HAYS Working for your tomorrow

INFORME GLOBAL SOBRE **CIBERSEGURIDAD** 2024

Más allá del talento cibernético tradicional.

Expertos en
Tecnología

CONTENIDO

Introducción

LA DEMANDA DE **CIBERCAPACIDADES**

La ciberdelincuencia sigue siendo uno de los mayores riesgos en nuestra era moderna, y ninguna organización, ya sea pública o privada, grande o pequeña, puede subestimar esta amenaza en 2024. Se estima que los ciberataques costarán al mundo 9,5 billones de dólares este año, dejando un impacto duradero en la reputación y las operaciones futuras de cualquier entidad que no logre contraatacar. Es imprescindible que ganemos esta lucha.

¿Cómo vencer a la ciberdelincuencia? Con las personas idóneas. Debemos implicar a los directivos, maximizar la tecnología y aprovechar el capital humano para ganar. El hilo conductor son las personas. Personas altamente motivadas, con talento e innovadoras. Encontrar y retener a las personas adecuadas, con las habilidades adecuadas, centradas en la tecnología adecuada es esencial para las empresas de hoy en día. Se calcula que hay 3,5 millones de vacantes de ciberseguridad en todo el mundo. En Hays, vemos a diario el impacto de este déficit. El talento preparado es escaso y la tecnología avanza a un ritmo sin precedentes. La nueva tecnología trae consigo innovación, así como mayores riesgos y vulnerabilidades. Más tecnología en nuestros espacios significa más delincuentes en nuestros espacios. Debemos contraatacar, pero los profesionales de la ciberseguridad luchan por mantener actualizadas sus competencias.

Los paradigmas de ayer no traerán los resultados de mañana. Debemos comprender dónde estamos hoy con la vista puesta en el mañana para trazar eficazmente nuestro camino hacia el futuro. Por eso es un gran privilegio presentar otro Informe Anual de Ciberseguridad Global de Hays, con opiniones de más de 1.000 CISO y líderes de ciberseguridad de todo el mundo.

Aunque más de la mitad de los encuestados afirmaron haber aumentado su equipo de ciberseguridad el año pasado, los líderes están más preocupados por sus presupuestos que hace 12 meses, siendo la inversión en personal el área que más preocupa. El dinámico clima geopolítico y económico actual ha afectado al gasto de más del 75% de nuestros encuestados, y los empleadores deben mirar más allá de los aumentos salariales para atraer al talento cibernético. Las oportunidades de trabajo remoto e híbrido, así como una mayor flexibilidad, son cada vez más importantes.

Es vital que trabajemos juntos para construir una cantera de talentos en ciberseguridad con las habilidades adecuadas para resolver los retos del mañana. Muchos de ustedes han reconocido y explorado el talento cibernético no tradicional como una solución, es decir, aquellos que no tienen ni educación formal ni experiencia en el campo. Sin embargo, podemos hacer aún más. Los datos de nuestra encuesta sugieren que los empleadores de todo el mundo no están aprovechando todo el potencial de esta reserva de talentos sin explotar.

La causa principal: la falta de inversión adecuada en formación y desarrollo dedicados, y la flexibilidad limitada de los departamentos de contratación para mirar más allá de los procedimientos típicos de contratación.

Simultáneamente, existe la necesidad de aprovechar la rápida evolución que estamos presenciando en la Inteligencia Artificial. Aunque nuestros encuestados creen que la IA puede respaldar sus capacidades de seguridad, existen dudas sobre su aplicación como herramienta, o potencial compañero de trabajo, para que lo utilice la plantilla.

A lo largo de nuestro informe, encontrarás comentarios de expertos y líderes de pensamiento en ciberseguridad de Hays que trabajan incansablemente en primera línea para ayudar a resolver estos retos. También es un honor para mí compartir las opiniones de los líderes en ciberseguridad de organizaciones de renombre mundial que se dedican a ganar esta lucha contra la ciberdelincuencia. Sus contribuciones no tienen precio.

Aunque más de la mitad de los encuestados afirmaron haber aumentado su equipo de ciberseguridad en el último año, los líderes están más preocupados por su presupuesto comparado con hace 12 meses.

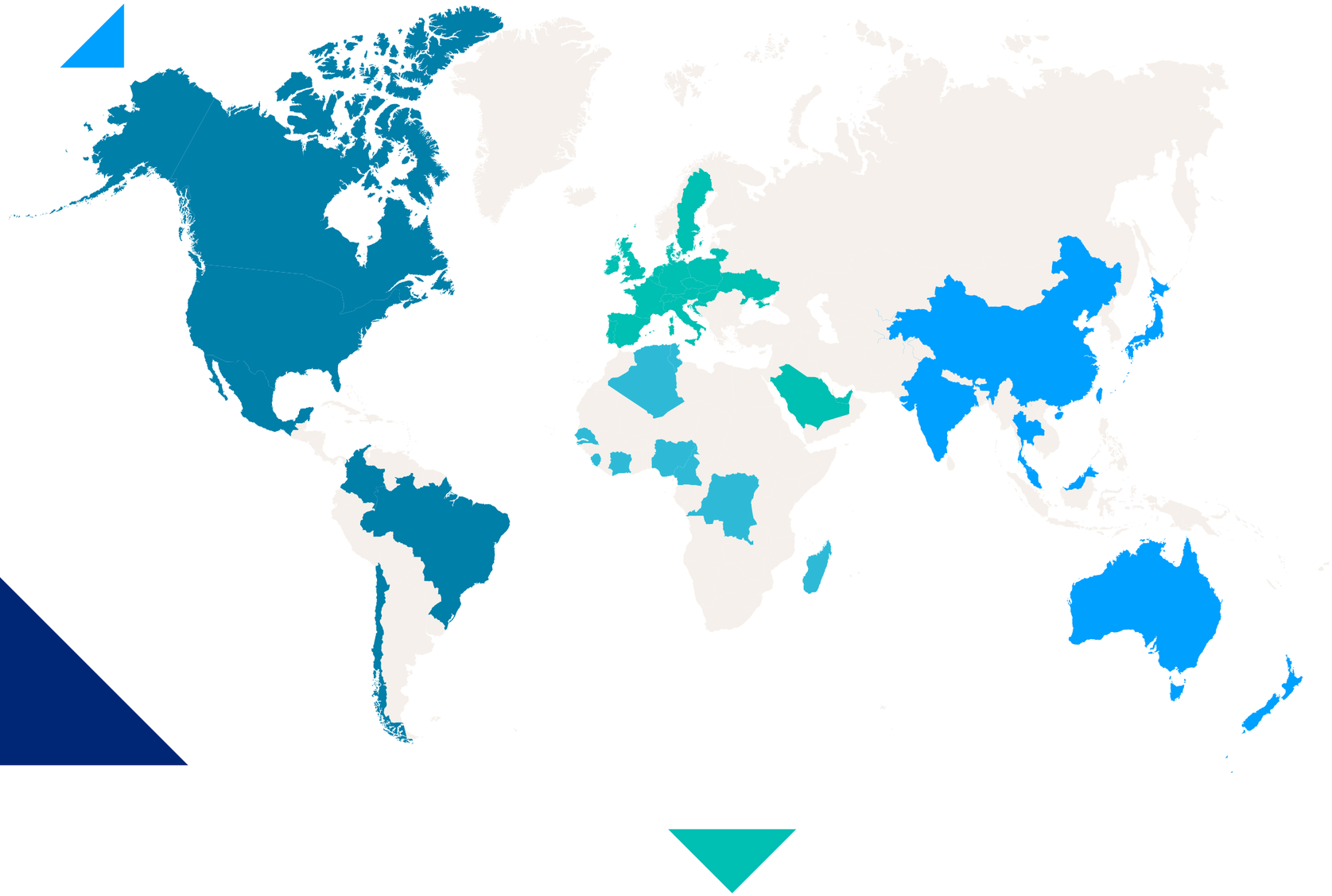
Confiamos en que los resultados de nuestra encuesta, así como los consejos de los expertos de dentro y fuera de Hays, te beneficien en tu diligente lucha diaria contra la ciberdelincuencia. Nadie puede sobrevivir como una isla aislada. Estamos juntos en esta lucha y estamos en ella para ganarla.

