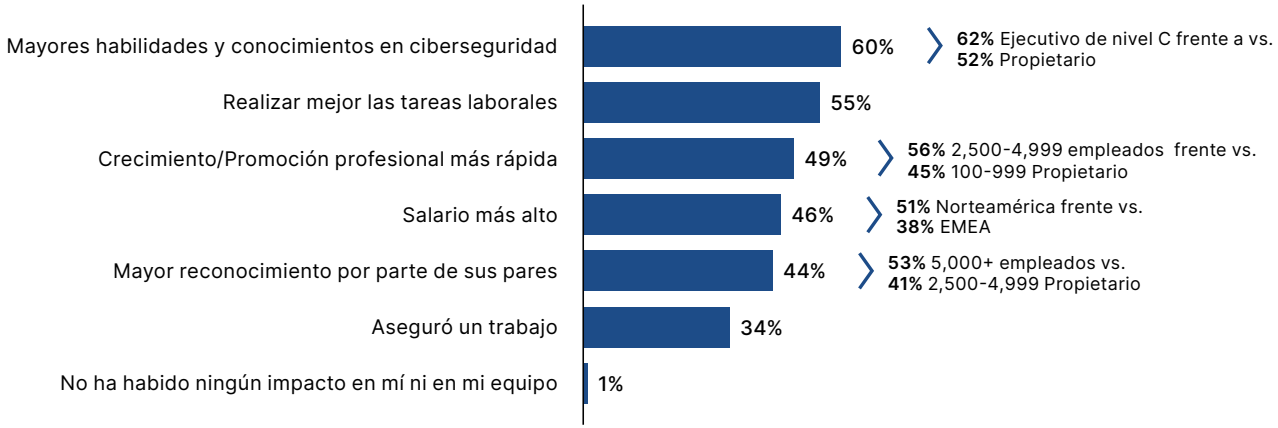
Si bien la demanda es alta, el 72 % de los encuestados dice que es difícil encontrar personas con certificaciones centradas en la tecnología. Este porcentaje es similar a 2022 (73 %), pero frente al 78 % en 2021, lo que sugiere que la búsqueda de talento certificado puede ser un poco más fácil.

El ochenta y nueve por ciento (89 %) de los líderes de TI dicen que pagarían para que un empleado obtuviera una certificación de ciberseguridad. Esta alta tasa de respuestas "sí" se mantuvo relativamente estable (90 % en 2022 y 91 % en 2021) durante los últimos tres años

Las certificaciones marcan una diferencia mensurable

Aquellos que tienen una certificación o trabajan con alguien que tiene una certificación notan beneficios claros. El aumento de habilidades y conocimientos encabeza la lista de esos beneficios.

El impacto de las certificaciones



PROFUNDIDAD DE LA DIAGRAMA

Certificaciones
Fomentar la confianza

Los líderes de TI conocen de primera mano el valor de las certificaciones

El 84 % de los encuestados tiene una certificación. Esto es lo mismo que en 2022 y cerca de 2021 (86 %).

- El 85 % tiene un miembro del equipo con una certificación, solo un uno por ciento menos que el año pasado y solo un poco por debajo de 2021 (88 %).
- La estabilidad relativa del porcentaje relacionado con las certificaciones durante tres años puede indicar que las personas y las organizaciones están viendo la importancia de las certificaciones.

Las certificaciones aumentan la concientización y el conocimiento

El 67 % de los encuestados dice que las certificaciones validan la concientización y el conocimiento en ciberseguridad, similar a 2022 (68 %).

- El 58 % dice que las certificaciones indican que está familiarizado con los productos de los proveedores de seguridad, frente al 54 % en 2022.
- Solo el 1 % dice que tener una certificación no tuvo ningún impacto en su trabajo.

Las certificaciones mejoran la postura de seguridad

El 61 % de los encuestados dice que las personas certificadas son más capaces de mantenerse al día con el panorama de seguridad en evolución. Esto representa una leve caída desde el 66 % en 2022, pero un aumento desde el 42 % en 2021.

- El 70 % de los que tienen esta opinión dicen que su organización enfrentó nueve o más ciberataques en el último año; el 59 % enfrentó entre uno y cuatro.
- Estas correlaciones pueden sugerir que aquellos que han tenido que defenderse de un ciberataque valoran las certificaciones.

