

Adopción de la inteligencia artificial en las áreas de ciberseguridad en América

2024

Índice

- 03 Introducción
- 05 Metodología
- 06 Adopción de la Inteligencia Artificial (IA) en las áreas de ciberseguridad en América Latina
- 11 Madurez y expectativas de la IA en el área de ciberseguridad
- 13 Beneficios y barreras para la implementación de la IA en ciberseguridad
- 15 Conclusiones y retos

Introducción

América Latina, al igual que el resto del mundo, se encuentra en una era digital en constante desarrollo que introduce avances tecnológicos revolucionarios que impulsan a las personas y a las empresas a actualizar sus conocimientos para destacar en el competitivo y exigente mercado actual. Aunque hay ciertas dudas sobre el uso de la inteligencia artificial (en adelante IA), esta tecnología se está posicionando como un motor de cambio, de evolución y de eficiencia en las grandes organizaciones.

Y es que, según el estudio que ya publicamos en NTT DATA realizado conjuntamente con el MIT, hay un evidente crecimiento en adopción de la IA, con un salto significativo del 58% en 2020 al 71% en 2023.

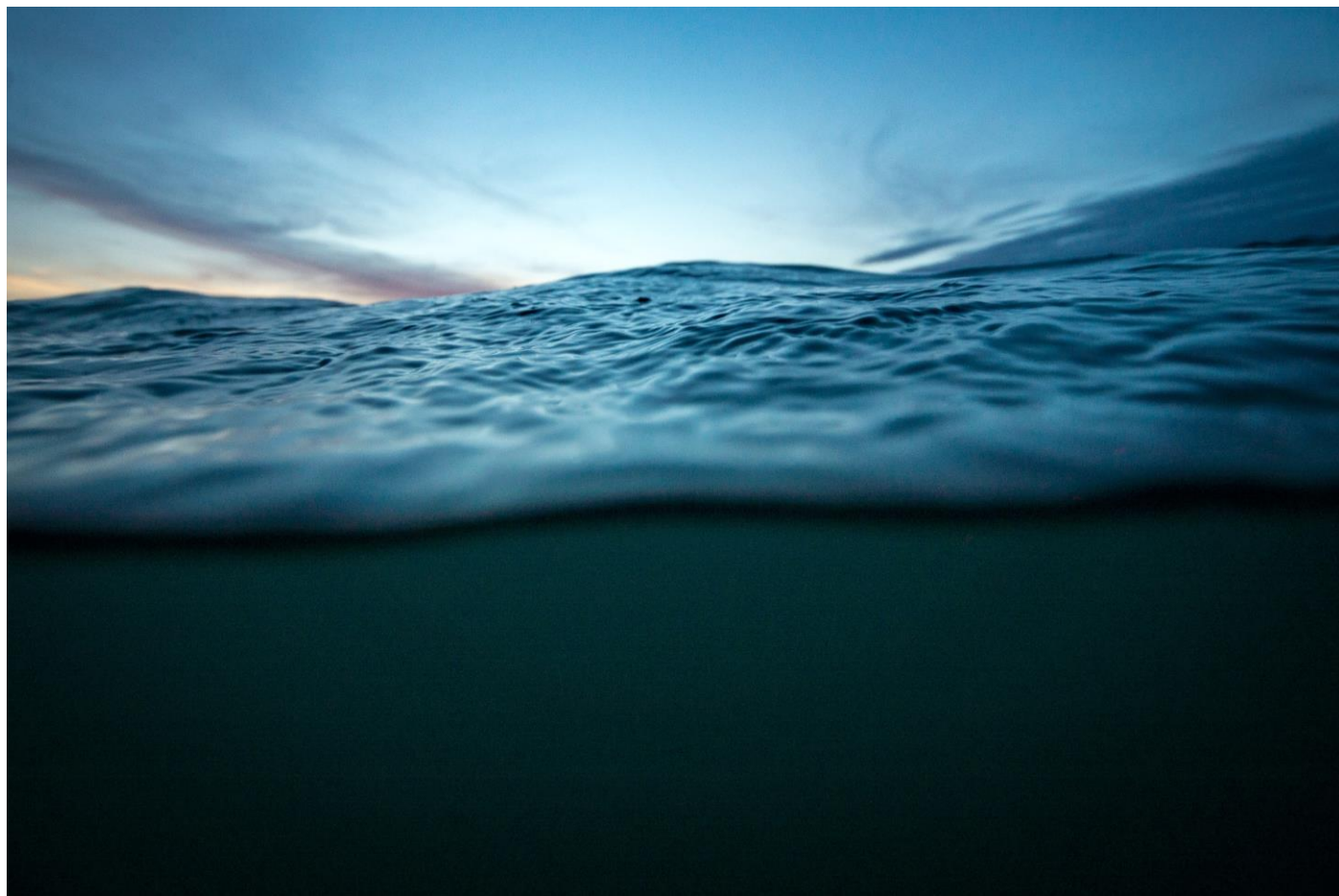
En este proceso, hay ámbitos específicos de una organización donde vale la pena entrar al detalle en cómo puede la IA ayudar a transformar ese ámbito. En particular, en este informe analizaremos cómo la IA puede transformar las áreas de ciberseguridad.

Los equipos de ciberseguridad, por la naturaleza de su trabajo, se someten a un constante flujo creciente de datos proveniente de fuentes internas (monitoreo de seguridad) y externas (inteligencia de amenazas), que en muchos casos deben ser procesados en tiempo y forma para garantizar la protección de los activos.

