FORTINET
Training Institute

Desafío de Competencias en Ciberseguridad 2025

Informe de investigación global

Índice

Metodología

Las conclusiones de este informe se basan en las respuestas recogidas en entrevistas online y en una encuesta por correo electrónico realizada a 1.850 responsables de TI y ciberseguridad, llevada a cabo por Sapio Research en febrero de 2025. Las respuestas provienen de 29 regiones:

- Argentina
- Australia
- Brasil
- Canadá
- Colombia
- Francia
- Alemania
- Hong Kong
- India
- Indonesia
- Israel
- Italia
- Japón
- China continental
- Malasia
- México
- Países Bajos
- Nueva Zelanda
- Filipinas
- Singapur
- Sudáfrica
- Corea del Sur
- España
- Suecia
- Taiwán
- Tailandia
- Emiratos Árabes Unidos
- Reino Unido
- Estados Unidos de América

Los resultados globales presentan un margen de error de ± 2,3% con un nivel de confianza del 95%.

Debido al redondeo, los porcentajes pueden no sumar exactamente el 100%.

Tamaño de la empresa

100-499 empleados **25%**
500-999 empleados **24%**
1.000-2.499 empleados **22%**
2.500-4.999 empleados **14%** más de 5.000 empleados **15%**

Género

69% de las personas encuestadas eran hombres **31%** de las personas encuestadas eran mujeres

Total de participantes: 1.850

Asia-Pacífico **30%**
Europa, Oriente Medio y África **27%**
América del Norte **22%**
Latinoamérica **22%**

Tipo de cargo

12% de las personas encuestadas ocupaban cargos de propietario **34%** ejercían funciones de alta dirección (nivel C) **9%** tenían el puesto de vicepresidente **11%** se desempeñaban como jefes de área **33%** ocupaban cargos de director

Los tres sectores empresariales más destacados:

Tecnología **22%**
Industria manufacturera **16%**
Servicios financieros **12%**

Resumen Ejecutivo

En 2024, la estrategia de ciberseguridad se centra más que nunca en la gestión de riesgos, impulsada por una amenaza en constante evolución, la necesidad de proteger la continuidad del negocio y el impacto creciente de la IA en la toma de decisiones empresariales. Las organizaciones mantienen una estrategia integral que combina formación en seguridad, certificaciones y la adopción de tecnologías adecuadas. Este compromiso se extiende desde la alta dirección hasta todos los empleados, reconociendo que cualquiera puede ser objetivo de ciberataques.

La IA se percibe como una amenaza, una oportunidad y un reto

49% de los encuestados temen que el uso de IA por parte de actores maliciosos aumente los ataques de ciberseguridad. **97%** ya utilizan o planean usar soluciones de ciberseguridad basadas en IA.

La falta de profesionales con conocimientos sólidos en IA (**48%**) es el principal reto que señalan los responsables de TI a la hora de incorporar la IA en la ciberseguridad.

Las juntas directivas carecen de conocimientos en ciberseguridad, aunque sea una prioridad

Sólo **49%** de los líderes creen que los miembros de sus consejos entienden plenamente los riesgos que implica el uso de la IA.

52% afirma que directivos o ejecutivos han enfrentado sanciones, cárcel, pérdida de cargo o empleo tras sufrir un ciberataque.

76% indica que sus consejos han reforzado el foco en la ciberseguridad en 2024, frente al 72% de 2023. Para mejorar la protección, los consejos han debatido o implementado:

- Formación obligatoria o certificaciones para el personal de TI y seguridad (62%)
- Capacitación en seguridad para todo el personal (55%)
- Adquisición de soluciones de seguridad que emplean IA (55%)

La falta de concienciación y formación en ciberseguridad sigue siendo la principal causa de brechas

Los líderes de TI siguen señalando que las tres causas principales de las brechas son:

- Falta de conciencia sobre seguridad (56%)
- Déficit de habilidades y formación en seguridad informática (54%)
- Insuficiencia de soluciones de ciberseguridad (50%)

Tras un ataque, la mayoría de los responsables opta por ampliar sus equipos de TI/seguridad (**63%**) o exigir certificaciones profesionales (**62%**)

Las competencias más demandadas en ciberseguridad son protección de datos, cloud y redes.

Las organizaciones buscan profesionales de ciberseguridad con certificaciones

89% prefiere contratar candidatos que cuenten con certificaciones.

67% de los encuestados considera que esto acredita el conocimiento y la conciencia en ciberseguridad.

Solo el **73%** pagaría la obtención de una certificación en ciberseguridad para un empleado, frente al 89% en 2023.

Se están dejando pasar fuentes de talento potenciales

70% de los responsables de TI cuentan con iniciativas de reclutamiento específicas para mujeres, y **57%** para minorías. Sólo **45%** las tienen para veteranos; y apenas **38%** para sus cónyuges. **65%** de los encuestados valoran las certificaciones profesionales al contratar.

Poco más de la mitad (**52%**) considera si el candidato cuenta con un título universitario de cuatro años.

INTRODUCCIÓN

Una creciente necesidad de gestionar el riesgo

Las organizaciones se enfrentan a una nueva realidad en ciberseguridad, donde las brechas son inevitables, la IA representa un riesgo real y las carencias de conocimiento suponen una amenaza crítica. Ya no basta con intentar mitigar el riesgo: ahora es imprescindible gestionarlo de forma proactiva y constante.

La gran mayoría (86%) de los participantes en la encuesta sobre brecha de competencias en ciberseguridad de este año afirman haber sufrido una o más brechas en 2024, y casi un tercio (28%) reporta cinco o más incidentes. Estos niveles son similares a los de los últimos años, y han aumentado notablemente respecto a la primera encuesta en 2021 (80% y 19%, respectivamente), lo que evidencia una tendencia que ha llegado para quedarse.

El impacto de estos incidentes de seguridad es considerable. Más de la mitad (52%) de las organizaciones encuestadas afirman que las brechas les han supuesto un coste superior a 1 millón $. Esta cifra es similar al 53% del año pasado y ha aumentado desde el 38% registrado en 2021.

Ante esta situación, las organizaciones recurren cada vez más a la inteligencia artificial para reforzar sus capacidades y su postura, aunque reconocen que la IA también puede utilizarse en su contra como motor de ciberataques nuevos o más sofisticados. La mayoría (80%) considera que las herramientas de IA están ayudando a sus equipos de TI y seguridad a ser más eficaces, aunque casi todos son conscientes de que la IA por sí sola no resolverá la escasez de profesionales cualificados.

Esta escasez equivale a un déficit de más de 4,7 millones de profesionales en ciberseguridad, según el Informe sobre la Fuerza Laboral en Ciberseguridad 2024 de ISC2. La falta de personal cualificado deja a las organizaciones más expuestas a los ataques, y los gobiernos ya han tomado nota. Muchos países han convertido la ciberseguridad en una prioridad nacional y han puesto en marcha iniciativas para ampliar y fortalecer la fuerza laboral en este sector.

Reducir esta brecha requiere una estrategia coordinada basada en tres pilares: mayor concienciación y formación, capacitación y certificación específicas, e implantación de tecnologías de seguridad avanzadas. Las organizaciones deben replantearse los requisitos que buscan en los candidatos, explorar distintas vías para alcanzar la especialización y seguir aprovechando el talento poco explorado.

Las organizaciones también deben apostar por la formación y el desarrollo en ciberseguridad. Este año, ha bajado el interés por invertir en certificaciones, situándose en un 73% frente al 89% del año anterior, lo cual resulta preocupante. Si esta tendencia se confirma, sería recomendable que las empresas revisaran esta decisión dentro de su estrategia de gestión de riesgos.

Contar con profesionales y empleados cualificados y conscientes es fundamental para gestionar los riesgos cibernéticos en un entorno que ha superado el ciclo tradicional de ataque y defensa. En la actualidad, para protegerse, las organizaciones deben mantener una actitud de vigilancia constante y estar siempre atentas a los riesgos.

49% de todos los encuestados teme que la inteligencia artificial aumente los ciberataques.

La IA se percibe como una amenaza, una oportunidad y un reto

Aunque las organizaciones muestran preocupación por los riesgos asociados a la IA, también la perciben como una herramienta con gran potencial para reforzar sus defensas—eso sí, siempre en manos de profesionales capacitados. La inmensa mayoría (97%) de los encuestados este año ya están utilizando o tienen previsto implementar soluciones de ciberseguridad con IA.

La principal inquietud respecto a la IA es su potencial para incrementar los ciberataques (49%). Esto refleja la creciente preocupación ante la posibilidad de que actores malintencionados utilicen la IA para crear ataques más avanzados, automatizados y dirigidos. Después, surgen otros riesgos con un nivel de urgencia similar: el 39% teme por la difusión de información falsa, ya que la IA generativa facilita la creación de contenidos falsos convincentes que pueden generar confusión, pánico o decisiones equivocadas; el 38% señala la vigilancia y las violaciones de la privacidad; y el 37% expresa temor ante el desarrollo de una IA superinteligente y el riesgo general de perder el control—una cuestión especulativa pero que está ganando peso en el debate público.

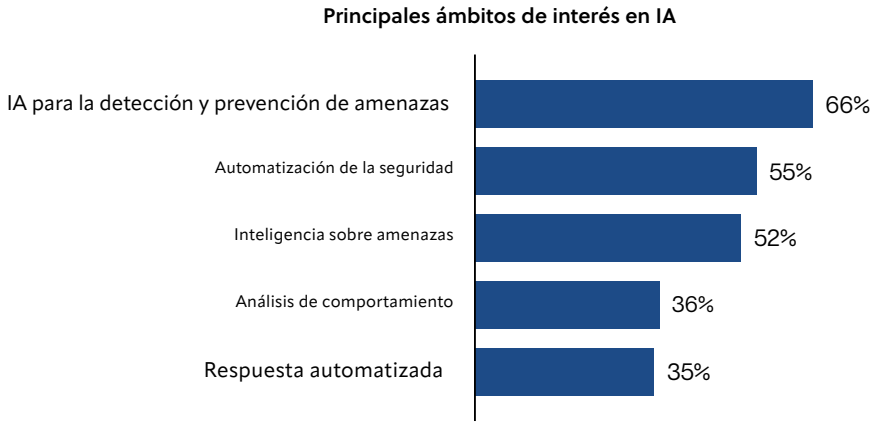
La preocupación por los ciberataques potenciados con IA podría estar impulsando la adopción de soluciones de ciberseguridad basadas en IA—el 65% de los encuestados ya las ha implementado, y otro 32% planea hacerlo en los próximos doce meses. Tan solo un 2% afirma no tener intención de incorporar este tipo de herramientas.