Un agradecimiento especial a todos nuestros colaboradores, así como a nuestro variado grupo de encuestados. Sin su disposición a compartir su considerable experiencia y conocimientos, no habríamos podido ofrecer estas valiosas perspectivas. ¡Gracias a todos!

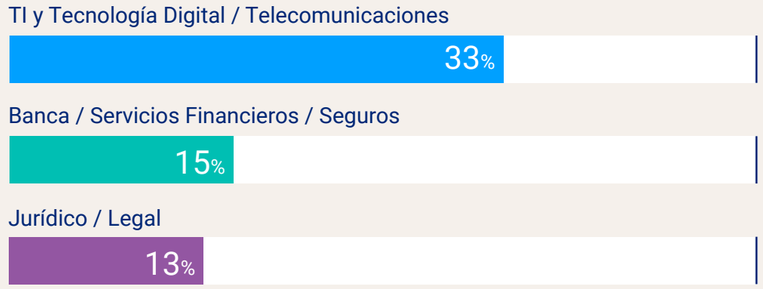
Michael Beaupre
Responsable de Soluciones en Ciberseguridad, Hays CEMEA

ACERCA DE LA **ENCUESTA**

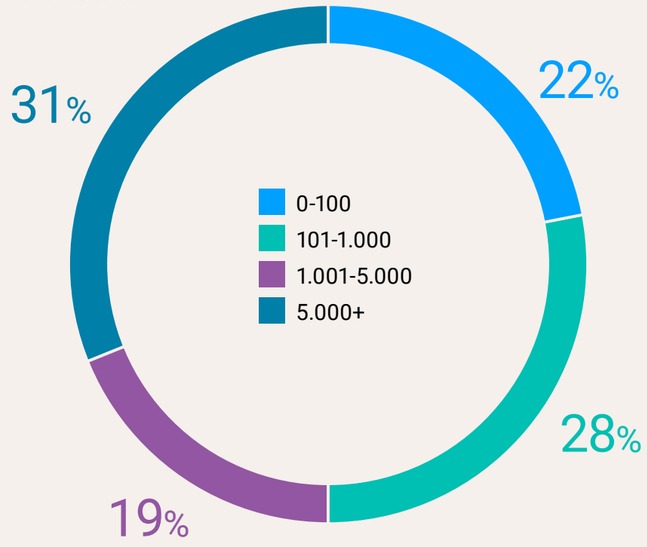
Nuestra encuesta fue completada a finales de 2023 por más de 1.000 líderes en ciberseguridad repartidos por 47 países de todo el mundo. Todos nuestros encuestados, contactados a través de nuestra base de datos global y mediante solicitud directa, han compartido cómo enfocan actualmente sus organizaciones la contratación y retención de personal, cómo esperan que la IA afecte a su trabajo a corto y medio plazo, y la inversión en seguridad.



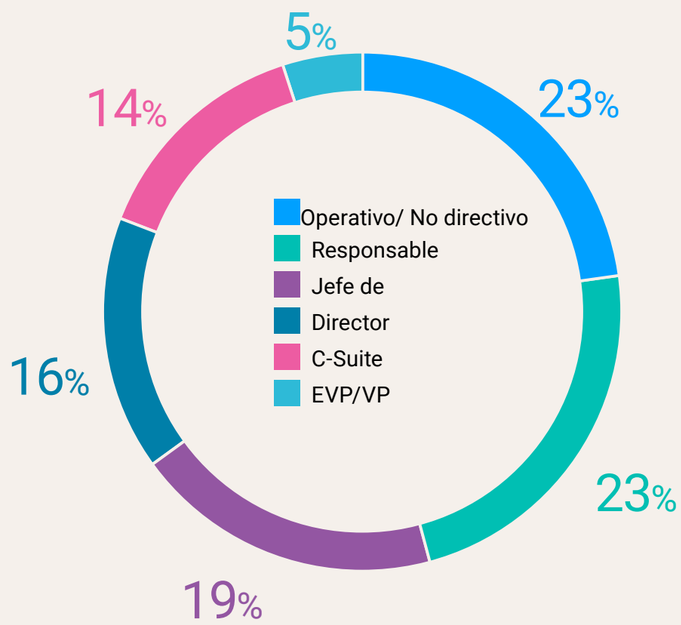
Principales sectores de actividad de nuestros encuestados:



Número de empleados de las organizaciones de nuestros encuestados:



Nivel de senority de los encuestados



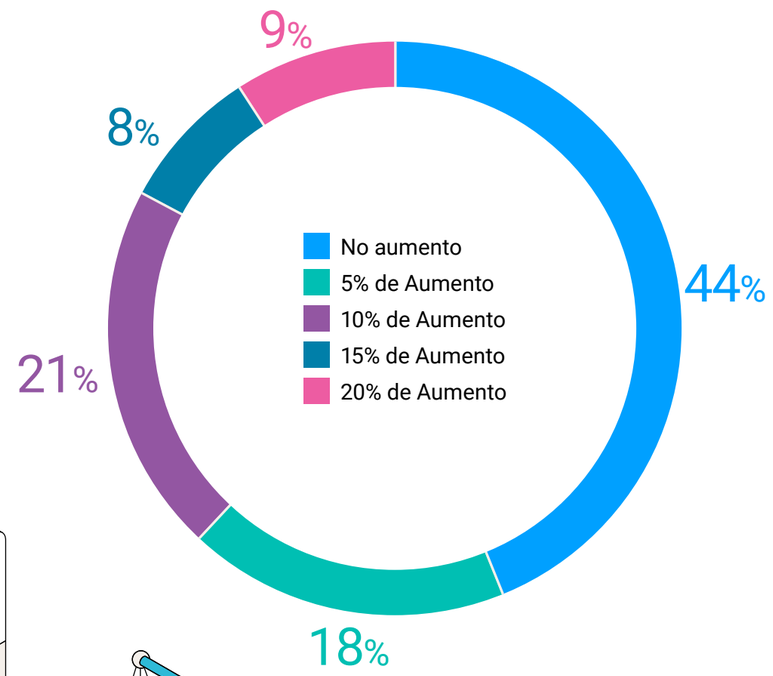
EL RETO: **CONTRATAR Y RETENER TALENTO** CUALIFICADO CON **RESTRICCIONES PRESUPUESTARIAS**

El informe del año pasado reveló que más de la mitad de los encuestados tenían dificultades para atraer a los talentos adecuados. Doce meses después, el panorama no ha cambiado: el 61% de los encuestados no valora muy positivamente su capacidad para atraer cibertalentos.

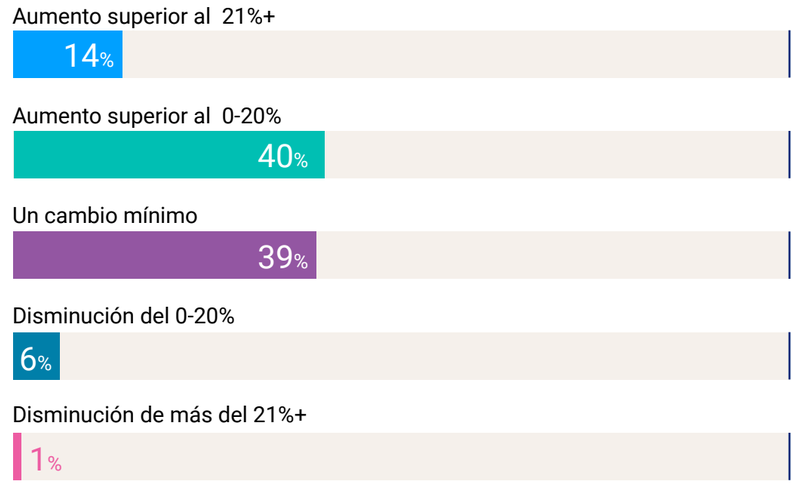
Una de las razones citadas para ello es la falta de trabajadores cualificados disponibles en la reserva de talentos actual. A su vez, esos profesionales pueden exigir unos salarios que muchos empleadores no pueden alcanzar (otro factor común entre nuestros encuestados). De hecho, casi la mitad de los empleadores en 2023 no aumentaron los salarios de los miembros existentes o nuevos de su plantilla de seguridad, mientras que sólo el 17% de los encuestados pudieron ofrecer un aumento salarial superior al 10%.