En el presente informe se pretende

explorar cómo las organizaciones de América Latina están viendo la adopción de la IA en las áreas de ciberseguridad. Para ello además de apoyarnos en la información obtenida en la encuesta principal (120 encuestas realizadas más 10 entrevistas), se ha extendido una encuesta a CISOs y oficiales de ciberseguridad que han respondido 32 organizaciones de los siguientes países: Argentina, Brasil, Chile, Colombia, Ecuador, México y Perú, además de que se han obtenido respuestas de organizaciones de ámbito regional.

La información incluida en este informe es información agregada de las respuestas obtenidas, puesta bajo la perspectiva que tenemos sobre IA y sobre ciberseguridad en NTT DATA.



Países participantes del estudio



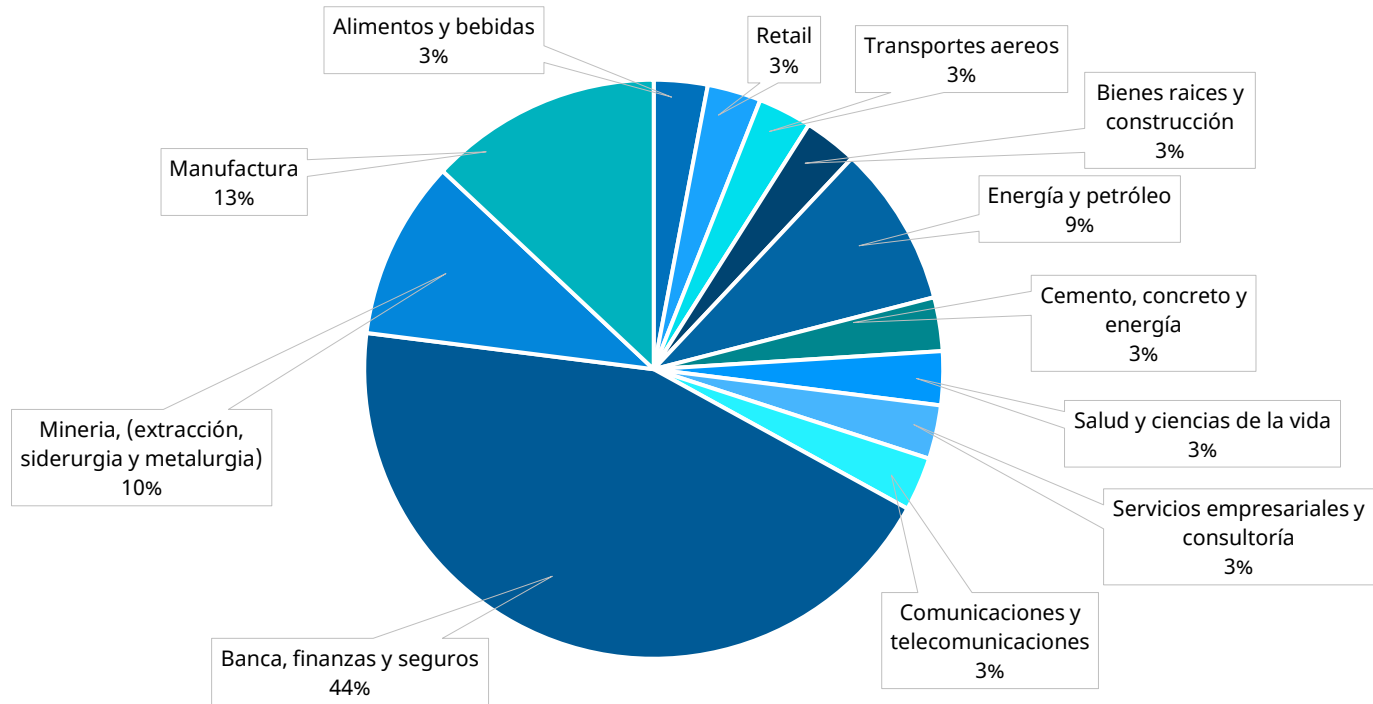
Metodología

Para entender cómo se percibe la madurez de la Inteligencia Artificial desde las áreas de ciberseguridad en las empresas de América Latina, además de apoyarnos en la información obtenida en la encuesta principal (120 encuestas realizadas más 10 entrevistas), se ha extendido una encuesta específica sobre adopción de IA en ciberseguridad a

CISOs y oficiales de ciberseguridad que han respondido 32 organizaciones de los siguientes países: Argentina, Brasil, Chile, Colombia, Ecuador, México y Perú, además de que se han obtenido respuestas de organizaciones de ámbito regional. Cabe resaltar que estos *insights* se

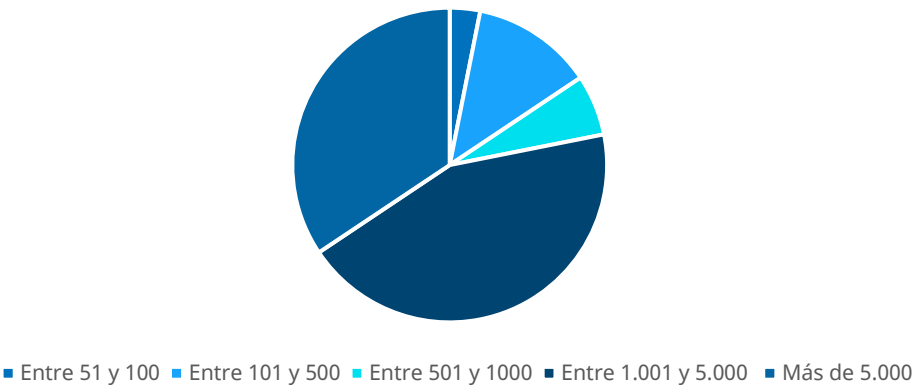
han obtenido de personas que juegan el rol de CISO o un rol relevante en las áreas de ciberseguridad. La muestra engloba diferentes sectores, siendo el sector de finanzas y seguros, y rubros pertenecientes a industria (minería, manufactura), quienes han mostrado una mayor curiosidad por el informe y los resultados en el proceso.