Cuantos más ataques sufra una organización, mayor será la probabilidad de que cuente con soluciones de ciberseguridad basadas en IA. Aproximadamente tres cuartas partes (76%) de las organizaciones que experimentaron nueve o más ciberataques en 2024 afirman haber desplegado herramientas de ciberseguridad con IA, lo que sugiere que la frecuencia de los ataques impulsa el interés por soluciones más innovadoras.

Al preguntarles cuál consideran el mayor reto para integrar la IA en la ciberseguridad, el 48% de los responsables de TI señala la falta de personal con conocimientos especializados en IA. Muy cerca, el 47% destaca la capacidad de garantizar la privacidad de los datos y la seguridad de la información, lo que está directamente relacionado con las preocupaciones sobre la desinformación, la vigilancia y las violaciones de privacidad.

Principales áreas de interés en IA para la ciberseguridad entre organizaciones

La detección y prevención de amenazas se destaca como el mayor campo de interés para aplicar la IA en ciberseguridad, seguidas muy de cerca por la automatización de la seguridad y la inteligencia de amenazas, según los encuestados.



97% de las organizaciones emplean o planean emplear soluciones de ciberseguridad impulsadas por IA.

ANÁLISIS EN PROFUNDIDAD

Impacto y retos de la IA

Los empleos en seguridad no están en peligro por la IA

Pocos líderes consideran que la IA reemplazará a los profesionales de ciberseguridad:

- El 87% espera que la IA mejore ciertos o muchos aspectos de sus funciones.
- El 9% opina que la IA sustituirá partes importantes de sus tareas.
- Solo un 2% cree que la IA podrá reemplazar completamente su puesto.

Las carencias de conocimiento pueden dificultar la adopción de la IA

Además de la falta de experiencia en IA, los encuestados prevén otros obstáculos para adoptar herramientas de ciberseguridad basadas en IA:

- El 44% señala que comprender o gestionar los posibles riesgos de la IA puede dificultar su adopción.
- El 43% indica que la incertidumbre o el escepticismo sobre el papel de la IA en la ciberseguridad también podría ser una barrera.

Las preferencias sobre cómo aprender a usar herramientas de IA son diversas

Las personas encuestadas mencionaron diversas formas preferidas para aprender sobre herramientas de IA:

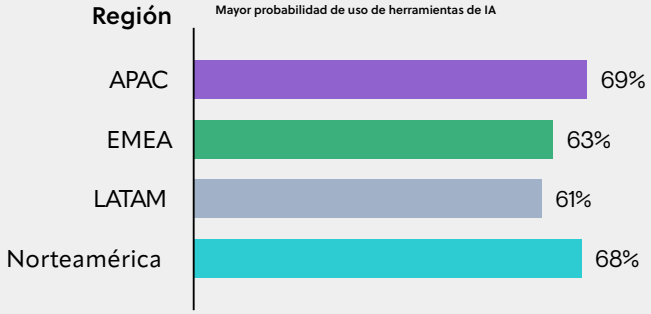
- Formación ofrecida por proveedores (55%)
- Formación independiente de proveedores (49%)
- Aprendizaje práctico en el puesto de trabajo (48%)

55% prefieren la formación ofrecida por proveedores para adquirir conocimientos sobre soluciones de ciberseguridad con IA.

Aspectos destacados por región

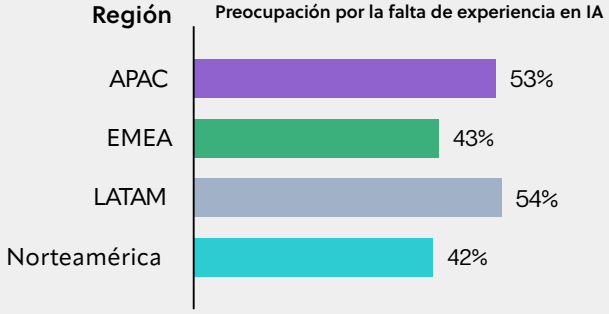
Las herramientas de ciberseguridad con IA son más frecuentes en APAC y Norteamérica

Las organizaciones de Asia Pacífico (APAC) y Norteamérica muestran una ligera mayor tendencia a emplear herramientas de ciberseguridad con IA.



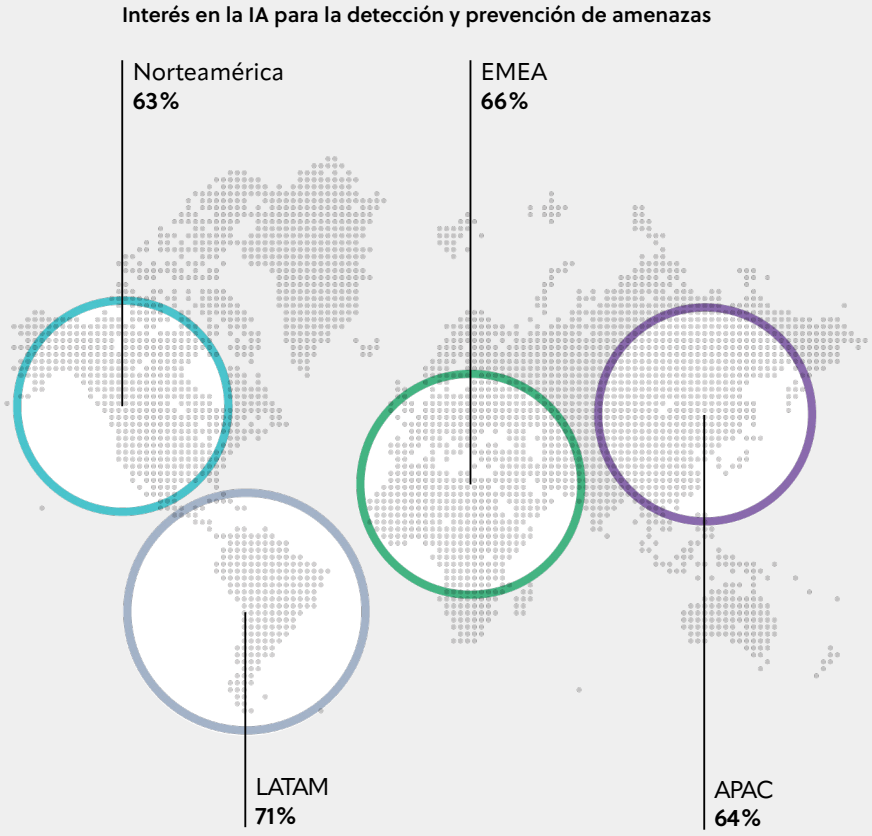
En algunas regiones, la preocupación por la experiencia en IA es más alta

La falta de conocimientos en IA preocupa especialmente en Latinoamérica (LATAM) y la región Asia-Pacífico (APAC).



Algunas regiones muestran mayor interés en la IA aplicada a la ciberseguridad

En LATAM, el uso de IA para la detección y prevención de amenazas es una prioridad especialmente alta.



Poner en marcha acciones

Refuerza la formación y la concienciación en seguridad

Los resultados sobre IA de este año están en línea con nuestro Informe Global de Investigación sobre Conciencia y Formación en Seguridad 2024, que reveló que el 62% de los líderes temían que sus empleados fueran más vulnerables a ataques debido a la IA. Teniendo en cuenta los datos actuales sobre falta de habilidades en IA y los riesgos relacionados con la desinformación, la privacidad de los datos y la seguridad de la información, parece que muchas organizaciones consideran que su personal aún no está completamente preparado para afrontar el reto de la IA.

Descubre cómo la IA puede ayudarte

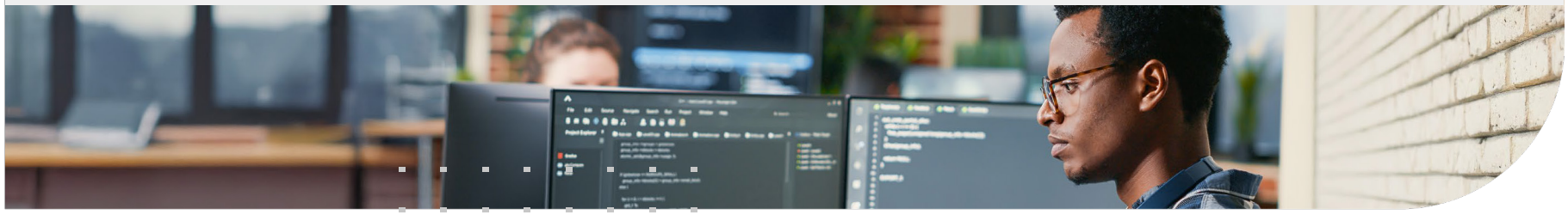
Las organizaciones también deben identificar en qué áreas la IA puede destacar; por ejemplo, actuando como un analista junior que revisa rápidamente registros para detectar la causa de amenazas y resaltar información clave. Así, los profesionales, como los ingenieros sénior, pueden centrarse en análisis urgentes y críticos, tomar decisiones y supervisar las respuestas. Promover la concienciación y ofrecer formación ayuda a abordar este desafío.

Haz las preguntas adecuadas sobre la IA

En lugar de preguntar si los proveedores "tienen IA", las organizaciones deben empezar a cuestionarse cómo pueden aprovechar la inteligencia artificial para alcanzar sus objetivos específicos de seguridad, como analizar registros (gestión de información y eventos de seguridad, SIEM) o responder automáticamente a amenazas (detección y respuesta en endpoints, EDR; detección y respuesta ampliada, XDR; y orquestación, automatización y respuesta de seguridad, SOAR).