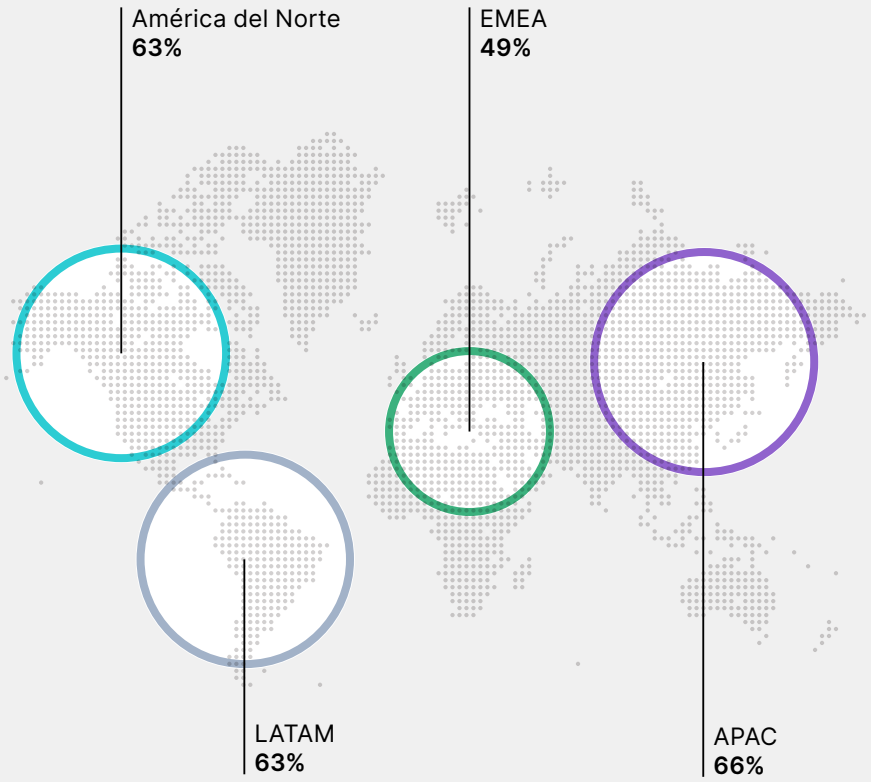
61% cree que las certificaciones mejoran la capacidad de una persona para mantenerse al día con el panorama de seguridad en evolución.

Aspectos destacados regionales

Las organizaciones de APAC tienen una gran confianza en las certificaciones

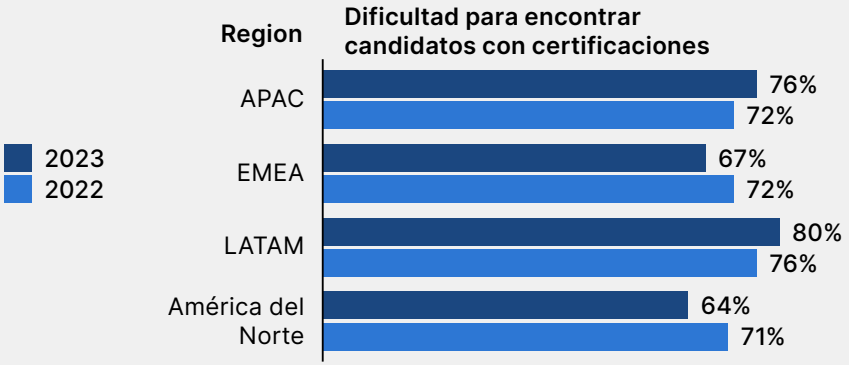
Los encuestados de APAC tenían más probabilidades de decir que las certificaciones aumentan las habilidades y el conocimiento.