Sector de las empresas participantes



Finalmente, las compañías participantes en esta segunda encuesta orientada a adopción de la IA en ciberseguridad son empresas grandes y relevantes en el mercado latinoamericano.

Empleados de empresas participantes



Percepción sobre la adopción de la Inteligencia Artificial (IA) en las áreas de ciberseguridad en América Latina

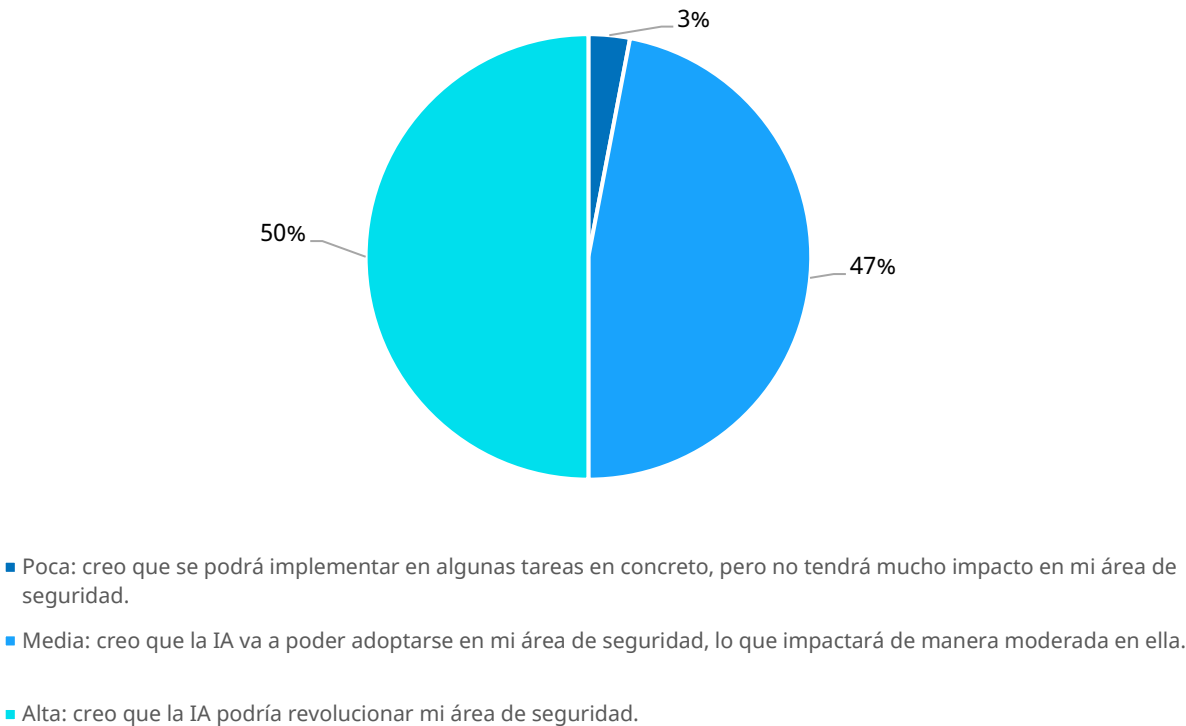
“ IA es un copiloto y nos puede ayudar mucho a ahorrar tiempo en la detección y análisis de eventos, pero siempre tiene que ser supervisada. *CISO de empresa de Industria, Chile*

El estudio de 2023 procura proporcionar un análisis exhaustivo sobre la consolidación y el avance de la IA en la región. Como resultado se evidencia un notorio crecimiento en su adopción, con un salto significativo del 58% en 2020 al 71%

en 2023. También se adentra en los desafíos significativos que enfrentan las empresas en la región, como la falta de conocimientos técnicos especializados y recursos financieros adecuados para la implementación efectiva de soluciones basadas en IA.

Un 20% de las empresas todavía no han incorporado la IA en sus operaciones, marcando un amplio margen para la expansión y el crecimiento futuro en la adopción de esta tecnología emergente.

Potencial de la IA percibida para las áreas de seguridad



El primer paso para adoptar una tecnología en un área es reconocer su impacto y su potencial. En el caso de la IA, casi la totalidad de las compañías reconoce que va a tener un impacto medio o alto respecto a la mejora y eficiencia de las tareas del área de ciberseguridad.



El uso de la IA irá incrementándose con el tiempo como parte de las soluciones de seguridad que venimos utilizando, por lo que su adopción en las empresas será incremental, las marcas cuyos productos no empiecen a utilizar la IA corren el riesgo de ser reemplazadas por las que si lo hagan.