Piensa en el modelo SOC como servicio

Dado que pocas organizaciones cuentan con personal especializado para gestionar estos sistemas de forma autónoma, el centro de operaciones de seguridad como servicio (SOCaaS) se presenta como una alternativa. Así, la empresa puede beneficiarse de la seguridad basada en IA y del asesoramiento experto, como una respuesta más rápida ante amenazas, sin la carga de gestionar la tecnología internamente.



Menos de la mitad **(49%)** de todos los líderes piensan que sus juntas directivas están completamente informado sobre los posibles riesgos que implica el uso de la IA para la organización.

Los consejos carecen de conocimientos en ciberseguridad, aunque sea una prioridad

A pesar de que los directores y ejecutivos corporativos siguen siendo responsables de las brechas de ciberseguridad, muchos miembros de los consejos de administración no tienen plena conciencia de los riesgos que implica el uso de la inteligencia artificial para sus organizaciones.

Menos de la mitad (49%) de los encuestados considera que los miembros de su consejo están completamente informados sobre los riesgos de la IA. Un 42% cree que el nivel de conocimiento es intermedio; mientras que el 7% opina que su consejo solo tiene una noción básica. Entre quienes perciben mayor conocimiento sobre IA, el 61% supervisa organizaciones que ya emplean herramientas de ciberseguridad basadas en IA. De los que detectan conciencia intermedia, el 36% utiliza estas soluciones. En cambio, solo el 3% de los miembros con menor conocimiento están usando herramientas de IA.

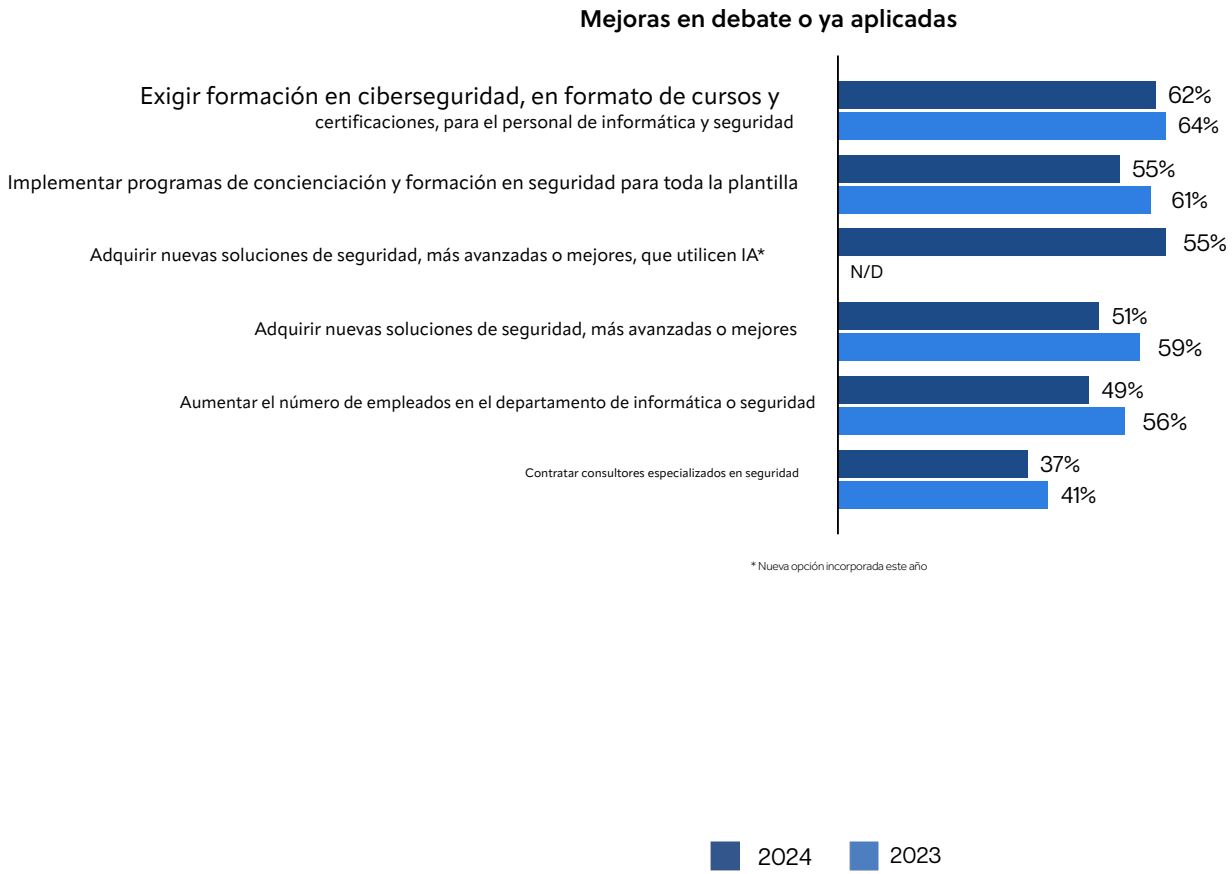
Aunque los consejos de administración intentan ponerse al día en materia de IA, en general están prestando más atención a la ciberseguridad: Más de tres cuartas partes (76%) de los encuestados afirman que su consejo ha aumentado el enfoque en ciberseguridad en 2024, frente al 72% en 2023. La inmensa mayoría considera la ciberseguridad una prioridad tanto empresarial (96%) como financiera (95%) para su organización, en mayor o menor medida.

El mayor interés de los consejos directivos en la ciberseguridad puede deberse en parte a que el 52% de las organizaciones encuestadas afirma que sus directivos o ejecutivos han afrontado sanciones económicas (33%), penas de prisión (15%) o la pérdida de empleo o cargo (33%) tras sufrir un ciberataque, cifras similares a las del año anterior. Ese 52% se eleva al 76% en aquellas organizaciones que experimentaron entre cinco y ocho ciberataques en 2024.

Para reforzar la ciberseguridad, los líderes señalan que sus consejos han debatido o puesto en marcha medidas como: formación obligatoria o certificaciones para el personal de IT y seguridad (62%); formación en concienciación sobre seguridad para toda la plantilla (55%— un descenso respecto al 61% en 2023); y la adquisición de soluciones de seguridad basadas en IA (55%).

Principales iniciativas impulsadas por el consejo en ciberseguridad

Un año más, la mayoría de los encuestados que conocen el enfoque de sus consejos directivos afirman que la formación y certificación obligatoria en ciberseguridad para el personal de TI y de seguridad son las acciones más debatidas o implementadas. Como novedad, más de la mitad (55 %) destaca que sus consejos también han considerado o puesto en marcha soluciones que incorporan IA.



ANÁLISIS EN PROFUNDIDAD

Las brechas siguen siendo relevantes—y los consejos lo saben

Las brechas siguen siendo frecuentes y costosas

La mayoría de las organizaciones sufrieron brechas de seguridad en 2024, y más de la mitad tuvo que asumir un coste considerable:

- El 86% experimentó una o más brechas; el 28% tuvo cinco o más.
- El 52% afirma que esas brechas les costaron más de $1 millón.
- Los ataques de malware, phishing y web representan el 78% del total, una cifra similar al año anterior (80%).

El tiempo de recuperación continúa afectando a las organizaciones

Los tiempos de recuperación tras los ciberataques han mejorado ligeramente:

- El 59% de las organizaciones tardó un mes o más en recuperarse de un ciberataque.
- Las administraciones públicas (nacional, autonómica y local) son las que más rápido se recuperan: el 58% lo hizo en menos de un mes.
- El tiempo medio de recuperación entre todos los encuestados es de 2,5 meses, una leve mejora respecto a los 2,7 de 2023.

La ciberseguridad está en el punto de mira de los consejos directivos

Aunque aún hay margen de mejora, los consejos están prestando más atención a los riesgos digitales:

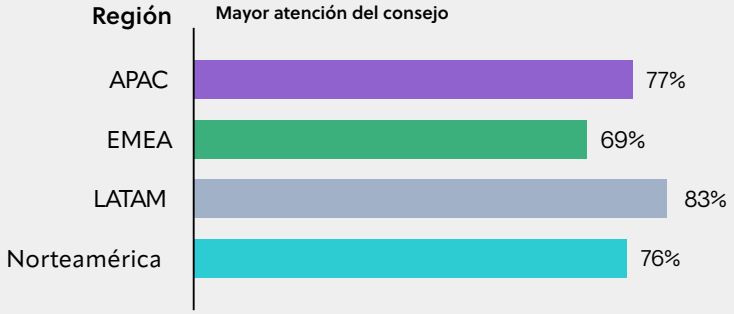
- Solo el 2% de los encuestados señala que en 2024 hay menos interés del consejo en la ciberseguridad.
- Los consejos de organizaciones grandes dan más prioridad a la ciberseguridad que los de empresas más pequeñas (83% para más de 5.000 empleados frente al 72% para las de 100–499 empleados).
- El 96% de los consejos considera la ciberseguridad una prioridad empresarial y el 95% la ve como prioridad financiera.

Solo **el 2%** de los participantes indicó que el consejo dedicó menos atención a la ciberseguridad en 2024.

Aspectos destacados por región

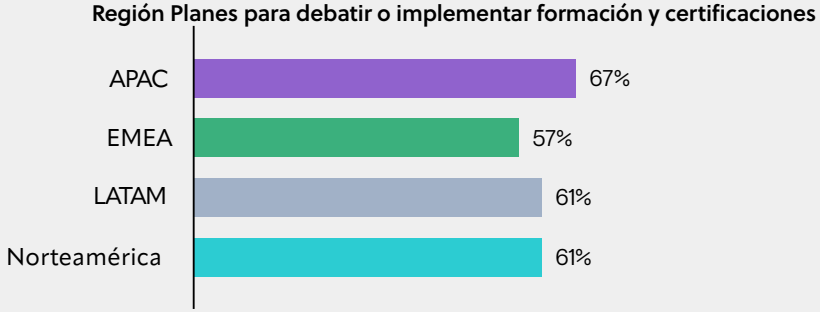
El interés del consejo en la ciberseguridad aumentó principalmente en LATAM

Las personas encuestadas en LATAM fueron las que más señalaron un mayor enfoque del consejo en ciberseguridad para 2024.