Las certificaciones aumentan las habilidades y el conocimiento



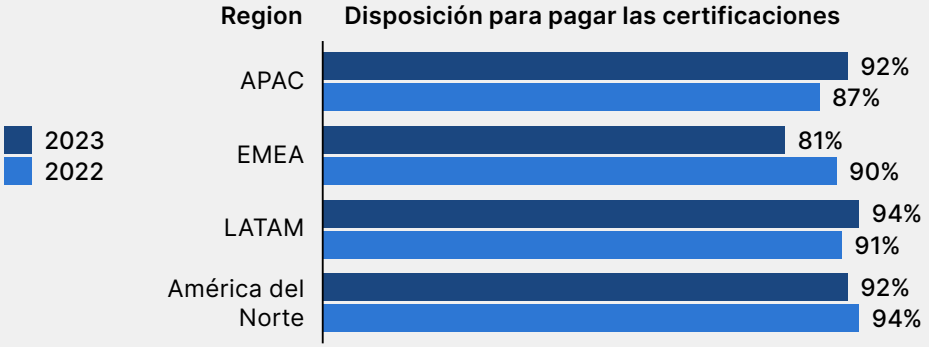
Los profesionales certificados son los más difíciles de encontrar en LATAM

Encontrar candidatos certificados se ha vuelto más difícil para las empresas de LATAM y APAC, y más fácil para las de América del Norte y EMEA.



Organizaciones de todo el mundo pagan las certificaciones de los empleados

La disposición a pagar por un empleado aumentó en APAC y LATAM, pero disminuyó en América del Norte y EMEA.



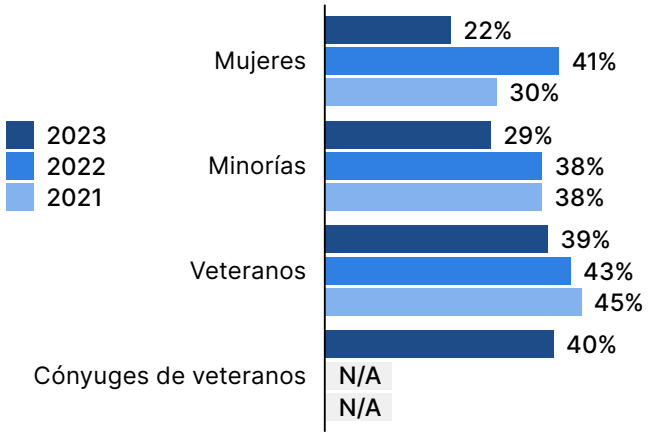
El **83%** de las empresas tienen objetivos de diversidad para contratar en los próximos dos o tres años.

Las organizaciones pueden estar ignorando a los candidatos de antecedentes subrepresentados

Con la persistencia de la escasez global de competencias en ciberseguridad y la equidad y la inclusión cada vez más arraigadas como pilares de la responsabilidad corporativa, la contratación de diversidad continúa siendo un objetivo declarado para muchas organizaciones.

La mayoría (83 %) de las empresas informan que tienen objetivos de contratación de diversidad programados para los próximos años, en línea con 2022, aunque un poco por debajo del 89 % en 2021. Las mujeres y los grupos minoritarios son los principales objetivos con un 76 % y un 64 %, respectivamente. Esto puede deberse a que mujeres y minorías calificadas

Dificultad para encontrar personas calificadas



son más fáciles de encontrar, aunque los encuestados dicen que se ha vuelto menos difícil encontrar candidatos de todos los grupos.[1] Los veteranos y sus cónyuges son los grupos que siguen al 49 % y al 41 %, respectivamente.