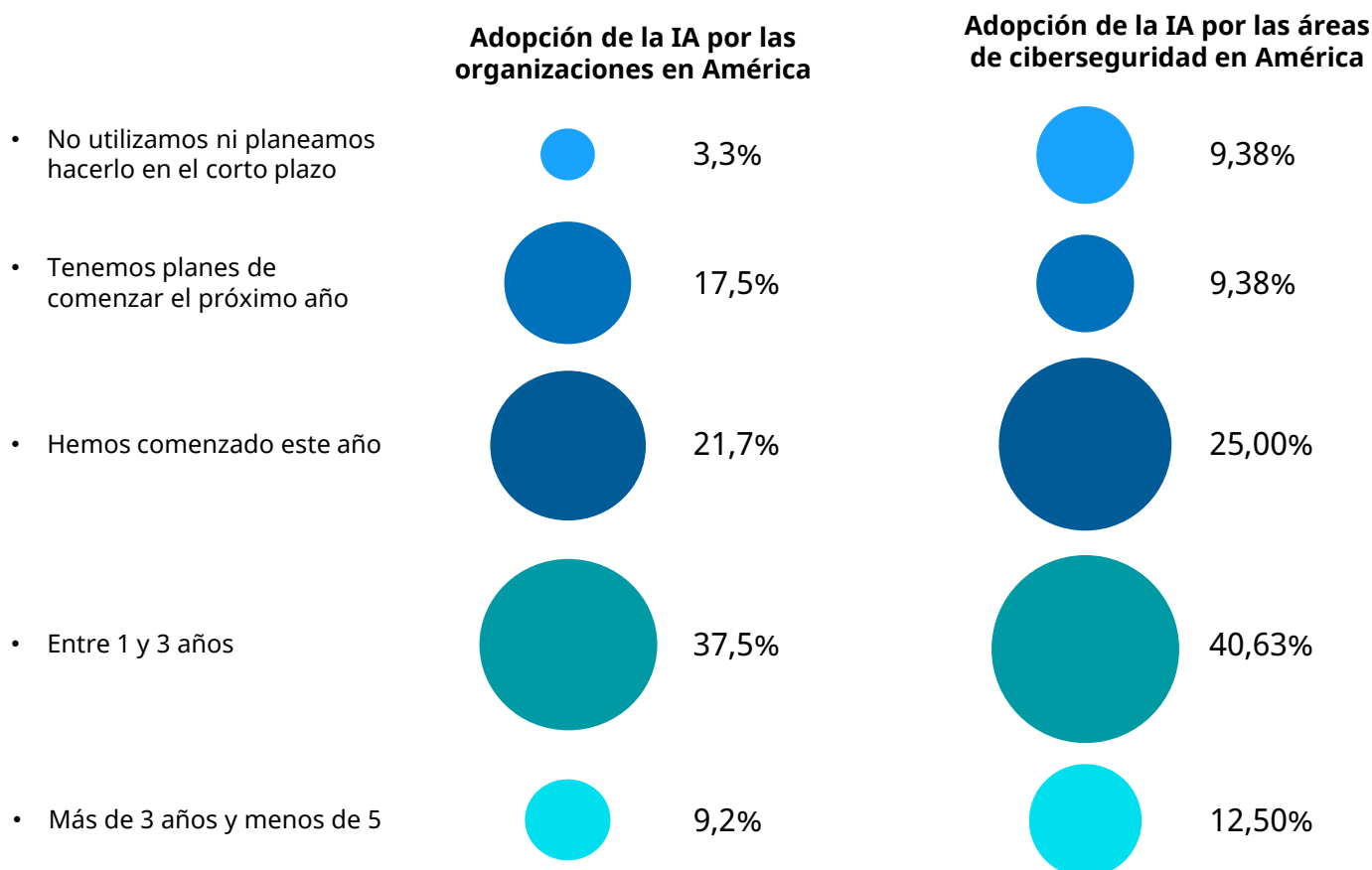
Empresa de industria, Perú

Percepción sobre la adopción de la Inteligencia Artificial (IA) en las áreas de ciberseguridad en América Latina

El siguiente diagrama muestra el tiempo que las empresas de América llevan trabajando con la IA (izquierda), y el tiempo que las áreas de ciberseguridad de las organizaciones de América llevan trabajando con la IA (derecha). Se puede observar que, en

ciberseguridad, por un lado, hay un mayor % de empresas que no desean iniciar con la adopción de IA en comparación con el 3,3% que no desea comenzar con la adopción en el resto de las áreas. Sin embargo, en los rubros de “hemos comenzado este año”, “llevamos entre 1 y 3

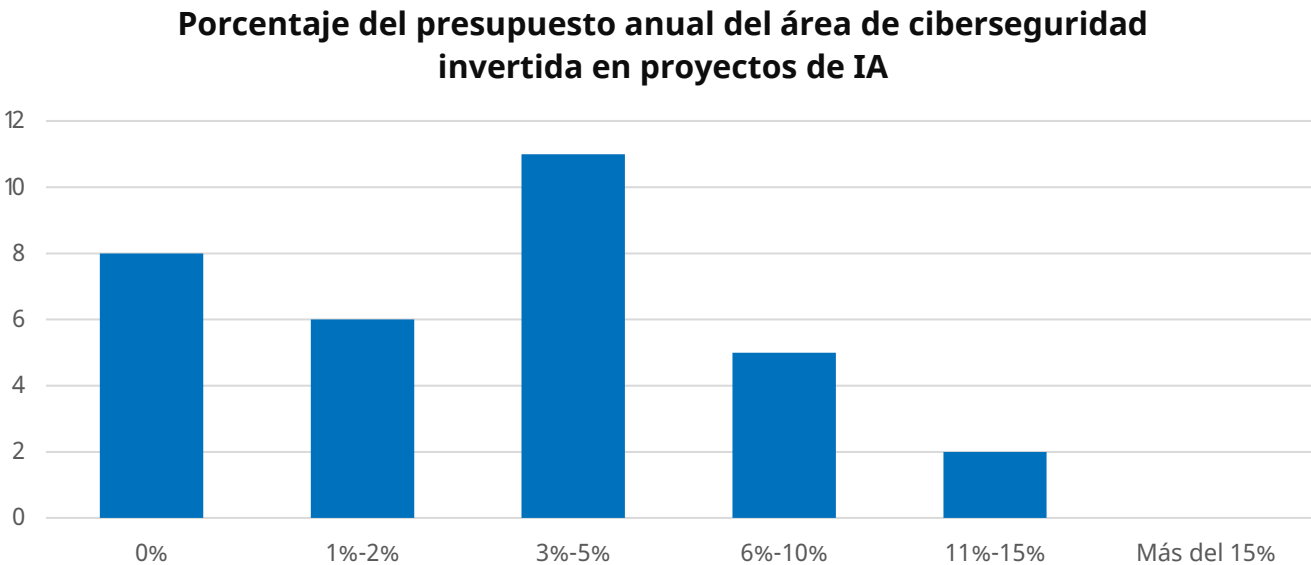
años” y “más de 3 años y menos de 5” hay un mayor % de empresas que dicen estar ya trabajando con IA en ciber frente a las organizaciones que reconocen estar adoptando IA. ¿Es esto una contradicción?