Además, esta falta de inversión en talento y equipos de ciberseguridad parece que va a continuar. De los encuestados, una mayor proporción de líderes están preocupados por su presupuesto en comparación con los encuestados para el informe del año pasado (72% en 2024, frente al 68% del año pasado). Esto se produce a pesar de que el 54% de los encuestados de este año esperan un aumento de su asignación de gastos (frente al 46% de nuestra encuesta de 2023). Como tal, atraer y retener a profesionales cualificados en ciberseguridad a través de beneficios monetarios es probable que resulte más difícil, haciendo que las alternativas, como el desarrollo de talentos no tradicionales, sean más viables para los empleadores en 2024.

Casi la mitad de los empleadores congelaron los salarios en 2023

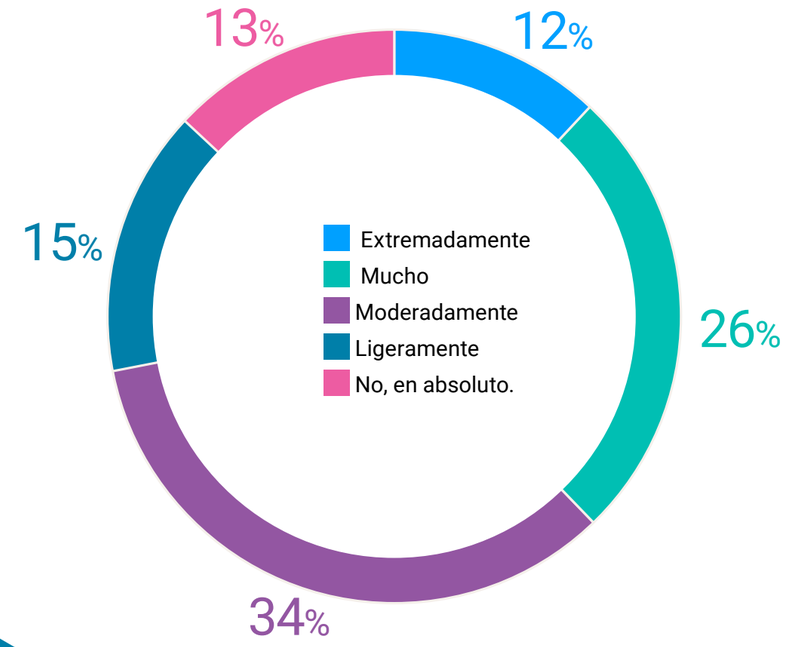


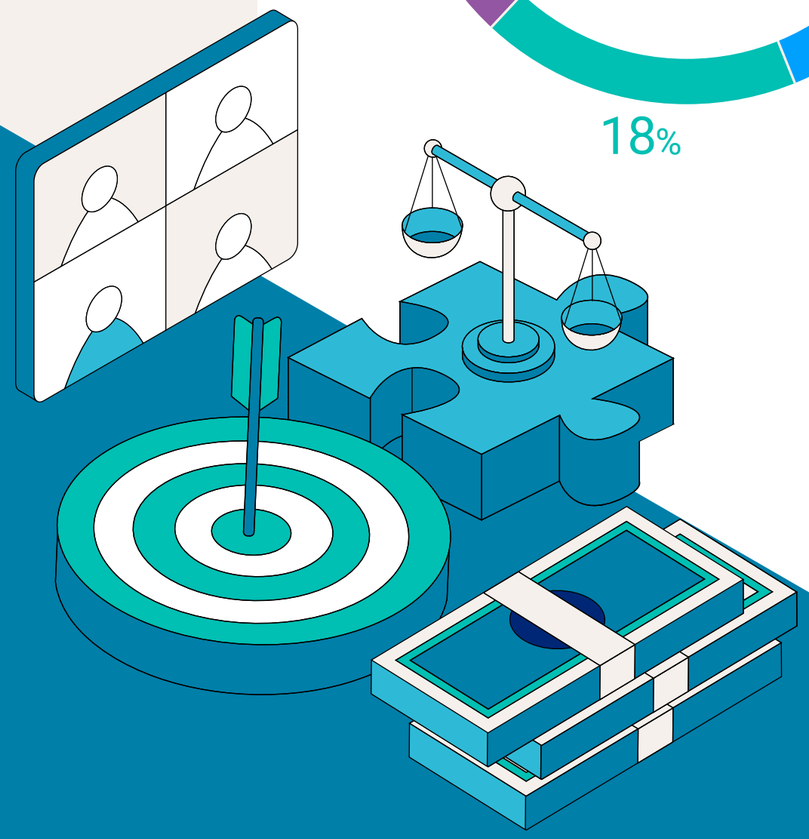
Los líderes en ciberseguridad prevén un aumento del presupuesto



Preocupación por los presupuestos a pesar del aumento

¿Hasta qué punto les preocupa el presupuesto cibernético en 2024?





61% no valora muy positivamente su **capacidad para atraer talentos en ciberseguridad.**

Matthew Cotton

Jefe de Soluciones de Ciberseguridad, ANZ

Nuestro informe ha seguido destacando los retos a los que se enfrentan muchos líderes cibernéticos a la hora de contratar talento cualificado. Como la escasez sigue siendo elevada, también lo son los niveles salariales, lo que crea un entorno desafiante. Esto también está repercutiendo en el nivel de 'agotamiento', que sigue siendo un problema importante en el área cibernética. Las empresas deben considerar formas alternativas de desarrollar su capacidad de capital humano en cibernética. Utilizar y actualizar las competencias de diferentes áreas de la tecnología debe convertirse en un objetivo clave para muchos.

Por ejemplo, los talentos en soporte informático/administración de sistemas ya conocen el panorama de las infraestructuras, las redes y los cortafuegos, etc. Los ingenieros eléctricos y mecánicos pueden convertirse en profesionales cualificados en seguridad OT y, a medida que las universidades siguen invirtiendo en programas de educación cibernética, se crean cada vez más talentos brillantes. Con educación, tutoría y el apoyo adecuado de los empleadores, estas personas son capaces de convertirse en la próxima generación de ciberdefensores.

Christian Toon

Jefe de Servicios Cibernéticos, Pinsent Masons

Identificar y atraer a los cibertalentos requiere una solución específica, lo que puede resultar difícil si implica desafiar el statu quo dentro de su organización. Por ejemplo, las personas dedicadas a la ciberseguridad buscan una mayor flexibilidad, pero, cuando se es un pequeño engranaje de una máquina mucho mayor que trabaja las horas típicas, ¿cómo se hace para cambiar el contrato de una persona? Puede que los contratantes sepan lo que tienen que hacer, pero en realidad se ven limitados por las restricciones.

Piense con originalidad cómo puede ofrecer algo atractivo dentro de los límites de la estructura organizativa. ¿Qué más puede ofrecer, como oportunidades de progresión?

Las actitudes tienen que cambiar porque ahora no contratamos para toda la vida. La mano de obra se mueve con rapidez y usted y sus equipos tienen que estar preparados. Adopte la mentalidad de desarrollar una línea de producción de talento dentro de su equipo.

Sybil VR Kleinmichel

Experta en Ciberseguridad, Hays DACH

Como antigua CISO del Grupo en un banco global, estoy familiarizada con el "Enigma de las Cibercapacidades". Es el dilema con el que viven hoy muchos líderes en ciberseguridad: los riesgos geopolíticos globales y de otro tipo impulsan el gasto empresarial. Esto conduce a la congelación de la contratación, a recortes presupuestarios o a ambas cosas en muchas industrias.