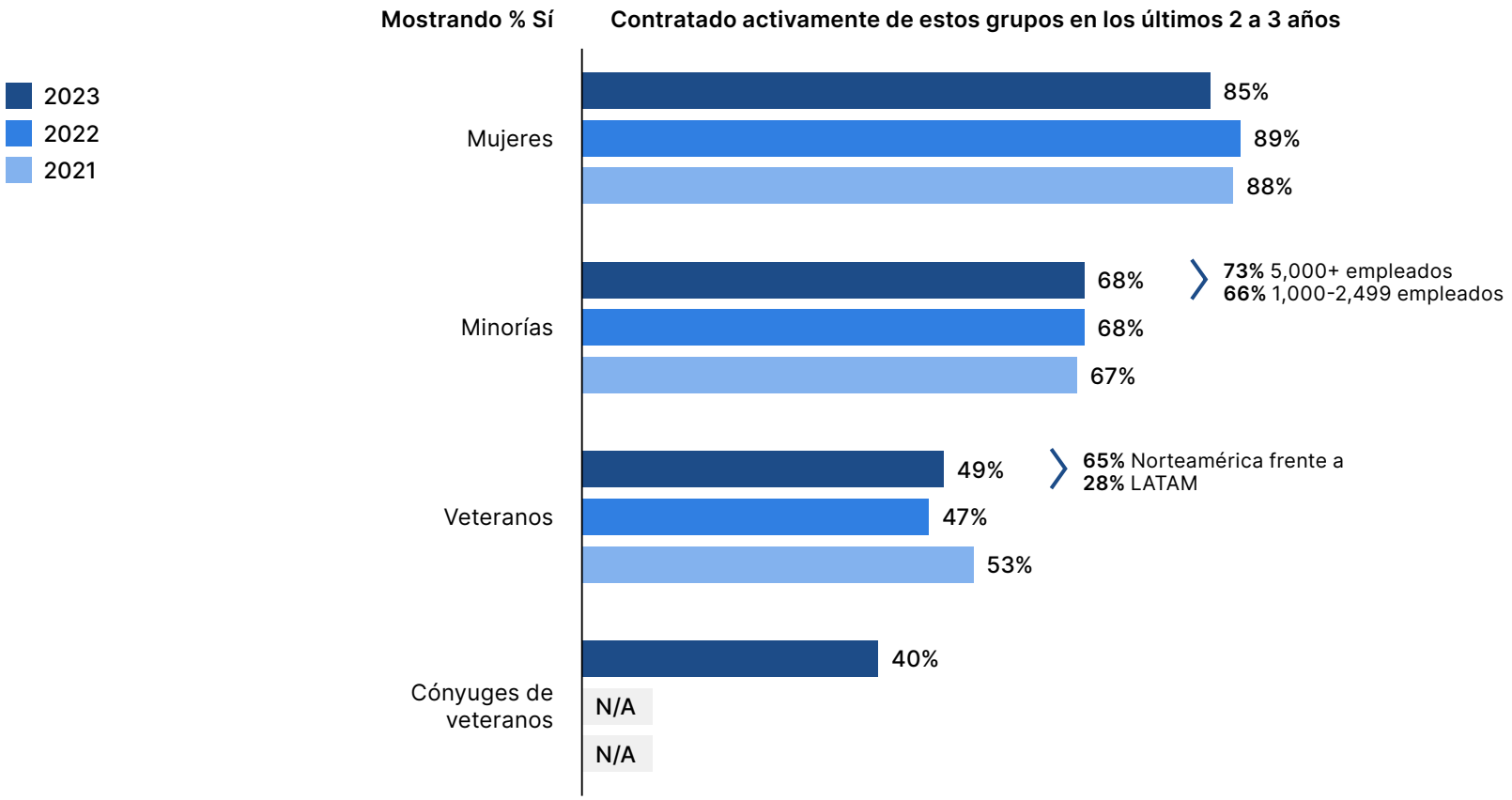
Si bien las mujeres calificadas (51 %) son más fáciles de encontrar, menos organizaciones contrataron activamente a mujeres en los últimos dos o tres años: el 85 % en 2023 frente al 89 % en 2022. La contratación activa de grupos minoritarios se mantuvo relativamente estable y las contrataciones de veteranos aumentaron ligeramente en 2023. El cuarenta por ciento (40 %) de las organizaciones informan que contratan cónyuges de veteranos.

Las organizaciones podrían considerar que es más fácil identificar y contratar a diversos empleados si cambian ciertos requisitos previos. Setenta y un (71 %) de los encuestados dicen que requieren títulos de cuatro años, en lugar de considerar calificaciones de antecedentes no tradicionales, como campos de entrenamiento, certificaciones profesionales y autoaprendizaje. Si las organizaciones cambiaran sus requisitos mínimos, esto, combinado con pasantías o programas de capacitación para contratación, que el 80 % de los encuestados ya ofrecen, podría ayudar a hacer crecer su grupo de talento.

[1] Esto es cierto para todos los grupos, excepto los cónyuges de veteranos, que no se rastrearon previamente.