De estos datos se desprenden dos reflexiones.
Por un lado, los fabricantes de herramientas ciberseguridad llevan años trabajando con la IA para mejorar controles defensivos tales como DLP, firewalls, protección antispam, asignación de roles en IAM, entre otros. Hay CISOs muy conscientes de la potencia de esas funcionalidades y si bien, no han desarrollado sistemas de IA ad-hoc

para el área, sí reconocen trabajar con la IA desde hace años.
Por otro lado, siendo que la encuesta de adopción de IA en las organizaciones de America Latina no fue enviada a CISOs, y parece que en las áreas de ciberseguridad se lleva más tiempo trabajando con IA que fuera de estas áreas, conviene reflexionar en como los CISOs están vendiendo su trabajo al interior de su compañía. Quizá falta una

socialización de como las herramientas en las que invierten hacen uso de la IA para mejorar la ciberseguridad de la organización. Y esta socialización es clave cuando se trata de conseguir más presupuesto. Actualmente, las áreas de ciberseguridad declaran invertir el siguiente % de su presupuesto en la adopción de la IA:



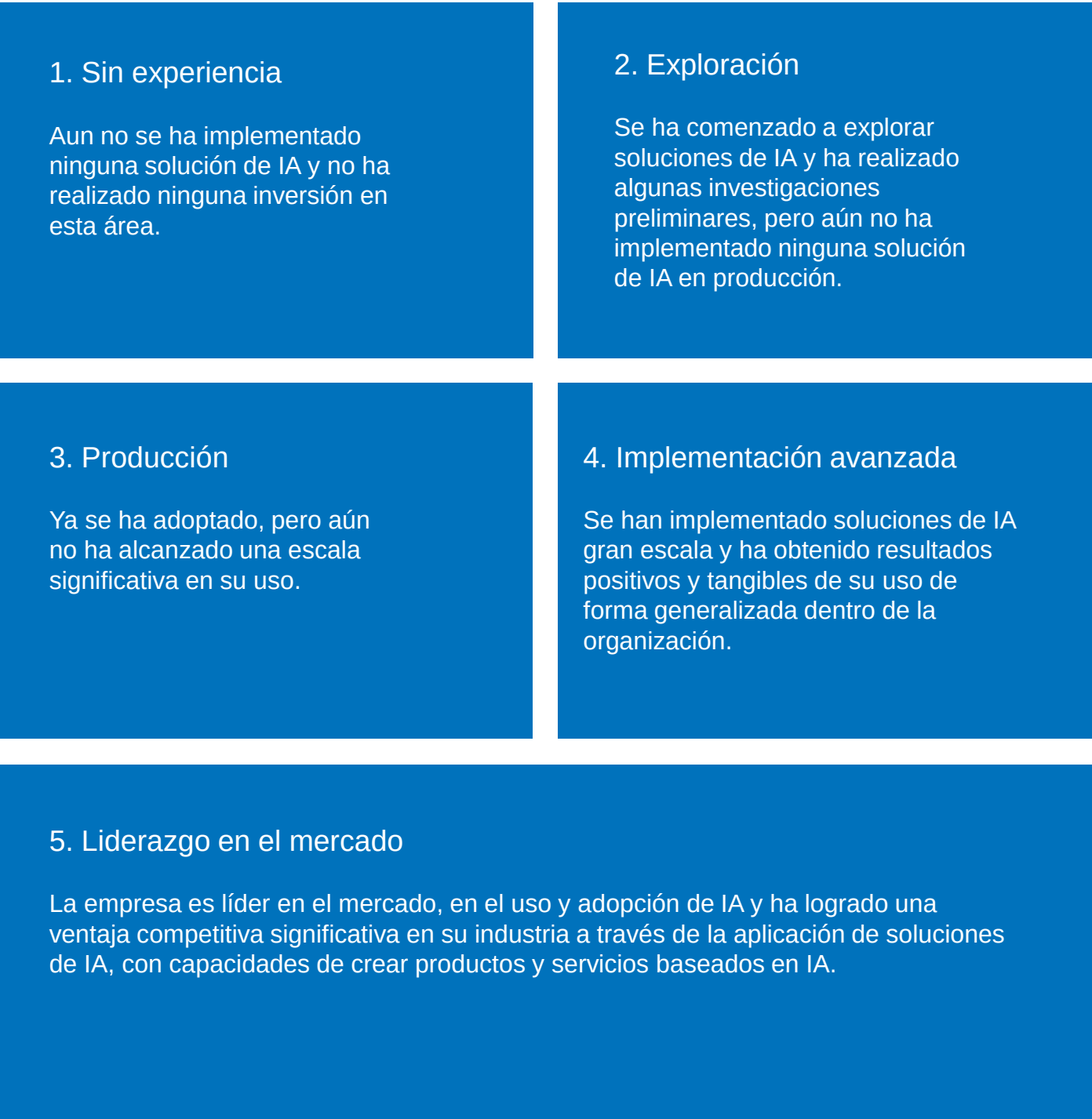
“ Hemos establecido un grupo de trabajo de IA, se han identificado casos de uso para la aplicación de AI y algunos de estos están relacionados con ciberseguridad de la información.