Creo que estamos en una época de los cambios tecnológicos más radicales de la historia, combinados con un aumento significativo de los ciberataques. Esto da lugar a una gran demanda de puestos de trabajo en cibernética y ofrece a los candidatos perspectivas reales de carrera. Para los proveedores de servicios financieros e infraestructuras críticas en Europa, los nuevos y adicionales requisitos normativos aumentan la complejidad. Garantizar una gobernanza, un cumplimiento y una ciberseguridad eficaces son preocupaciones tanto globales como locales. Para gestionar estos riesgos, hay que atraer y conservar a buenas personas.

Muchos encuestados dudan de su capacidad para atraer a grandes talentos. Tú puedes, ofreciendo a tu gente un gran lugar para trabajar, y siendo los mejores líderes que puedas ser. Nuestro informe plantea cuatro prioridades principales de los empleados 1) salarios más altos 2) el deseo de un trabajo flexible/remoto 3) la preferencia por trabajar en organizaciones con un propósito y 4) la necesidad de una continua actualización de conocimientos. Aunque te preocupen tus presupuestos, hay muchas cosas que cada uno de ustedes pueden hacer para atraer a gente buena. ¿Las has tenido en cuenta?

Para los proveedores de servicios financieros e infraestructuras críticas en Europa, **los nuevos y adicionales requisitos normativos añaden complejidad.**

CONSIDERACIONES PARA LOS RESPONSABLES DE CIBERSEGURIDAD

DESARROLLO DEL **TALENTO**

Dado que la contratación de ciberprofesionales cualificados supone un reto para muchos de los encuestados, la formación y el desarrollo ofrecen a las empresas una fuente de talento alternativa.

De los empleadores que luchan por atraer talentos en ciberseguridad, el 61% cita la falta de candidatos cualificados como un factor importante. Dado que los expertos en ciberseguridad con experiencia escasean, una alternativa viable es la contratación o el reciclaje de talentos potenciales que demuestren las habilidades transferibles necesarias para tener éxito en un puesto de seguridad. Es una solución que también puede ayudar a las organizaciones que luchan por ofrecer salarios competitivos a esos candidatos ya cualificados.

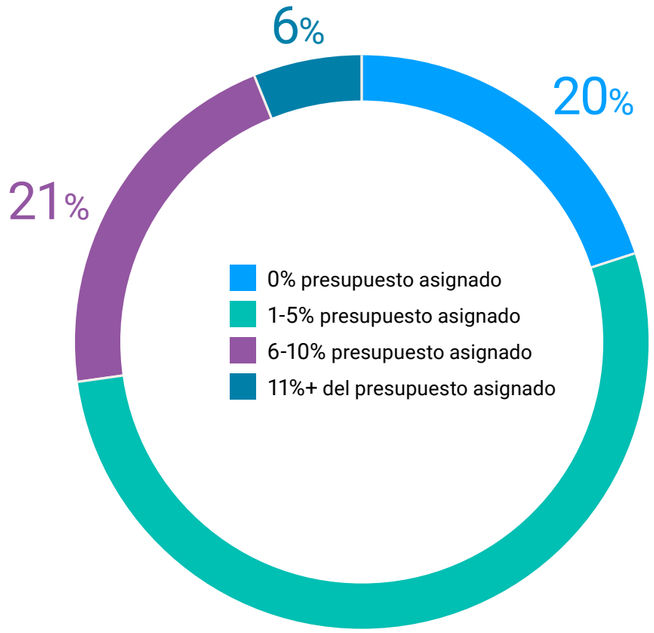
Entre nuestros encuestados, los graduados y los empleados existentes dentro de la organización fueron nombrados como las principales fuentes para su futura mano de obra de ciberseguridad. Sin embargo, es posible que las organizaciones no quieran o no puedan comprometerse a formar o reciclar a personal procedente de esos entornos. Una conclusión clave de nuestra encuesta es que el 62% de los encuestados afirmaron que su empresa no dispone actualmente de un programa interno de desarrollo de talentos para aumentar su plantilla de ciberseguridad. En la actualidad, el 73% de las organizaciones invierte el 5% o menos de su presupuesto de ciberseguridad en el desarrollo de talentos. Mientras tanto, casi el doble de los encuestados considera que cualquier inversión adicional debería dedicarse a la plantilla de ciberseguridad que a los recursos de formación.

En la actualidad, parece que las organizaciones no asumen la responsabilidad de identificar y desarrollar futuros talentos, lo cual es necesario si las empresas se toman en serio la retención de talentos y la cobertura integral de sus carencias de cibercapacidades. Sin una mayor priorización de este riesgo, combinada con un mayor compromiso de los miembros de los consejos de administración para centrarse e invertir en este ámbito, es poco probable que el reto de crear una mejor plantilla de ciberseguridad tenga éxito o sea sostenible.

62%
de las organizaciones no tienen un **programa de desarrollo del talento.**

Escasa inversión en desarrollo de talentos

¿Qué porcentaje de presupuesto de ciberseguridad se destina al desarrollo de talentos?



Dado que los expertos en ciberseguridad con experiencia son escasos, una alternativa viable es **la contratación o la reconversión de talentos potenciales** que demuestren las capacidades transferibles.

Fuentes más populares de futuros talentos

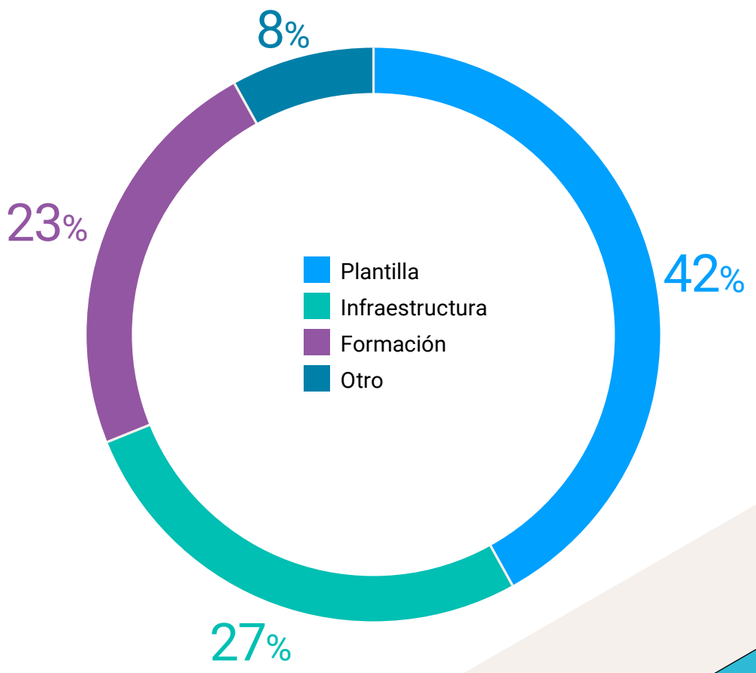
1. Graduados.
2. Internos.
3. Universitarios.
4. Otros.
5. Disciplinas no cibernéticas.

Retos más compartidos en la contratación de talento

1. Expectativas salariales.
2. Escasez de candidatos cualificados.
3. Falta de conocimientos profundos.
4. Falta de experiencia.
5. Competencia de otras empresas.

Los líderes buscan aumentar la plantilla

¿En qué área es más necesaria una inversión adicional?



James Walsh

Director de Soluciones de Ciberseguridad, Hays UK&I

"El informe de este año ha puesto de relieve la escasez de talento cibernético "preparado" a escala mundial. No existe un remedio inmediato para este difícil escenario, pero sin duda hay enfoques que las organizaciones pueden adoptar para mitigar y cambiar este paradigma.

Una solución sostenible empieza por que los departamentos cibernéticos y sus respectivas organizaciones pasen de considerarse simplemente "consumidores de cibertalentos" a ser "creadores de cibertalentos".

Esto puede lograrse aprovechando los numerosos programas de formación existentes para emplear y desplegar talentos tanto de dentro como de fuera de su organización. Sin embargo, el éxito depende de la implicación de la alta dirección y de los departamentos de RRHH/Talento, con la aportación de los equipos cibernéticos/técnicos.