La contratación activa varía

La contratación activa de mujeres es ligeramente inferior en 2023 que en el año anterior, mientras que la contratación de veteranos aumentó ligeramente, aunque fue menor que en 2021.



PROFUNDIDAD DE LA DIAGRAMA

Los programas de reclutamiento dirigidos tienden a generar más contrataciones

Más organizaciones tienen programas dirigidos a mujeres

Las mujeres continúan siendo el enfoque principal de las iniciativas estructuradas de reclutamiento de diversidad.

- El 73 % de los responsables de la toma de decisiones de TI tienen iniciativas de reclutamiento estructuradas dirigidas a las mujeres.
- Esta proporción se mantuvo relativamente estable en los últimos años: el 73 % en 2022 y el 75 % en 2021.

Los candidatos minoritarios siguen siendo un objetivo importante

El reclutamiento dirigido de candidatos minoritarios se ha mantenido estable desde 2021.

- El 60 % de las organizaciones informan iniciativas de reclutamiento estructuradas para candidatos minoritarios.
- Esto se mantiene casi sin cambios desde el 59 % de años anteriores.

Los veteranos y sus cónyuges continúan siendo subutilizados

Los veteranos a menudo tienen una base sólida de habilidades de seguridad que se acumulan al trabajar en contextos altamente disciplinados y seguros.

Estas habilidades podrían traducirse en ciberseguridad.

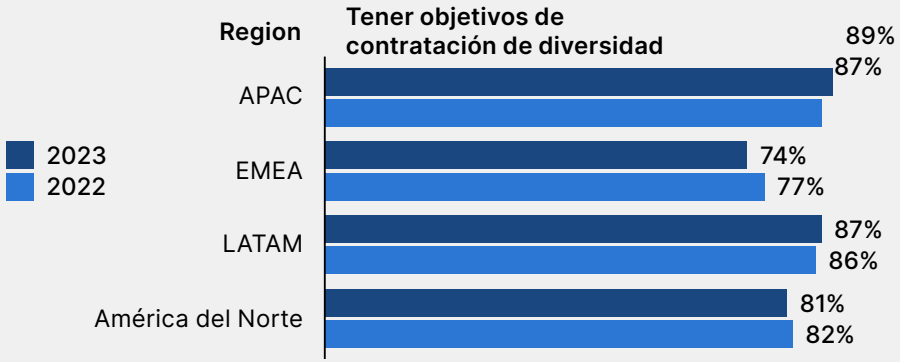
- Menos de la mitad (45 %) de los encuestados tienen iniciativas de reclutamiento dirigidas a veteranos. Esto es un poco superior a 2022 (43 %), pero inferior a 2021 (51 %).
- Incluso menos organizaciones (36 %) tienen programas estructurados dirigidos a los cónyuges de los veteranos.

Más organizaciones (73 %) tienen programas estructurados dirigidos a mujeres y más (85 %) informan que contratan activamente a mujeres, lo que sugiere una correlación entre los programas y los resultados.

Aspectos destacados regionales

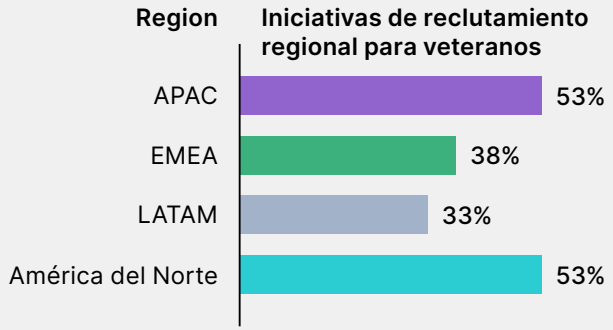
APAC lidera los objetivos de contratación de diversidad

Las empresas de APAC tienen más probabilidades de tener objetivos de contratación de diversidad durante los próximos dos o tres años. Las empresas en EMEA siguen siendo menos propensas.