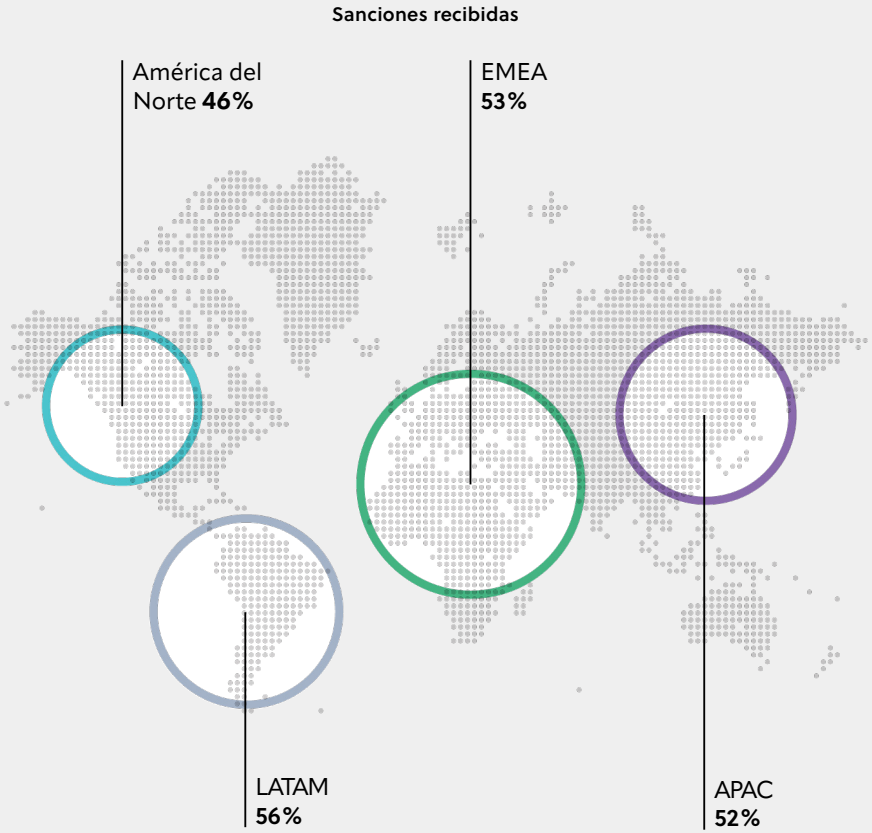
En todas las regiones, los consejos directivos apuestan por la formación y certificación en ciberseguridad

Los consejos han debatido o puesto en marcha programas de capacitación y certificación en ciberseguridad para el personal de TI y seguridad en todas las regiones, destacando especialmente en APAC.



Más directivos y ejecutivos afrontaron sanciones en LATAM

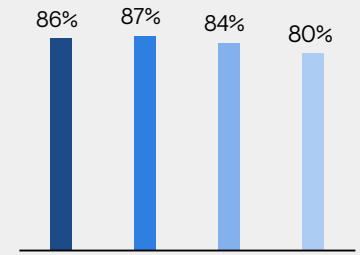
LATAM registró la mayor cantidad de miembros del consejo y ejecutivos multados, encarcelados o que perdieron su cargo o empleo debido a ciberataques.



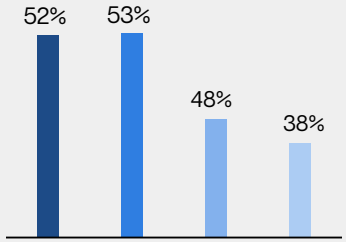
PERSPECTIVA INTERANUAL

Ciberseguridad y gobierno corporativo

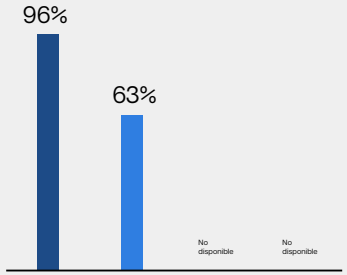
EL IMPACTO DE LAS BRECHAS



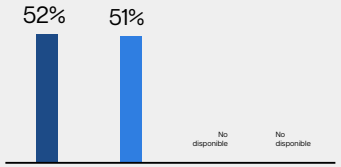
Uno o más incidentes de seguridad sufridos en los últimos 12 meses



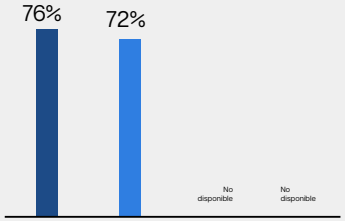
Las brechas supusieron un coste superior a $1 millón USD



Se tardó más de un mes en recuperarse tras un ciberataque



Directivos o ejecutivos sancionados con multas, prisión o pérdida de empleo o cargo tras una brecha de seguridad



Mayor atención del consejo de administración a la ciberseguridad

2024 2023 2022 2021

Ponerse en marcha

Forma a tu consejo directivo en ciberseguridad e inteligencia artificial

A pesar de que la ciberseguridad sigue ganando importancia, entre 2023 y 2024 los consejos directivos apenas han experimentado cambios en este ámbito. Dada la gravedad de las brechas y la responsabilidad personal que recae sobre directivos y ejecutivos, esta falta de avance indica que aún queda mucho por hacer, especialmente cuando el conocimiento sobre los riesgos de la IA sigue siendo bajo en los consejos, a pesar del aumento de su uso y del incremento previsto de los ataques impulsados por la inteligencia artificial.

Los consejos directivos desempeñan un papel fundamental en la definición de estrategias para la gestión de riesgos y la resiliencia cibernética. Es imprescindible contar con miembros con conocimientos y conciencia en la materia, además de asegurar la creación y fortalecimiento de comités dedicados a la ciberseguridad.

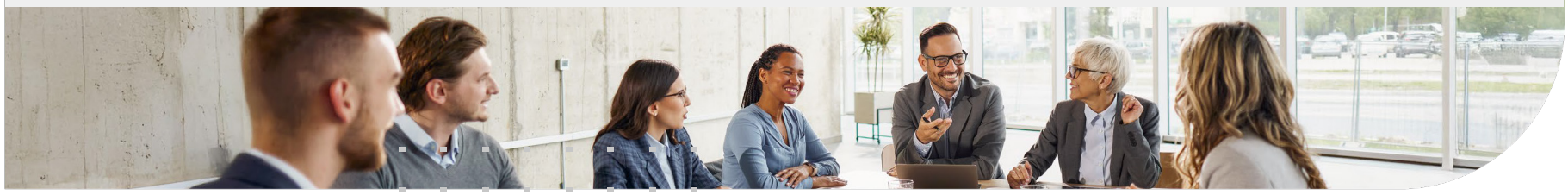
Como parte de una estrategia integral de ciberseguridad, es posible que los consejos necesiten recibir formación específica y actualizarse sobre los riesgos, desafíos y oportunidades que presenta la inteligencia artificial. La ciberseguridad es una responsabilidad compartida, y los consejos deben asumir su compromiso.

Elabora un plan de gestión de riesgos de ciberseguridad

Los miembros proactivos del consejo pueden iniciar su proceso de concienciación sobre IA consultando sobre el nivel de preparación de su organización para gestionar riesgos de ciberseguridad. Una pregunta útil sería averiguar el tiempo medio de respuesta (MTTR) ante ataques, ya que una detección lenta suele traducirse en una recuperación más lenta.

Asegúrate de contar con las soluciones de ciberseguridad adecuadas

Para reducir un MTTR elevado, las organizaciones pueden buscar herramientas que permitan detectar amenazas de forma temprana y responder con rapidez. Ejemplo de ello es una plataforma SOAR (orquestación, automatización y respuesta de seguridad), que aborda los incidentes en el momento en que ocurren. Otras opciones incluyen EDR (detección y respuesta en el endpoint), NDR (detección y respuesta en la red) y XDR (detección y respuesta extendidas), que trabajan conjuntamente para ofrecer una visión integral que facilita una reacción ágil.



56% de los responsables de IT consideran que la falta de conciencia sobre ciberseguridad es la principal causa de las brechas de seguridad.

La falta de concienciación y formación en ciberseguridad sigue siendo la principal causa de brechas de seguridad

Los líderes de TI señalan tres factores interrelacionados como causa de las brechas de ciberseguridad: falta de conciencia sobre seguridad entre los empleados (56%), carencia de habilidades y personal de TI o seguridad debidamente capacitado (54%), y ausencia de las soluciones de ciberseguridad necesarias (50%).

Estas cifras son similares a las del año pasado, aunque la falta de concienciación ha pasado a ser el principal motivo, mientras que las carencias en habilidades, formación y productos de ciberseguridad han descendido ligeramente, ambos cuatro puntos porcentuales menos respecto a 2023, cuando estaban en 58% y 54% respectivamente.

La mayoría de los participantes (67%) afirma que la escasez de competencias en ciberseguridad supone riesgos adicionales para sus organizaciones, una cifra prácticamente igual que en 2023 (70%). Las áreas donde más se requieren estas competencias son la protección de datos, la seguridad en la nube y la seguridad de redes.

En sintonía con las principales causas de brechas de seguridad, los responsables de TI señalan que ante un ciberataque sus principales medidas serían:

- Reforzar el equipo interno de TI o seguridad (63%)
- Exigir formación en ciberseguridad mediante certificaciones para el personal de TI y seguridad (62%)
- Implementar programas de concienciación y formación para empleados (59%)
- Adquirir nuevas soluciones de seguridad (56%)

Los ciberataques siguen teniendo como objetivo a los usuarios finales

Una vez más, el malware, el phishing y los ataques web lideran la lista de tipos de ataque con un 78%, muy cerca del 80% registrado en 2023. Los ciberdelincuentes identifican claramente a los usuarios como el punto más vulnerable de la seguridad de las organizaciones, reforzando así la percepción de los responsables de TI sobre las causas de las brechas de seguridad.