A lo largo de mis años de trabajo en este sector, puedo afirmar sin temor a equivocarme que no faltan ganas de trabajar y de perfeccionarse en ciberseguridad. El reto, en cambio, es superar la constante necesidad percibida de talento "ya hecho"

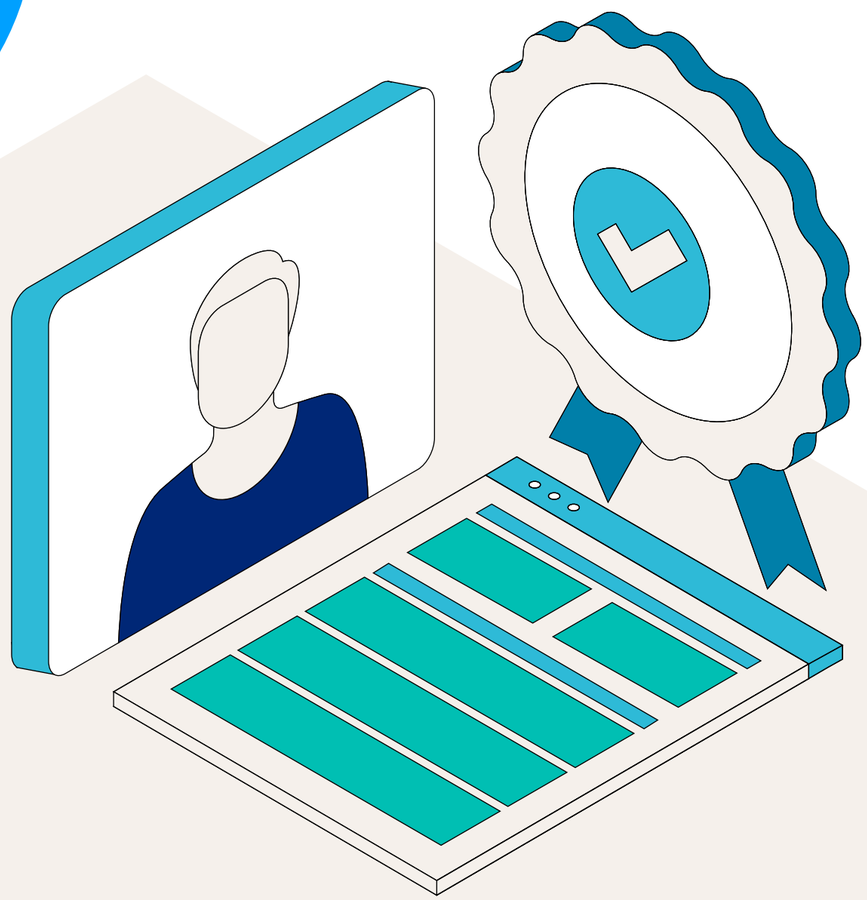
Neil Khatod

Director de Soluciones de Ciberseguridad, Hays Américas

"Cuando me incorporé a Hays, reflexioné sobre la aplicación de algunos conceptos clave que aprendí en el ejército: como soldado, se nos enseña a no aceptar nunca la derrota, ni abandonar a un camarada caído. Esto puede parecer etéreo, pero aplicar estas ideas a la lucha cibernética puede significar la diferencia entre el éxito de un equipo y sucumbir ante los delincuentes. Es esa determinación y ese trabajo en equipo lo que dice que debemos defender, que debemos ganar y que debemos encontrar la forma de adaptarnos como equipo.

La creación de esta mano de obra no se consigue, así como así. Las empresas tienen que buscar personas adaptables, comprometidas, que aprendan durante toda la vida y que tengan facilidad para resolver problemas técnicos. A menudo pasados por alto, los increíbles y comprometidos profesionales que abandonan el ejército pueden resolver y han resuelto muchos retos en el ámbito cibernético. He tenido el privilegio de ver a estos ciberprofesionales militares en acción, y puedo hablar de primera mano de los beneficios y el nivel de talento que supone incorporarlos a un equipo.

Como los delincuentes se adaptan constantemente, nuestra fuerza de trabajo defensiva debe hacer lo mismo. Depende de nosotros, los líderes, fomentar un cuadro de aprendices de por vida."



Una solución sostenible empieza por que los departamentos cibernéticos y sus respectivas organizaciones pasen de considerarse simplemente **"consumidores de cibertalentos"** a ser **"creadores de cibertalentos".**

INTELIGENCIA ARTIFICIAL (IA) Y AUTOMATIZACIÓN

El impacto de la Inteligencia Artificial en el mundo laboral ofrece a la vez una solución y plantea un reto para los equipos de ciberseguridad de todo el mundo.

Aunque existe una creencia generalizada entre los encuestados (89%) de que la IA resultará útil para mejorar las capacidades de seguridad, casi la mitad de los líderes cree que la automatización no provocará una pérdida de puestos de trabajo, y sólo el 36% predice que lo hará de aquí a 2026. Ante este impacto previsto, que sugiere que las herramientas de IA podrían implantarse para apoyar a los profesionales en lugar de sustituirlos, la mejora de las competencias y la formación en estas tecnologías se convierte en una prioridad aún mayor.

A pesar de ello, la implantación va con retraso. Sólo el 57% de los encuestados habrá formado a su personal de ciberseguridad en herramientas de IA en el próximo año, y una cuarta parte de los líderes afirma que no tiene previsto hacerlo en absoluto.

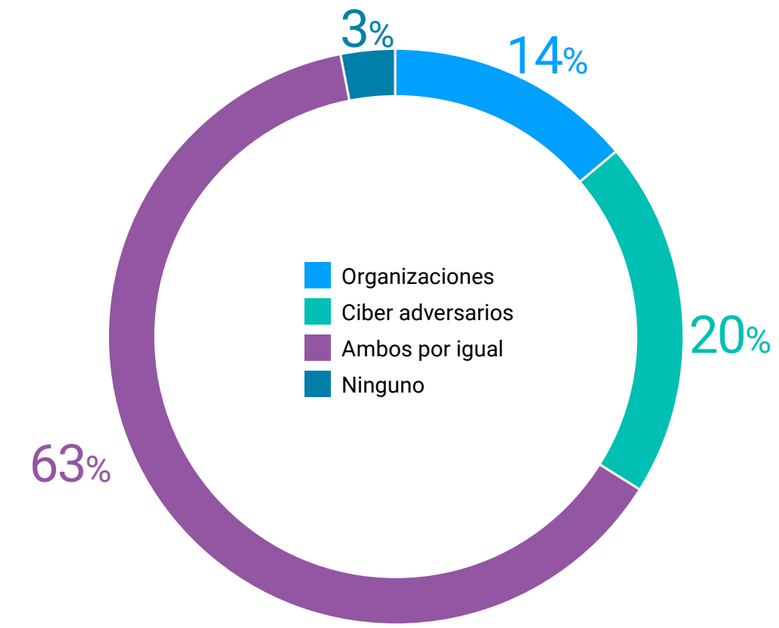
La Unión Europea ha publicado el proyecto de reglamento sobre la Ley de IA, que incluye, entre otras cosas, requisitos para los sistemas de IA de alto riesgo. Éstos tendrán que cumplir una amplia gama de condiciones, sobre todo relacionadas con la gestión de riesgos, las pruebas, la solidez técnica, la formación y la gobernanza de los datos, la transparencia, la supervisión humana y la ciberseguridad (artículos 8 a 15). Esto significa que existe una necesidad real de que las empresas garanticen una competencia y supervisión adecuadas de la IA. Si el 25% de los líderes que respondieron no están planificando la capacitación en IA de sus plantillas, este statu quo puede representar un riesgo que todavía no se está supervisando adecuadamente.