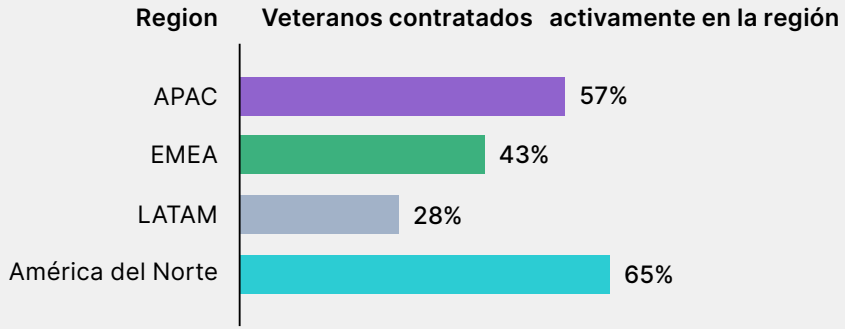
Los veteranos son los más buscados en América del Norte y APAC

Las empresas de América del Norte y APAC tienen más probabilidades de tener iniciativas de reclutamiento estructuradas para veteranos.



Los veteranos se contratan con más frecuencia en América del Norte y APAC

Esto va de la mano con la prevalencia de las iniciativas de reclutamiento.



Conclusión

En 2023, la ciberseguridad fue claramente un problema en toda la empresa para muchas organizaciones, con implicaciones desde el nivel de la junta hasta las primeras líneas. Los resultados de esta encuesta muestran que los participantes están adoptando una respuesta triple a la ciberseguridad que combina capacitación, concientización y tecnología. Esta respuesta proporciona una estrategia integral para enfrentar amenazas actuales y emergentes.

Invertir en capacitación y certificación para personal dedicado de TI y seguridad y aumentar la concientización sobre las mejores prácticas de ciberseguridad entre todos los empleados contribuye en gran medida a fortalecer la postura de seguridad de una organización. Esto será especialmente importante a medida que se desarrollen nuevas amenazas y las tecnologías, como la IA, hagan que los ataques sean más precisos y sofisticados a mayor escala.

Los profesionales de TI/seguridad mejor capacitados, más informados y altamente calificados son esenciales para proteger a los ejecutivos y miembros de la junta de ser sancionados por violaciones. Un personal consciente de la seguridad proporciona defensas críticas de primera línea. Cuanto más se responsabilice a los líderes corporativos, más ciberseguridad se considerará "responsabilidad de todos".

Invertir en certificaciones, garantizar que las certificaciones se mantengan actualizadas y reclutar de grupos de talento diversos y no tradicionales ayudará a cerrar las brechas de habilidades. Las organizaciones pueden restringir su acceso a talento especializado y listo para desarrollar en ciberseguridad al ser demasiado rígidas en su requisito de credenciales fundamentales. Al expandir sus grupos de reclutamiento para incluir candidatos cuyas credenciales están fuera de los títulos tradicionales de cuatro años o antecedentes de capacitación y desarrollo, las organizaciones podrían desbloquear nuevas posibilidades, especialmente si también están dispuestas a pagar por certificaciones y capacitación.

Al final del día, y como parece reconocer la mayoría de los encuestados, los recursos humanos capaces necesitan las herramientas y conjuntos de habilidades de ciberseguridad adecuados para combatir las amenazas y enfrentar la velocidad y el volumen de los ataques actuales. Redondear las habilidades, el conocimiento y las certificaciones con tecnologías avanzadas sigue siendo clave.

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 ofrecemos ciberseguridad donde la necesite con la cartera integrada más grande de más de 50 productos de grado empresarial.

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

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 disponibles para todas las poblaciones. La colaboración con organizaciones de alto perfil y muy respetadas de los sectores público y privado, incluidos los CERT, las entidades gubernamentales y el mundo académico, es un aspecto fundamental del compromiso de Fortinet de mejorar la ciberresiliencia a nivel mundial.

FortiGuard Labs, la organización de investigación e inteligencia frente a amenazas de élite de Fortinet, desarrolla y utiliza tecnologías de IA y aprendizaje automático de vanguardia para proporcionar a los clientes una protección de primera categoría oportuna y consistente, e inteligencia frente a amenazas procesable. Obtenga más información en fortinet.com, el Fortinet Blog, Fortinet Training Institute y FortiGuard Labs.

FORTINET
Training Institute

www.fortinet.com

June 24, 2024 2:49 pm