Los 20 tipos de ataque más frecuentes

	2024	2023	2022
1. Ataques de malware	40%	44%	45%
2. Ataques de phishing	32%	36%	36%
3. Ataques web	30%	31%	36%
4. Ataques a contraseñas	27%	30%	35%
5. Caballos de Troya	24%	29%	31%
6. Ransomware	24%	26%	28%
7. Ataques DoS y DDoS	23%	26%	27%
8. Suplantación de DNS	19%	20%	22%
9. Interpretación de URLs	18%	17%	18%
10. Ataques de spear-phishing	17%	19%	18%

	2024	2023	2022
11. Dispositivos USB externos o medios físicos	17%	16%	No disponible
12. Ataques de inyección SQL	16%	16%	16%
13. Ataques de phishing dirigido a ejecutivos ('whale-phishing')	16%	14%	16%
14. Amenazas internas	14%	14%	18%
15. Ataques de tipo 'drive-by'	14%	14%	14%
16. Secuestro de sesión	14%	13%	12%
17. Ataques por fuerza bruta	13%	15%	15%
18. Coacción, chantaje o soborno a personal interno	12%	12%	No disponible
19. Escucha ilícita de comunicaciones ('eavesdropping')	12%	11%	13%
20. Ataques XSS	12%	11%	12%

ANÁLISIS EN PROFUNDIDAD

La escasez de talento sigue siendo un riesgo importante

Las organizaciones se enfrentan a retos para contratar

Aunque el proceso de selección y contratación sigue siendo complicado, la situación no es tan grave como en años anteriores:

- Más de la mitad (52 %) de los participantes afirma que tiene dificultades para captar y contratar talento en ciberseguridad, una mejora respecto al 60 % registrado en 2021.
- La inteligencia artificial está aportando soluciones: el 80 % indica que las herramientas de IA para seguridad ayudan a los equipos de TI y protección a ser más eficaces y ágiles.

Las habilidades clave y algunos tipos de experiencia siguen siendo difíciles de encontrar

Algunos perfiles siguen siendo especialmente difíciles de encontrar:

- Los profesionales con experiencia en ingeniería de redes y seguridad siguen siendo escasos (58 %, frente al 62 % en 2023).
- Justo detrás están quienes cuentan con experiencia específica en IA aplicada a ciberseguridad (57 %).
- Los puestos más complicados de cubrir son los de IA/aprendizaje automático y seguridad en la nube (30 %).

La contratación sigue siendo altamente competitiva

Las organizaciones encuentran obstáculos para retener personal de ciberseguridad por varios motivos clave:

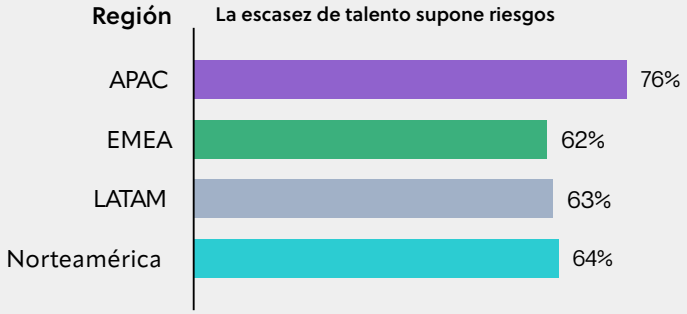
- Algunas entidades señalan la falta de formación y oportunidades para mejorar competencias (48 %).
- Otras comentan que no pueden competir con las ofertas salariales y beneficios de otras compañías (42 %).
- Muy pocas (13 %) afirman no tener problemas para conservar a sus empleados.

Aproximadamente un tercio de los encuestados afirma que los puestos relacionados con IA/aprendizaje automático y seguridad en la nube son los más difíciles de cubrir.

Puntos destacados por región

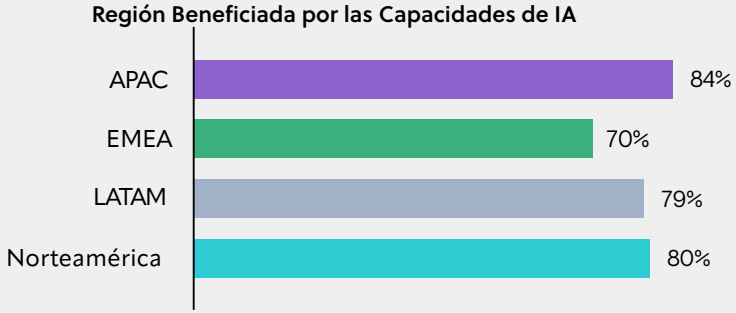
La escasez de profesionales impacta especialmente en APAC

Las organizaciones de APAC son las que más reconocen que la falta de expertos en ciberseguridad les genera riesgos adicionales.



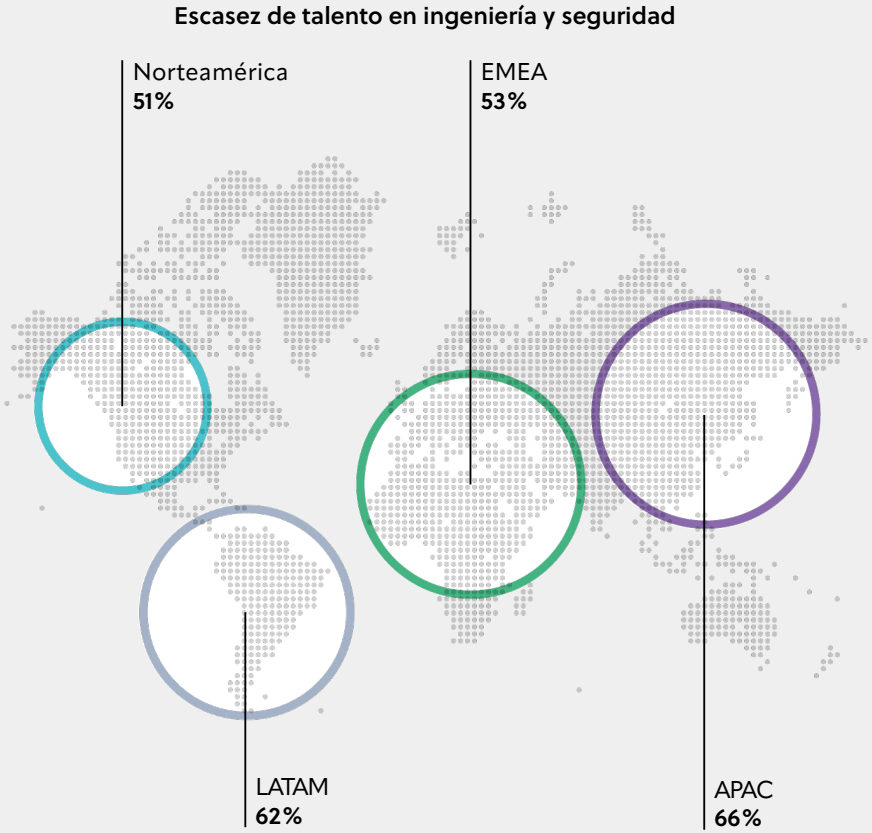
En todas las regiones, las soluciones que aprovechan la inteligencia artificial están aportando beneficios

Las organizaciones de APAC coinciden más que ninguna en que las herramientas de ciberseguridad basadas en IA mejoran la eficacia y la eficiencia.



La experiencia en ingeniería de redes y seguridad es más limitada en APAC

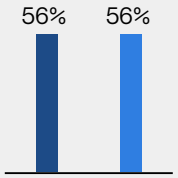
Las organizaciones de APAC tienen mayores dificultades para encontrar candidatos con experiencia específica en ingeniería de redes y seguridad.



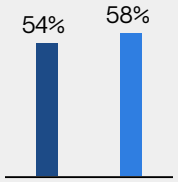
PERSPECTIVA ANUAL

Causas y respuestas frente a los ciberataques

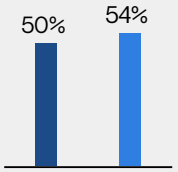
PRINCIPALES CAUSAS DE INCUMPLIMIENTOS



Falta de concienciación sobre seguridad entre los empleados

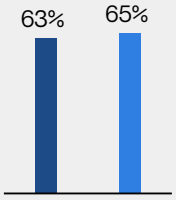


Insuficiencia de habilidades en ciberseguridad y de personal especializado en TI o seguridad informática

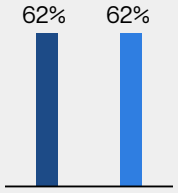


Carencia de soluciones de ciberseguridad necesarias

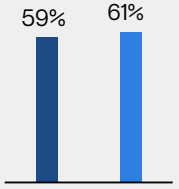
PRINCIPALES RESPUESTAS ANTE CIBERATAQUES



Ampliar el equipo de TI o de seguridad



Exigir certificaciones en ciberseguridad para el personal de TI y seguridad



Implementar programas de concienciación y formación en seguridad para todo el personal

2024 2023

Poner en marcha medidas

Gestiona el riesgo cibernético de manera proactiva

Aunque ciertos tipos de ciberataques son más habituales que otros (ver página 21), las organizaciones no pueden anticipar exactamente qué ataques pueden sufrir.

Las organizaciones deben abordar la ciberseguridad como una iniciativa estratégica que involucre a toda la empresa, gestionando los riesgos de forma proactiva y no limitándose solo a defenderse y reaccionar ante incidentes.

Contrata en base a competencias y conocimientos en ciberseguridad

Como parte de este plan, los responsables de seguridad deben facilitar una comunicación clara entre los encargados de selección y el departamento de RRHH para garantizar que las personas más capacitadas ocupen los puestos vacantes o de nueva creación, priorizando su encaje en la organización y su experiencia en ciberseguridad. Al evaluar al equipo, la formación y certificación pueden ayudar tanto a los nuevos empleados como a los actuales a adquirir o actualizar sus competencias en las áreas que más preocupan.

Busca formación y certificaciones reconocidas en el sector

Los líderes de seguridad deben identificar proveedores de ciberseguridad que ofrezcan programas de certificación reconocidos por la industria y un enfoque sólido en la capacitación orientada a roles. Las certificaciones más valiosas se corresponden con áreas clave de la ciberseguridad y fomentan el desarrollo continuo de habilidades en todos los niveles de experiencia.

Mantén actualizados los programas de formación y concienciación

La estrategia también debe contemplar la implantación y revisión constante de los programas de concienciación en seguridad para todo el personal, así como la evaluación continua de la arquitectura de red y sus vulnerabilidades, alineando estos procesos con el plan y las personas encargadas de ejecutarlo.