CISO de entidad de alcance regional

Percepción sobre la adopción de la Inteligencia Artificial (IA) en América Latina

Etapas de madurez de las empresas respecto al uso de la IA

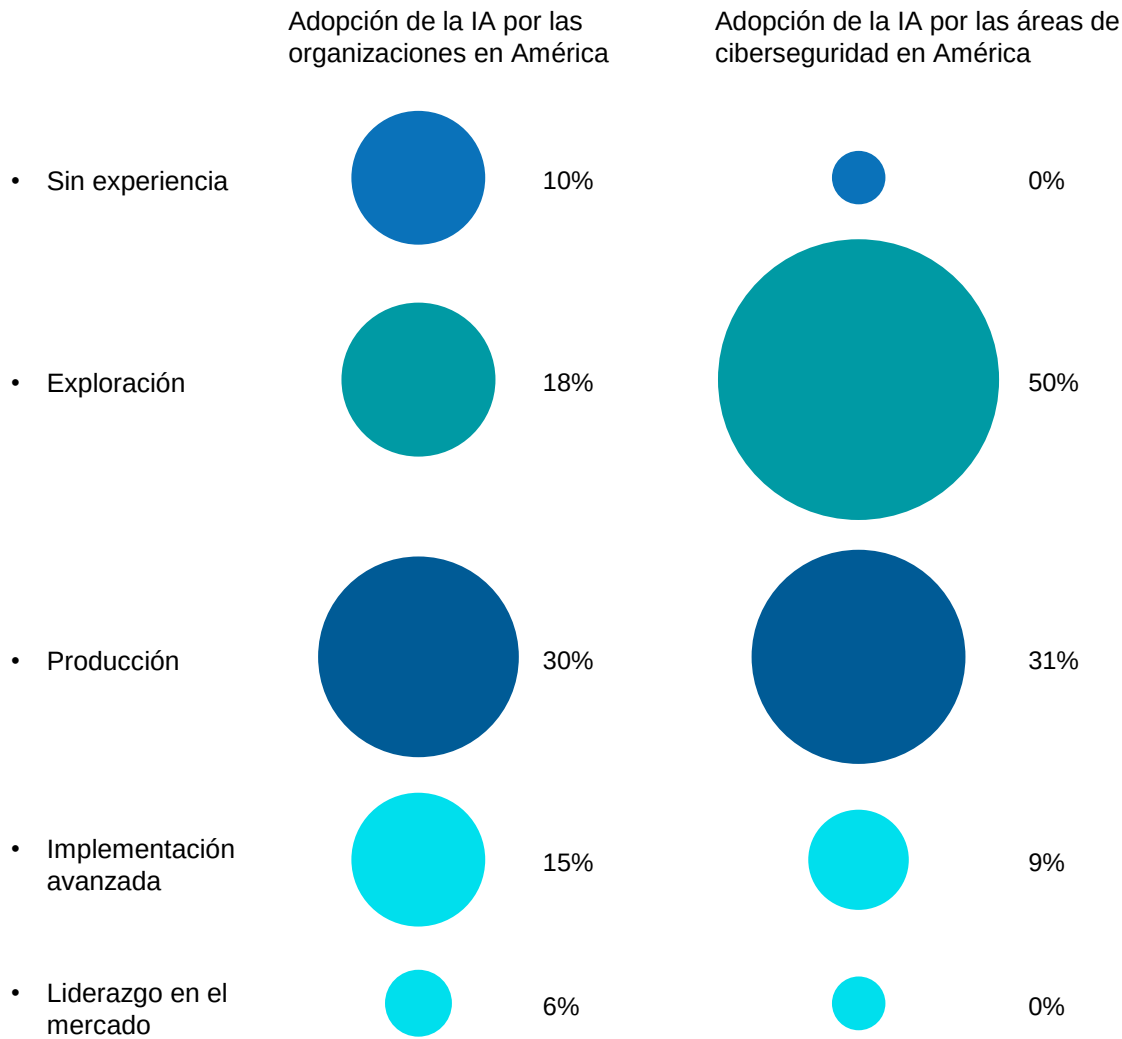
El siguiente diagrama detalla el camino que siguen las empresas en su jornada de adopción:



Aunque en el caso de fases de madurez parece que todas las compañías han tenido contacto con la IA en las áreas de ciberseguridad, se aprecia que están un nivel de madurez menor en las áreas de IA

que en otras áreas de la compañía. De hecho, aunque el 53,13% de las compañías dice llevar trabajando con IA más de un año, no se sienten aún líderes en el mercado. Esto invita a reflexionar si es que la

adopción ha sido consciente o a través de herramientas de ciberseguridad que incluyen IA y qué provoca ese estancamiento.