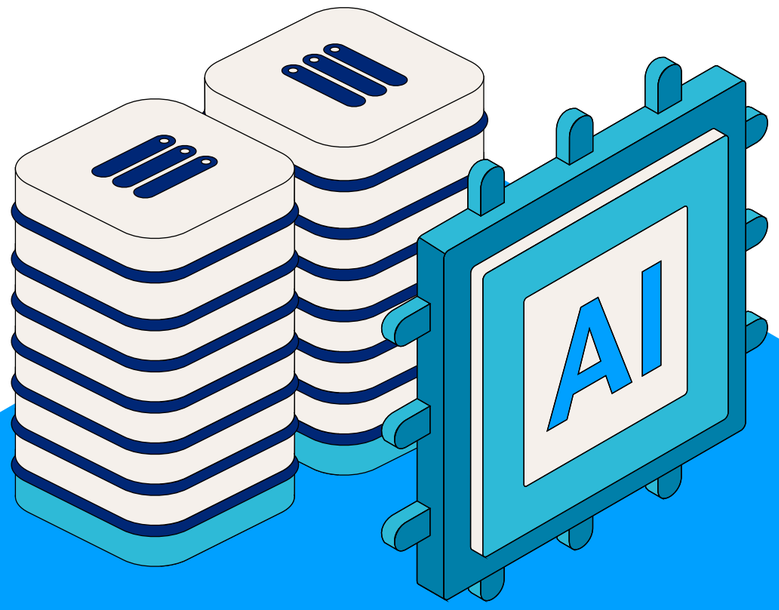
Estas actitudes se producen en un contexto de gran preocupación por los ciberataques basados en la IA. Aunque la mayoría de los encuestados cree que esta tecnología en rápida evolución beneficiará por igual tanto a las organizaciones como a los ciberdelincuentes, existe una mayor sensación de que los adversarios ganarán la partida.

No adoptar estas tecnologías, aunque sea en un marco seguro y rígido, puede dejar a las organizaciones jugando a ponerse al día con los atacantes, que son más rápidos en explorar y utilizar las vulnerabilidades. Se trata de puntos débiles creados (como en el caso de los mejores correos de phishing) o identificados (como dentro de las vulnerabilidades conocidas públicamente) con IA. Dado que casi la mitad de nuestros encuestados indicaron que no tienen previsto formar a su personal en esta tecnología y las herramientas disponibles en un futuro inmediato, se ha puesto de manifiesto otra tendencia preocupante.

La IA brinda oportunidades a todas las partes

¿Quién obtendrá la mayor ventaja de la evolución de la IA?



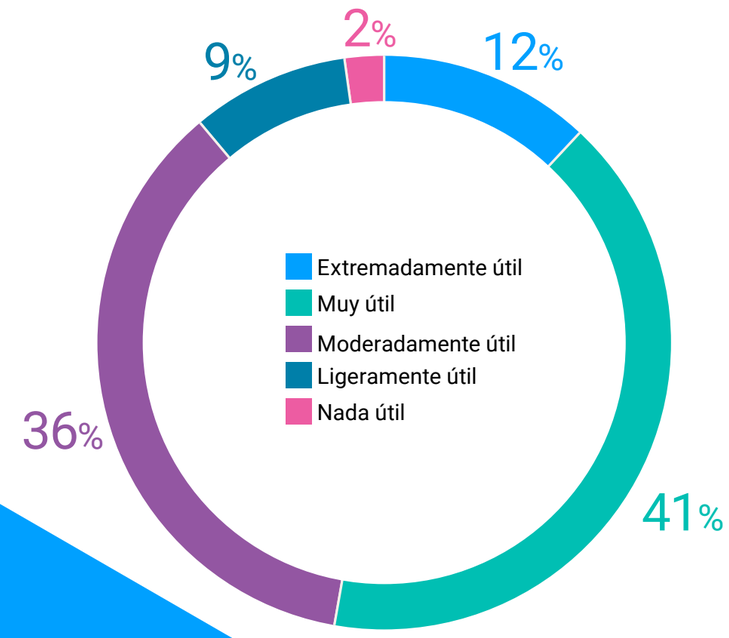


89%

se preocupan por los riesgos potenciales de las amenazas de la IA.

La IA tiene un papel que desempeñar en el desarrollo del talento

¿Hasta qué punto será útil la IA para que las organizaciones desarrollen las capacidades de sus equipos de ciberseguridad?



Las organizaciones están divididas sobre si la IA puede sustituir eficazmente al talento en ciberseguridad

Julia Dudenko
CISO,
Haniel

"Es hora de empezar a explorar las herramientas de IA, pero hay que enmarcarlo como una exploración. Desde el punto de vista de la ciberseguridad, tenemos que explicar claramente los riesgos del uso de la IA. Cuando se elabora una hoja de ruta de la IA, es importante encontrar el equilibrio entre aprovechar los beneficios, pero, al mismo tiempo, crear un marco muy sólido para orientar a los empleados sobre lo que pueden hacer con la IA. Si algo no está bien, ¿cuál es el riesgo? ¿Qué puede ocurrir para tener un diálogo muy abierto sobre esto? Y creo que esto ayuda de nuevo, la comprensión ayuda de nuevo entonces a abrazar las oportunidades de la IA.

Por un lado, la IA nos ayuda a aumentar la eficiencia, por lo que podríamos reducir el número de empleados. Al mismo tiempo, la IA utilizada por los delincuentes aumenta el número de ataques y su sofisticación, por lo que podríamos necesitar más personal para combatirla."

Jason Yuen
Socio de Consultoría Tecnológica y Líder de Ciberseguridad en Malasia
EY

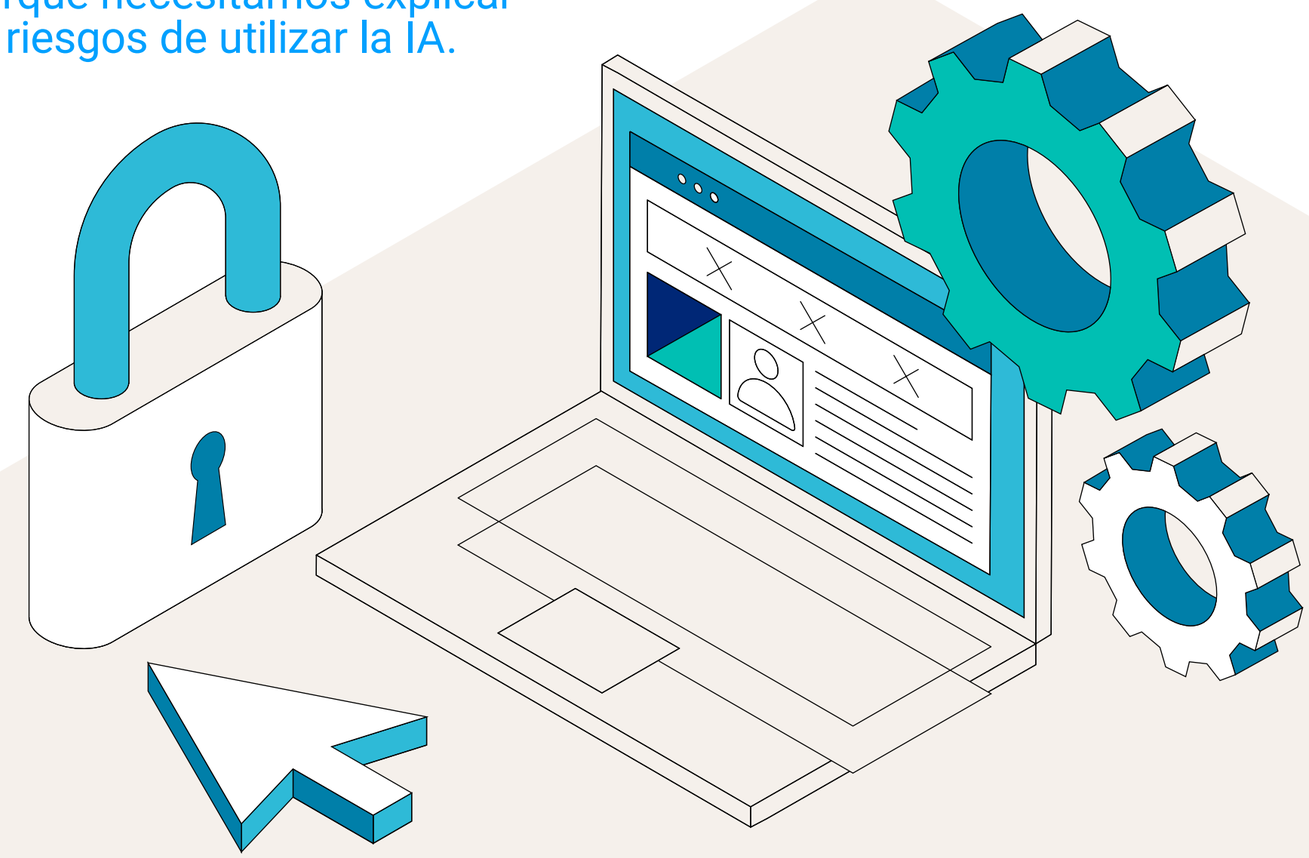
"Hay tal escasez de profesionales en ciberseguridad que no creo que la IA afecte a los puestos de trabajo a corto o medio plazo. En primer lugar, ¡simplemente no tenemos suficientes personas!