Si las organizaciones desean añadir una capa extra de protección frente a los errores humanos que sus empleados puedan cometer sin querer, utilizar herramientas de seguridad impulsadas por IA, capaces de proteger el correo electrónico, los navegadores y las aplicaciones de colaboración, puede reducir notablemente las superficies de ataque más vulnerables. Al neutralizar automáticamente las amenazas en las aplicaciones que los empleados usan a diario, los equipos de seguridad pueden responder de forma más ágil y evitar que pequeños fallos humanos se conviertan en incidentes de seguridad graves.

89% de los responsables de TI prefieren contratar a candidatos con certificaciones.

Las organizaciones buscan profesionales de ciberseguridad con certificaciones

En 2021, el primer año de la encuesta sobre la Brecha de Competencias en Ciberseguridad, el 81% de los participantes señaló que prefería contratar profesionales de ciberseguridad con certificaciones. Un año después, ese porcentaje ascendió hasta el 90%—y desde entonces prácticamente no ha cambiado.

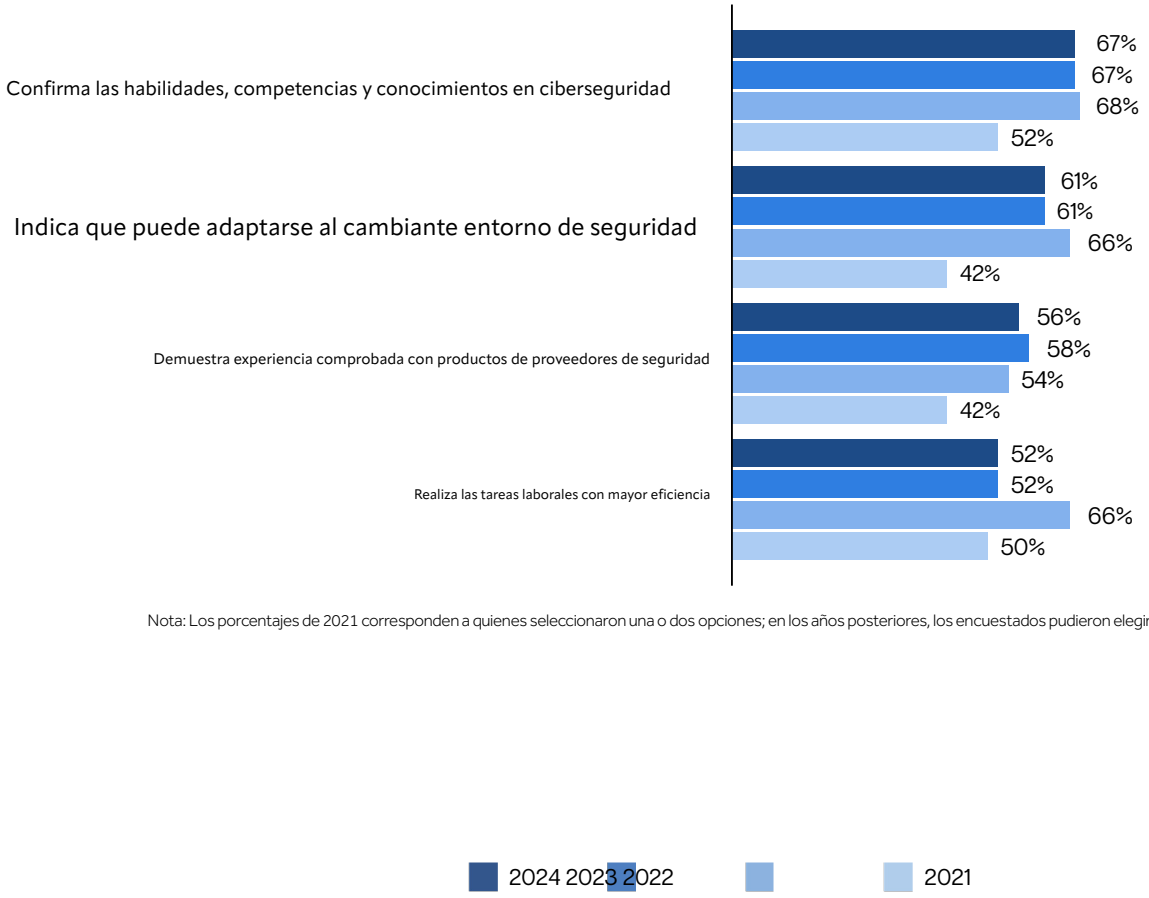
En 2024, el 89% de los responsables de TI manifestó preferir candidatos con certificaciones. Una amplia mayoría (67%) señaló que buscan certificaciones al contratar a un miembro del equipo o a un subordinado directo, ya que consideran que valida el conocimiento y la conciencia en ciberseguridad. Casi la misma proporción (61%) ve las certificaciones como una señal de capacidad para adaptarse al panorama de seguridad en constante evolución. Más de la mitad (56%) considera que las certificaciones demuestran familiaridad con los productos de los proveedores de seguridad.

A pesar de las ventajas y la clara preferencia por las certificaciones, el porcentaje de organizaciones dispuestas a financiar la obtención de certificaciones para sus empleados ha descendido notablemente en la última encuesta, situándose en un 73% frente al 89% en 2023. Un cuarto de las entidades (25%) afirma que no costearía una certificación, cuando en 2023 solo era el 7%. Aunque no está claro el motivo de este cambio, parece contradecir el reconocimiento de que la formación y las certificaciones marcan la diferencia.

El conocimiento y el rendimiento impulsan la preferencia por las certificaciones

Al analizar los resultados de las encuestas de los últimos cuatro años, queda claro que los participantes prefieren de forma constante a los candidatos certificados, valorando las habilidades, conocimientos y competencias que aportan.

El impacto de las certificaciones



Nota: Los porcentajes de 2021 corresponden a quienes seleccionaron una o dos opciones; en los años posteriores, los encuestados pudieron elegir más de dos alternativas.

ANÁLISIS EN PROFUNDIDAD

Las certificaciones tienen un impacto real

La presencia de certificaciones sigue siendo alta

La mayoría de los encuestados cuenta con personas en sus equipos que tienen certificaciones orientadas a la tecnología, o poseen certificaciones ellos mismos:

- El 86% tiene a alguien en su equipo con una certificación tecnológica.
- El 81% cuenta con certificaciones tecnológicas propias (aunque este porcentaje ha bajado desde el 84% en 2023 y sigue la tendencia descendente desde el 86% en 2021).

Las certificaciones aportan beneficios evidentes

Los encuestados siguen destacando varios beneficios de las certificaciones, tanto para ellos mismos como para sus compañeros:

- El 61% informa una mejora en sus habilidades y conocimientos sobre ciberseguridad.
- El 55% menciona que puede desempeñar mejor sus funciones laborales.
- El 50% señala un avance más rápido en su carrera profesional o la posibilidad de ascensos.

Las empresas de mayor tamaño suelen valorar más las certificaciones

Las empresas de mayor tamaño suelen dar más importancia y muestran mayor disposición a invertir en certificaciones:

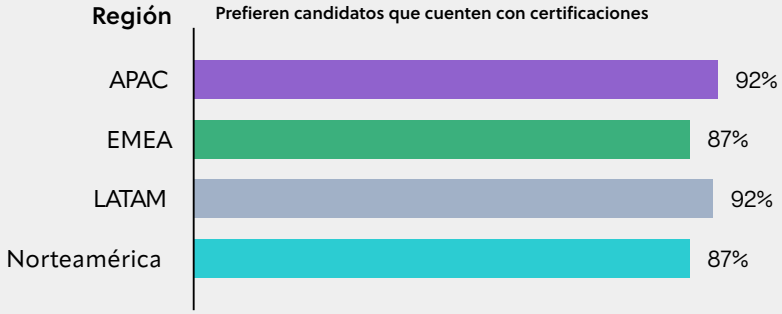
- El 77% de las organizaciones con 5.000 empleados o más están dispuestas a cubrir los costes de certificaciones, frente al 72% en las empresas más pequeñas.
- Aproximadamente el 69% de los participantes de organizaciones con más de 1.000 empleados buscan certificaciones, en comparación con el 64% en aquellas con entre 500 y 999 empleados.

El 86% de los encuestados afirma que en su equipo hay alguien con una certificación tecnológica.

Puntos destacados por región

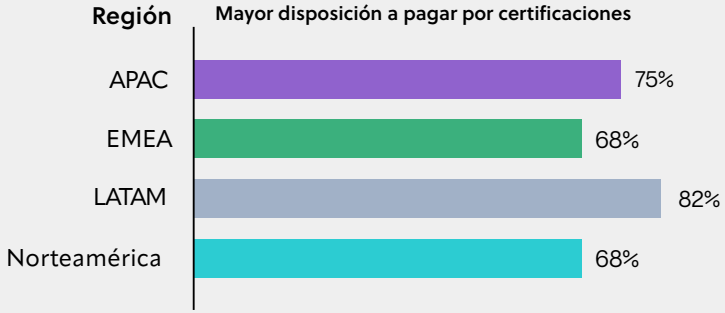
En todas las regiones, las organizaciones muestran preferencia por candidatos certificados

La preferencia por certificaciones orientadas a tecnología es más alta en APAC y LATAM.