“ La IA en ciberseguridad de la información tiene un enorme potencial; sin embargo, es importante moderar las expectativas en cuanto a la velocidad de adopción, que debería ser gradual, comenzando por actividades puntuales y repetitivas, y ampliando luego su uso a tareas más complejas.

CISO de empresa de Industria, Perú

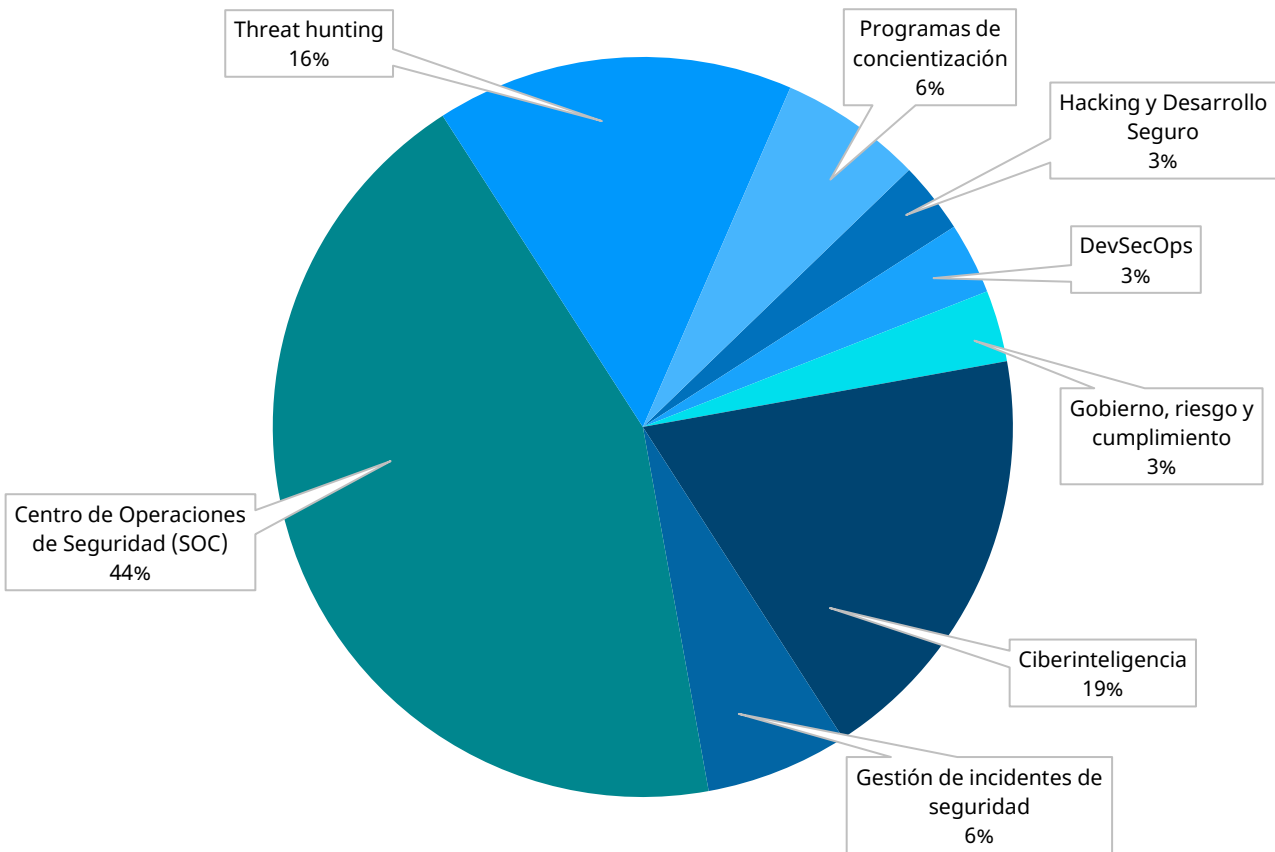
Madurez y expectativas de la IA en el área de ciberseguridad

“ La IA va a ser un elemento importante en la ciberseguridad de las compañías, pero, tiene un difícil reto en la respuesta y recuperación. Está llegando por las herramientas de protección que que están empezando a implementarlas.

CISO de industria minera, Perú

Tras entender cómo se perciben las organizaciones en la adopción de la IA en las áreas de ciberseguridad, se ha analizado en qué actividades de ciberseguridad se ha venido aplicando la IA. El área donde mayoritariamente se ha usado la IA es en el SOC; Sin embargo, en las actividades de Red team y de gestión de incidentes de identidades, ninguna organización declara haber usado esta tecnología.