Donde veo que la IA nos ayudará es en la velocidad de análisis. Por ejemplo, ¿qué es lo que hay que arreglar en mi infraestructura? ¿Dónde están mis puntos débiles? ¿Dónde es más probable que ataquen los delincuentes? Y creo que la velocidad a la que la IA puede cotejar, por ejemplo, los tipos de ataques frente a los que mi organización es potencialmente susceptible, es realmente útil. Tradicionalmente, cotejar esta información llevaría demasiado tiempo o simplemente no merecería la pena.

Aquí es también donde veo que los profesionales de la ciberseguridad aportan valor: siendo capaces de hacer estas preguntas y dirigir los recursos hacia donde hay que poner remedio de una forma más eficiente."

Las organizaciones recurren a la IA para la seguridad

Es hora de empezar a **explorar las herramientas de IA**, pero debe enmarcarse como una exploración, porque necesitamos explicar claramente los riesgos de utilizar la IA.



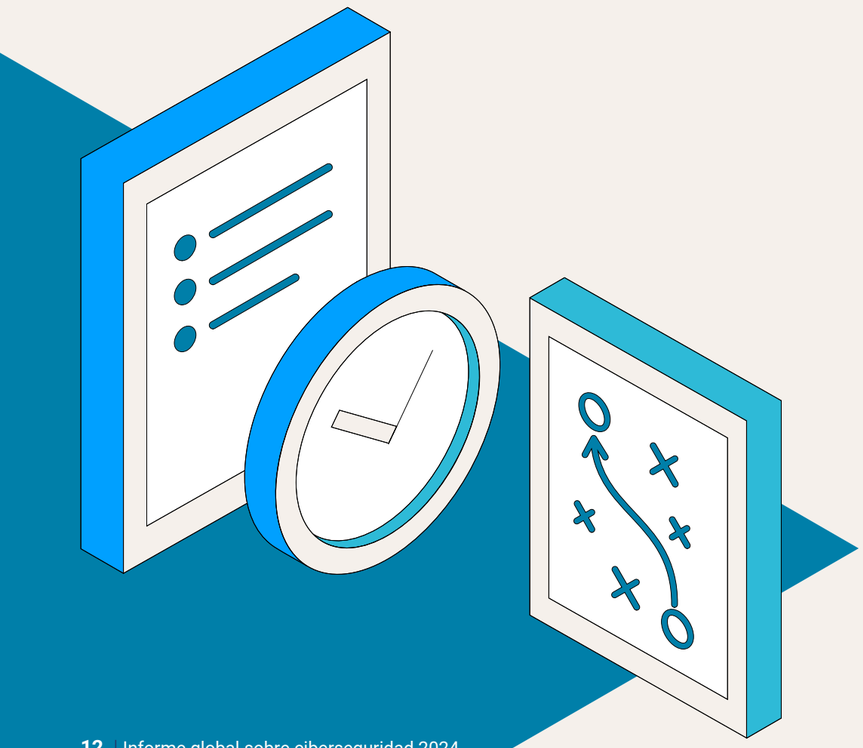
PLAN DE **ACCIÓN**

Este informe ha dejado claro hasta qué punto los responsables de ciberseguridad de todo el mundo están luchando por incorporar el talento cualificado que se necesita en el mundo actual.

Los factores económicos mundiales siguen limitando la inversión que las organizaciones están dispuestas a hacer en seguridad, lo que repercute aún más en las oportunidades de aumentar la plantilla o pagar salarios competitivos en una situación en la que las competencias son escasas.

Explorar el talento no tradicional puede permitir a tu organización cerrar esta brecha de habilidades con un esfuerzo de inversión menor. Sin embargo, tal y como están las cosas, muchos empleadores no están proporcionando acceso a la formación adecuada, un problema que va a empeorar a medida que la IA evoluciona rápidamente.

Si tu organización se enfrenta a los mismos retos que muchos de nuestros encuestados, tenemos varias recomendaciones y pasos a seguir para ti.



1.Fíjate en el talento no tradicional:

Si tienes en cuenta a personas con aptitudes transferibles, que pueden carecer de experiencia pero están dispuestas a desarrollarse, para puestos dentro de tu plantilla de ciberseguridad, tu organización aún puede encontrar buenas soluciones. Para hacerlo con eficacia, te recomendamos que amplíes tu búsqueda a candidatos con aptitudes en TI en general y en otras disciplinas, sobre todo en funciones de administración y desarrollo. En Hays, hemos ayudado a clientes de todo el mundo a identificar y evaluar a los candidatos adecuados para dar el paso a la ciberseguridad. También ofrecemos servicios de asesoramiento cibernético, que incluyen que uno de nuestros expertos cualificados (antiguos CISO, CIO y COO) evalúe tu situación actual antes de diseñar una hoja de ruta de cibercapacidades. Esta hoja de ruta se adapta a tu situación actual de cumplimiento de las normas de seguridad informática y cibernética y a tu estrategia de seguridad de la información.

2. Diseña una estrategia de formación para garantizar un éxito sostenible:

Independientemente del nivel de experiencia de tu personal cibernético, para garantizar una seguridad sostenible es necesario actualizar continuamente sus conocimientos. Las empresas citaron las oportunidades de formación como una de las mejores medidas para atraer talento y retener al personal existente. Si actualmente no puedes ofrecer un plan de desarrollo para todos, diseñar una estrategia de formación para la mejora de las cibercapacidades en tu organización puede ayudarte a garantizar que puedes beneficiarte de la contratación de cibertalentos no tradicionales.

3.Adopta las tecnologías emergentes y asegúrate de que el equipo esté informado de las ventajas y los inconvenientes:

Las organizaciones deben adaptarse rápidamente a un mundo en el que las soluciones de IA son cada vez más sofisticadas a un ritmo que no habíamos visto antes. Aunque aún está por determinar hasta qué punto los trabajadores cualificados pueden utilizar estas herramientas, nuestro estudio muestra que los encuestados creen firmemente que la IA puede apoyar las capacidades de su equipo. Para que las organizaciones puedan aprovecharla plenamente, estas herramientas deben incorporarse a la formación y el desarrollo del personal de seguridad. Los líderes de ciberseguridad deben colaborar con la junta directiva en un marco para utilizar estas herramientas con el fin de defenderse de los ciberadversarios que pueden utilizarlas sin tener en cuenta el cumplimiento de la normativa o la legalidad.

4.Explorar la posibilidad de incorporar contratistas o asesores cibernéticos de Hays

Aunque una plantilla permanente puede exceder el presupuesto de tu organización, la contratación de “profesionales contratados” ad hoc puede ser una solución asequible y adecuada para cubrir hoy tu déficit de competencias cibernéticas. Las tendencias apuntan a que las empresas aumentarán su demanda de contratistas técnicos en 2024, algo en lo que Hays apoya a sus clientes con regularidad. Si tu organización necesita servicios de operaciones cibernéticas, a corto plazo o a tiempo parcial, puede que te resulte beneficioso plantearte un cambio de enfoque a la hora de contratar para puestos como Ingenieros de Gestión de Información y Eventos de Seguridad (SIEM) o de Orquestación, Automatización y Respuesta de Seguridad (SOAR), o consultores de Inteligencia sobre Ciberamenazas. Hays ofrece asociaciones con organizaciones acreditadas que pueden prestar estos servicios bajo demanda para que puedas centrarte en tu actividad principal. Si no estás seguro de qué enfoque es el más deseable o eficaz, nuestros asesores cibernéticos de Hays pueden ayudarte con un análisis “como está/como debería estar”, identificando las ganancias rápidas y ayudándote a elevar la planificación estratégica de todo tipo de opciones de empleo y externas para garantizar una dotación adecuada de recursos cibernéticos.