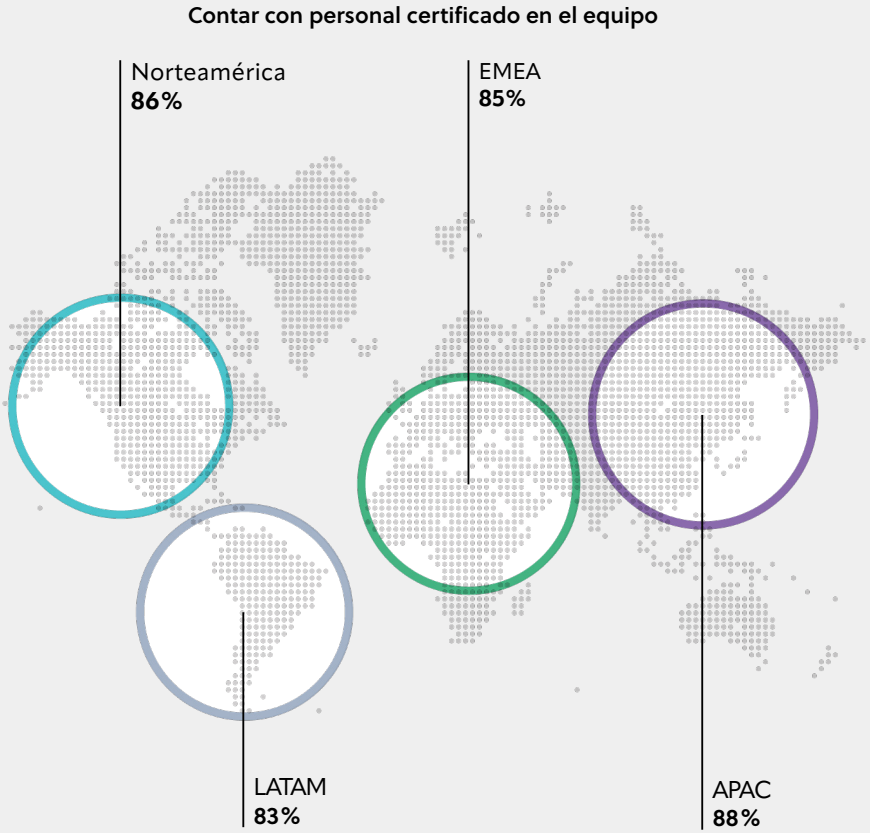
Las organizaciones de LATAM destacan por su disposición a invertir en la certificación de sus empleados

La voluntad de pagar certificaciones en LATAM supera en 7 a 14 puntos porcentuales a otras regiones.



Es habitual encontrar miembros certificados en los equipos de todas las regiones

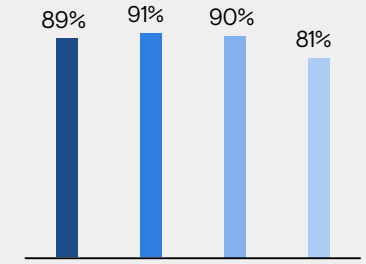
En APAC, los encuestados son quienes más suelen tener a alguien certificado en su equipo.



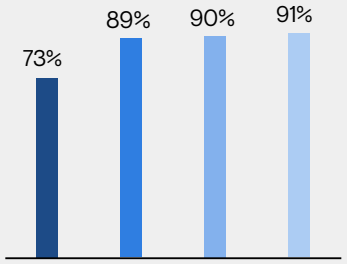
Perspectiva año tras año

Demanda de certificaciones

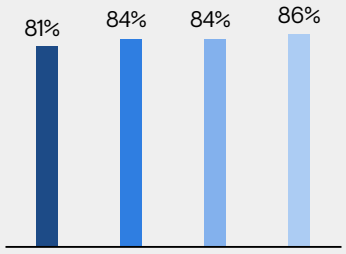
Por qué son importantes las certificaciones



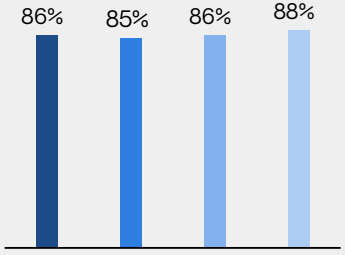
Preferencia de los responsables de IT por contratar personas con certificaciones tecnológicas



Disposición de los responsables de IT para financiar la certificación en ciberseguridad de sus empleados



Responsables de IT con certificaciones



Responsables de IT con miembros del equipo certificados

2024 2023 2022 2021

Poner en marcha medidas

Explora diferentes caminos para alcanzar la especialización

Las investigaciones de Fortinet revelan que las organizaciones deben adoptar diversos "caminos hacia la especialización" para superar la brecha de competencias y cubrir puestos clave en ciberseguridad. Las certificaciones son una de esas rutas, ya que aportan experiencia práctica y credenciales reconocidas por el sector.

La mayoría de los líderes lo tienen claro: el 61% destaca que mejorar las habilidades y conocimientos en ciberseguridad es el principal beneficio de las certificaciones. Además, los responsables tienden a contratar a quienes ya cuentan con alguna certificación.

Da prioridad al desarrollo de habilidades y conocimientos de los empleados

Lo que resulta desconcertante este año es la disminución de organizaciones dispuestas a costear certificaciones. Se necesita recopilar más información para esclarecer las causas de este descenso. En el contexto económico actual, podría considerarse que las organizaciones muestran preocupación por los costes. Si ese es el motivo, conviene recordar que los ahorros generados por la inteligencia artificial y la automatización de la seguridad pueden liberar recursos para invertir en la formación de los empleados, ofreciéndoles la oportunidad de adquirir las competencias y conocimientos necesarios para reforzar la seguridad de la empresa.

Aprovechar la certificación para retener talento

La retención de empleados clave también es fundamental. Las organizaciones deben invertir en su equipo como parte de su estrategia de fidelización. Casi la mitad de los encuestados (48%) señala la falta de oportunidades de formación y mejora profesional como el principal reto para mantener al personal. Los responsables de IT parecen ser conscientes de esto, dada su preferencia por candidatos certificados, lo que hace aún más llamativa la reducción de empresas dispuestas a sufragar certificaciones.

Los veteranos **(43%)** y los cónyuges de veteranos **(41%)** son los perfiles calificados más difíciles de encontrar.

Se están pasando por alto fuentes de talento potencial

Aunque las organizaciones han logrado avances aprovechando ciertos grupos de talento poco explotados en los últimos cuatro años, siguen afirmando que la brecha de habilidades pone en riesgo su ciberseguridad. En parte, el problema podría estar en cómo definen a los "candidatos cualificados".

El porcentaje de organizaciones que afirma tener dificultades para encontrar candidatas mujeres y personas pertenecientes a minorías cualificadas ha disminuido notablemente desde nuestra primera encuesta sobre la brecha de habilidades en ciberseguridad en 2021: del 30% al 20% en 2024 para mujeres y del 38% al 29% para minorías.***Brecha de habilidades en ciberseguridad*** encuesta en 2021—del 30% al 20% en 2024 para mujeres y del 38% al 29% para candidatos de minorías.

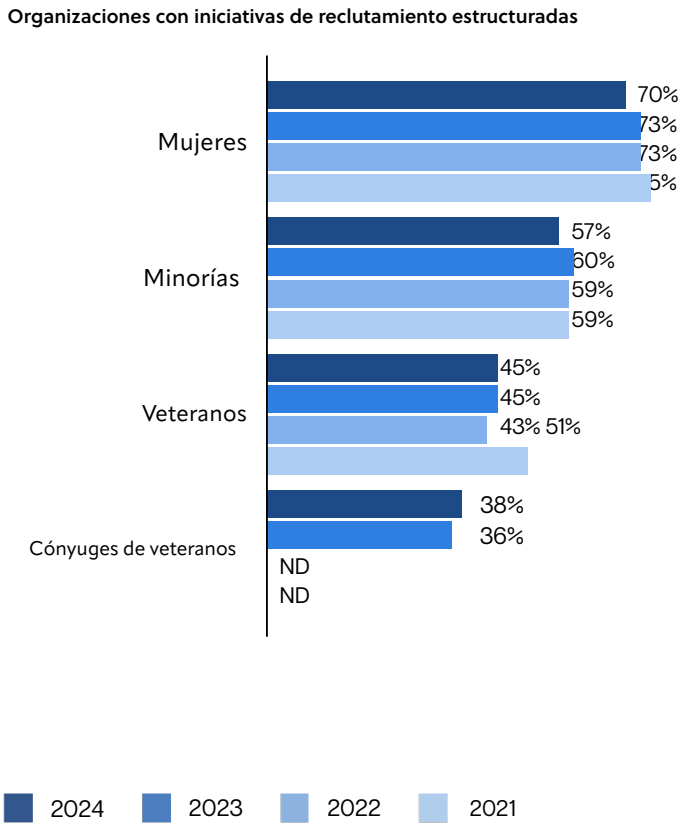
Dicho esto, estos datos se han mantenido prácticamente sin cambios en los últimos dos años, y tanto los veteranos como sus cónyuges siguen siendo mucho más difíciles de captar, con tasas del 43% y 41% respectivamente. Aunque parte de esta dificultad puede deberse a la oferta o estar relacionada con el acceso a determinados grupos de talento, también puede deberse a que las organizaciones descartan a posibles candidatos por sus requisitos.

Además de las dificultades para acceder a ciertos grupos de talento, también puede deberse a que las organizaciones descartan a posibles candidatos por no cumplir con requisitos específicos.

Más de la mitad (52%) de las organizaciones tiene en cuenta si un candidato posee un título universitario de cuatro años al contratar, y una clara mayoría (65%) valora las certificaciones profesionales. Si se consideraran otros niveles de formación o acreditaciones, se podría atraer a más talento, siempre que las empresas estén dispuestas a invertir en desarrollo profesional tras la incorporación.

Parece que las iniciativas estructuradas de reclutamiento para grupos clave de talento están disminuyendo poco a poco

Desde 2021, el porcentaje de participantes que indica que su organización cuenta con iniciativas estructuradas de reclutamiento para mujeres, minorías, veteranos y cónyuges de veteranos ha disminuido en todos los casos, salvo en el de cónyuges de veteranos.



ANÁLISIS EN PROFUNDIDAD

Los niveles de empleo reflejan la dificultad para contratar

Las mujeres constituyen la mayor parte de las contrataciones no tradicionales en TI y seguridad

En promedio, según el conjunto de organizaciones encuestadas:

- El 27% del personal en equipos de TI y seguridad son mujeres.
- El 20% proviene de contextos minoritarios.
- El 17% son veteranos.
- El 15% son cónyuges de veteranos.

Algunas organizaciones sí valoran credenciales alternativas

Las personas encuestadas indicaron que considerarían factores más allá de títulos universitarios de cuatro años:

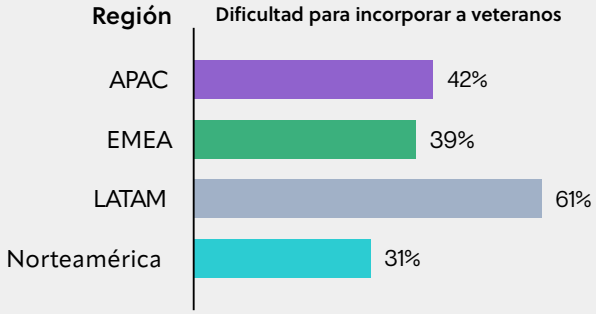
- El 43% afirma que consideraría si el candidato posee un diploma.
- El 38% señala que tendría en cuenta si el candidato ha recibido formación por parte de proveedores.