5.Garantiza la flexibilidad y las oportunidades de trabajo a distancia para atraer y retener el talento:

Los encuestados enumeraron las oportunidades de trabajar a distancia, el equilibrio adecuado entre la vida laboral y personal y una mayor flexibilidad como beneficios enormemente populares entre los candidatos y los trabajadores actuales. Si tu organización no ofrece actualmente estas ventajas al personal fijo o contratado, es probable que te resulte más difícil contratar y conservar el talento adecuado en 2024.

PERSPECTIVAS **REGIONALES**

Aunque en este informe se han destacado las tendencias y los retos mundiales, en nuestro estudio hay ejemplos de ciertos países que se desvían del consenso. Hemos seleccionado algunos datos destacados de los países con mayor número de encuestados que ofrecen más información.

Australia

- El 65% ha aumentado su plantilla en 2023, frente al 53% en todo el mundo.
- Sólo el 40% ve un aumento de su presupuesto en 2024, frente al 54% global.
- A pesar de ello, sólo el 58% de los encuestados están “En extremo”, “Muy” o “Moderadamente” preocupados por su presupuesto (72% en todo el mundo).

China

- El “Equilibrio trabajo-vida privada/Bienestar” es la estrategia de retención más citada, mientras que el “Trabajo a distancia/ Híbrido” fue la más popular a nivel mundial.

Francia

- Los “beneficios monetarios” se citaron como el método número uno para atraer talentos, pero no se encontraban entre las cinco razones principales a nivel mundial.
- Así, sólo el 31% de los encuestados afirmaron que no ofrecían un aumento salarial en 2023, frente al 44% en todo el mundo.
- Un tercio de los encuestados cree que la IA beneficiará más a los ciberadversarios, mientras que sólo el 5% afirma que dará ventaja a las organizaciones (estos porcentajes son del 20% y el 14% respectivamente en todo el mundo).
- Sólo el 24% cree que la IA no afectará a la plantilla, frente al 44% global. De hecho, el 57% cree que tendrá un impacto dentro de dos años, un aumento significativo respecto al 36% mundial.
- Aproximadamente dos tercios de los encuestados (66%) afirman que su presupuesto aumentará en 2024, frente al 54% en todo el mundo.
- A pesar de ello, el 86% está “En extremo”, “Muy” o “Moderadamente” preocupado por su presupuesto, frente al 72% mundial.
- El 38% afirma que más del 5% de su presupuesto de ciberseguridad se destina al desarrollo del talento, un porcentaje significativamente superior al de los encuestados que gastan esa cantidad en todo el mundo (26%).

Alemania

- El 55% de los encuestados no cree que la IA vaya a afectar a la plantilla (frente al 44% global)

Japón

- El 26% de los encuestados ha informado de un aumento de la plantilla en 2023, frente al 53% global.
- Sólo el 23% califica su capacidad para atraer talento como “Alta” o “Muy alta” (39% en todo el mundo).
- Sin embargo, el 74% no ha ofrecido un aumento salarial en 2023, frente al 44% mundial
- El 97% está “En extremo”, “Muy” o “Moderadamente” preocupado por los ataques de IA, frente al 88% a nivel mundial.
- Sólo el 34% habrá empezado a formar a su plantilla en herramientas de IA en el próximo año, frente al 57% en todo el mundo. Asimismo, el 53% no tiene previsto hacerlo, más del doble que la respuesta global (25%).
- Los encuestados consideran que la inversión adicional en formación es más importante que en personal.

Malasia

- Las empresas que valoran muy positivamente su capacidad para atraer talentos mencionan la oferta de desarrollo y crecimiento profesional, así como los beneficios monetarios. Globalmente, los encuestados creen que son más atractivas las mayores oportunidades de flexibilidad y conciliación de la vida laboral y familiar.
- En contraste con la opinión global, son más los encuestados que creen que la IA beneficiará a las organizaciones frente a los ciberadversarios.
- Sin embargo, el 98% está “En extremo”, “Muy” o “Moderadamente” preocupado por los ataques de IA, frente al 88% global.
- Sólo el 20% está formando actualmente a su personal en herramientas de IA, mientras que la proporción mundial es del 32%.
- Sólo el 31% cree que la IA no afectará a la plantilla, frente al 44% mundial.
- El 72% espera que su presupuesto aumente el año que viene, mucho más que el 54% global.
- A pesar de ello, el 92% está “En extremo”, “Muy” o “Moderadamente” preocupado por su presupuesto, frente al 72% mundial.

Singapur

- Sólo el 28% valora positivamente su capacidad para atraer talento, frente al 39% mundial.
- Sólo el 11% no tiene previsto formar a los trabajadores en herramientas de IA, muy por debajo del 25% mundial.
- En cuanto al personal, sólo el 21% prevé que la IA no afectará al personal, frente al 44% mundial. El 55% cree que tendrá un impacto dentro de dos años, muy por encima del 36% mundial.
- El 89% está “En extremo”, “Muy” o “Moderadamente” preocupado por su presupuesto, frente al 72% mundial.

Reino Unido

- Tres veces más encuestados consideran que la IA beneficia a los ciberadversarios (27%, frente al 20% mundial) que a las organizaciones (9%, frente al 14% mundial).
- El 61% de los encuestados están “En extremo”, “Muy” o “Moderadamente” preocupados por su presupuesto en 2024, lo que supone un notable descenso respecto al 72% mundial.

EE.UU.

- Sólo el 47% de los encuestados no valoran muy positivamente su capacidad para atraer talento, frente al 61% a nivel mundial.
- El 47% de los encuestados tiene un programa de desarrollo de talentos dentro de su organización, frente a sólo el 38% a nivel mundial.
- Sólo el 77% de los encuestados están “En extremo”, “Muy” o “Moderadamente” preocupados por los ataques de IA, mientras que la cifra mundial es del 88%.
- El 42% está formando actualmente a la plantilla para utilizar herramientas de IA, lo que supone un aumento significativo respecto al 32% global.
- Asimismo, el 60% de los encuestados no cree que la IA vaya a afectar a la plantilla, mientras que la media global es del 44%.

SOBRE NOSOTROS

En Hays, invertimos en asociaciones para toda la vida que permitan a las personas y a las empresas alcanzar el éxito. Sabemos que en un mercado tan cambiante como el tecnológico, es aún más importante proporcionar a las organizaciones un acceso rápido a los mejores talentos que marcarán una verdadera diferencia. Llevamos años cultivando un ecosistema de candidatos únicos y muy comprometidos, y trabajaremos contigo para hacer crecer o ampliar tu empresa utilizando nuestra experiencia única en sectores y tecnologías. Nuestros conocimientos se basan en la experiencia, la inteligencia y los datos, y son posibles gracias a nuestra inversión en nuevas tecnologías y sistemas.

Como socio de confianza de organizaciones de todo el mundo, tanto si necesitas un profesional como un equipo nuevo, podemos ayudarte a planificar el mañana.

Si estás interesado en debatir las conclusiones o recomendaciones de nuestro informe, ponte en contacto con tu representante local de Hays hoy mismo. Estaremos encantados de discutir las soluciones adecuadas para las necesidades de tu organización.

Americas – Neil.Khatod@hays.com
Asia – Mohammad.Qasim@hays.com.my
Australia and New Zealand – Matthew.Cotton@hays.com.au
CEMEA – Michael.Beaupre@hays.de
UK and Ireland – James.Walsh1@hays.com

Obtén más información en: expertsintechnology.hays.com
Hays.com.co
Hays.com.mx
Hays.cl

Expertos en
Tecnología