Las mujeres representan, de media, el **27%** del personal de TI y seguridad en las organizaciones encuestadas.

Aspectos destacados por región

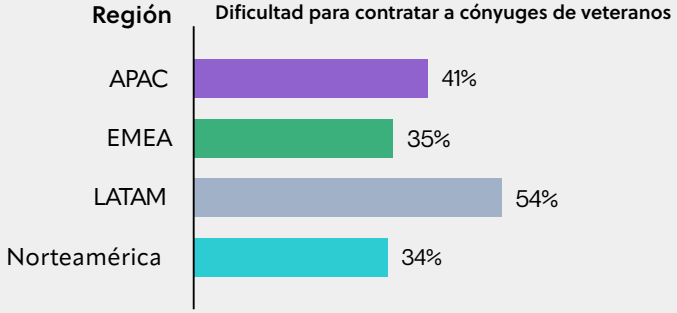
En LATAM es más complicado atraer veteranos que en otras regiones

En Norteamérica la captación de veteranos resulta menos compleja.



Lo mismo ocurre con los cónyuges de los veteranos

Las organizaciones de EMEA y Norteamérica encuentran menos dificultades para incorporar cónyuges de veteranos.



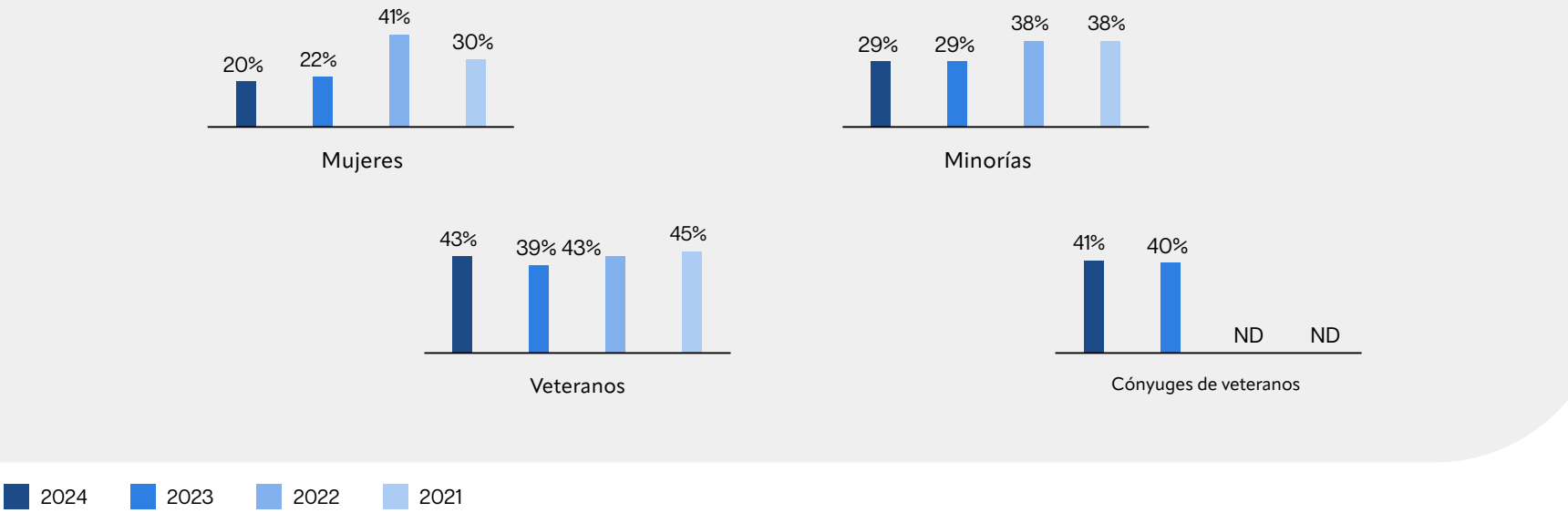
En Norteamérica es donde más difícil resulta encontrar mujeres candidatas cualificadas

En Norteamérica y EMEA, un porcentaje ligeramente mayor de organizaciones afirma que encontrar mujeres candidatas cualificadas es complicado.

VISIÓN INTERANUAL

Captación de talento en fuentes poco exploradas

PERFILES CUALIFICADOS MÁS DIFÍCILES DE ENCONTRAR



Poniendo en marcha soluciones

Ten en cuenta tanto las competencias como los conocimientos

Buscar talento en grupos reducidos dentro de un mercado laboral competitivo exige estrategias flexibles y creativas. Apostar únicamente por credenciales tradicionales, como títulos universitarios de cuatro años, puede limitar el acceso de las empresas al talento que realmente necesitan.

Como se destaca en este informe, investigaciones recientes de Fortinet muestran que las organizaciones deben explorar diferentes vías para captar y desarrollar talento, incluyendo la combinación de credenciales y formación práctica.

Colabora estrechamente con RRHH en la definición de los requisitos de los puestos

Los responsables de ciberseguridad deben colaborar con Recursos Humanos para asegurar que lo publicado las cualificaciones requeridas para un puesto se ajusten a las competencias y conocimientos que necesita la organización, que se consideren todos los posibles grupos de talento y que se permitan diferentes opciones de formación para cubrir el puesto.

Impulsar alianzas público-privadas (PPP) que aborden la brecha de habilidades en ciberseguridad

A gran escala, crear una reserva de talento para la industria global de ciberseguridad que abarque a todas las poblaciones requerirá una cooperación más estrecha entre el sector empresarial, académico y gubernamental. En Estados Unidos y otros países, ya se está dando paso a programas de ciberseguridad de dos años financiados por gobiernos para ayudar a reducir la brecha de competencias.

Conclusión

La ciberseguridad se ha convertido en una cuestión estratégica de gran relevancia para las organizaciones a nivel mundial, impulsada por el avance de la inteligencia artificial y el amplio abanico de riesgos que suponen las amenazas digitales para los negocios. La necesidad de adoptar un enfoque estratégico está llevando la ciberseguridad más allá de la alta dirección, alcanzando incluso a los consejos de administración.

A medida que los consejos asumen mayor responsabilidad en materia de ciberseguridad, los consejeros corporativos se ven obligados a comprender mejor los desafíos para poder tomar decisiones informadas en la gestión de riesgos. En ciertos casos—especialmente en lo referente a la inteligencia artificial—esto puede requerir formación y capacitación en riesgos digitales para los miembros del consejo.

La inteligencia artificial, al mismo tiempo que presenta riesgos, ofrece un enorme potencial para fortalecer las soluciones de ciberseguridad. Más allá del consejo directivo, es fundamental que todas las personas de la organización sean conscientes de la IA y que los equipos de ciberseguridad dispongan de las competencias necesarias para utilizar herramientas basadas en inteligencia artificial.

También es fundamental que los equipos comprendan tanto las capacidades como las limitaciones de la inteligencia artificial: identificar en qué áreas puede aportar eficiencia y facilitar el trabajo, y reconocer dónde sigue siendo imprescindible la intervención de profesionales cualificados con criterio experto.

Esta demanda de personal especializado mantiene vigente la escasez global de talento en ciberseguridad. Las organizaciones pueden aumentar sus posibilidades de cubrir puestos clave si replantean los requisitos exigidos a los candidatos —por ejemplo, dejando de priorizar títulos universitarios de cuatro años— y accediendo a fuentes de talento poco aprovechadas.

Reducir la brecha de habilidades también implica invertir en formación y desarrollo profesional. En lugar de esperar a la persona “perfecta”, puede ser más efectivo contratar talento con alto potencial y buena adaptación, y formarlo específicamente para el puesto. Los resultados de este año indican que apostar por la formación y el desarrollo también favorece la retención de talento. En este sentido, es importante recalcar que la reticencia a invertir en certificaciones que se ha detectado en los resultados de este año puede poner en serio peligro los objetivos de ciberseguridad de las organizaciones. La formación y las certificaciones siguen siendo pilares esenciales en el enfoque integral de la ciberseguridad, junto con la concienciación general de los empleados y la implementación de tecnologías adecuadas.

Fortinet lleva años apostando por una estrategia integral basada en concienciación, formación y tecnología. Según la encuesta de este año, este enfoque se integra perfectamente en el marco más amplio de la gestión holística del riesgo cibernético. A medida que la gestión de riesgos evoluciona, permite a las organizaciones protegerse de forma proactiva, salvaguardar sus datos y sus negocios, sin importar cómo cambien las amenazas y las tecnologías.

Acerca de Fortinet

Fortinet (NASDAQ: FTNT) es un referente clave en la transformación de la ciberseguridad y en la integración de redes y seguridad. Nuestra misión es proteger a las personas, los dispositivos y los datos en cualquier lugar, y actualmente ofrecemos soluciones de ciberseguridad donde nuestros clientes las necesitan, respaldados por el mayor portafolio integrado del sector, con más de 50 productos de nivel empresarial.

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

El Instituto de Formación Fortinet, uno de los programas de capacitación más grandes y completos del sector, está comprometido a ofrecer formación en ciberseguridad y nuevas oportunidades profesionales para todos. La colaboración con reconocidas organizaciones de los sectores público y privado, incluidos los Equipos de Respuesta ante Emergencias Informáticas ("CERTS"), organismos gubernamentales y el mundo académico, es clave en el compromiso de Fortinet para fortalecer la resiliencia digital a nivel global.

FortiGuard Labs, la organización de investigación y análisis de amenazas líder de Fortinet, desarrolla y emplea avanzadas tecnologías de inteligencia artificial y aprendizaje automático para ofrecer a sus clientes protección de primer nivel y datos útiles sobre amenazas, siempre a tiempo y con la máxima calidad. Descubre más en fortinet.com, el Blog de Fortinet y en FortiGuard Labs.

FORTINET
Training Institute

www.fortinet.com

4 de septiembre de 2025, 15:02 h