Actividades de ciberseguridad donde se ha aplicado la IA

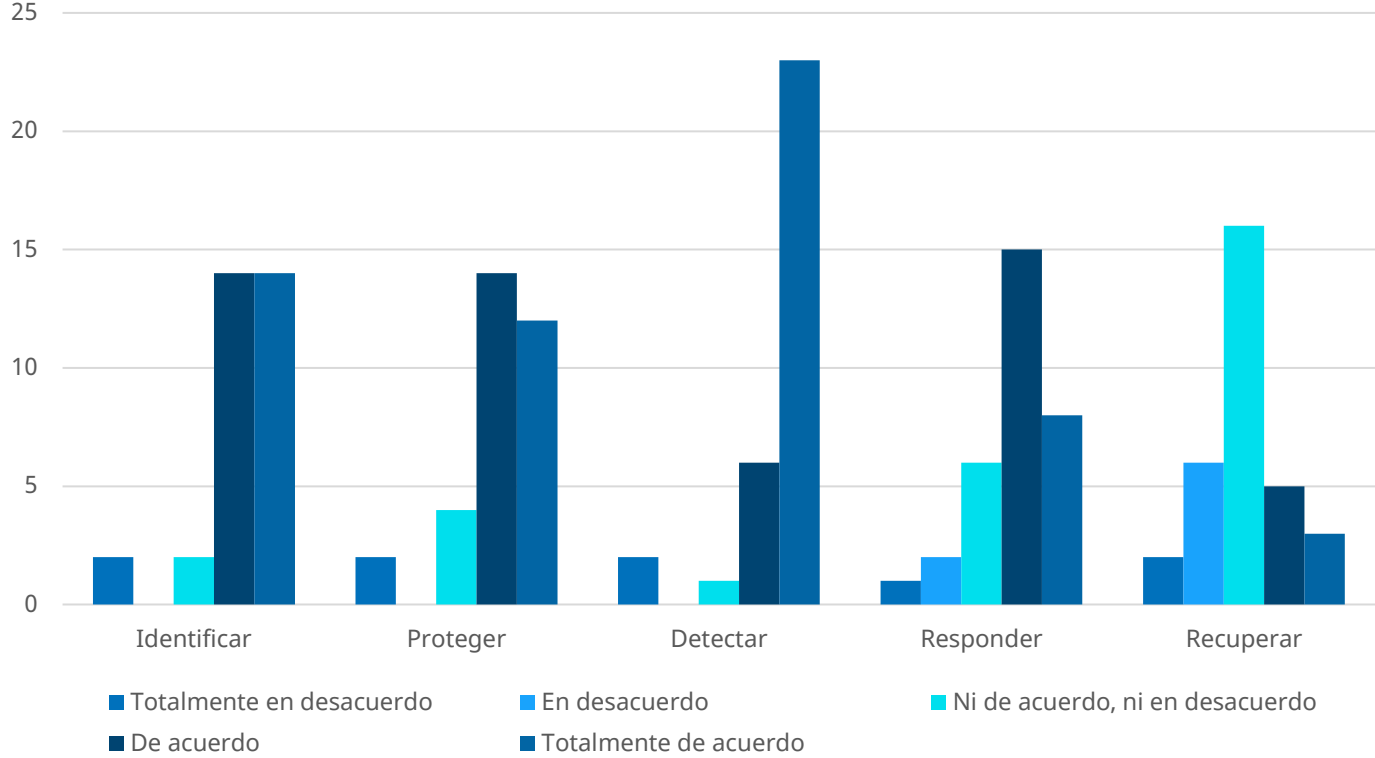


Además, las organizaciones coinciden en que la IA puede apoyar en los dominios de identificar, proteger, detectar y responder. La

fase de recuperación es en las que más dudas se tiene, quizá porque hoy en día se percibe como una actividad que se realiza pocas veces y

no vale la pena entrenar un sistema para que nos de soporte en esa fase.

Funciones de la NIST en las que IA puede ayudar



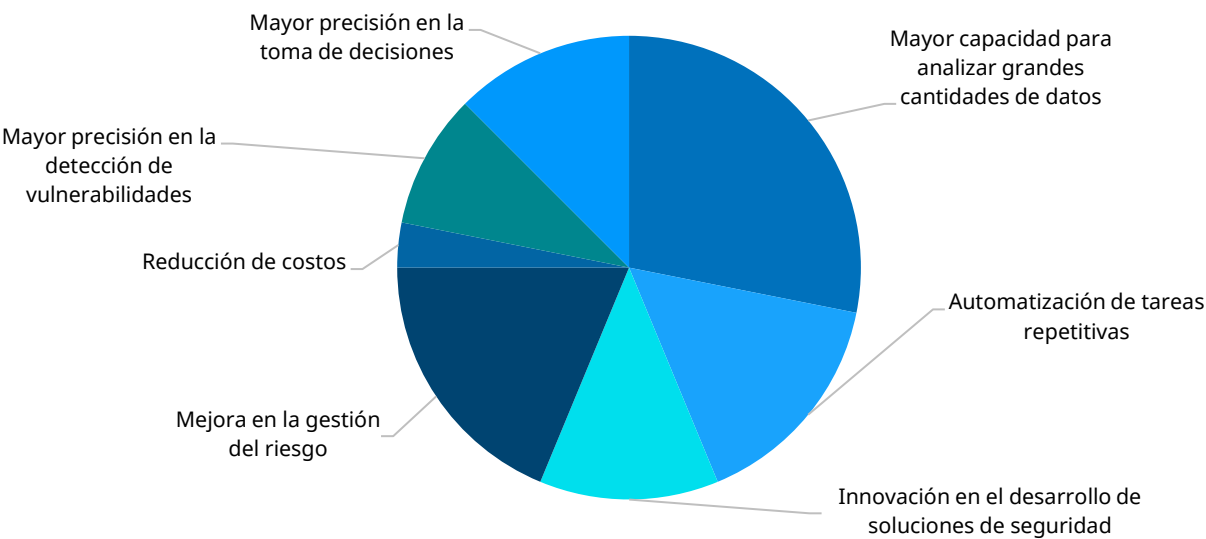
Beneficios y barreras para la implementación de la IA en ciberseguridad

Una de las preguntas realizada fue la relacionada con los beneficios

esperados con la adopción y el uso de la IA. No ha habido una respuesta

unánime, siendo varios los beneficios percibidos con igual peso.

Beneficios esperados con el uso de la IA

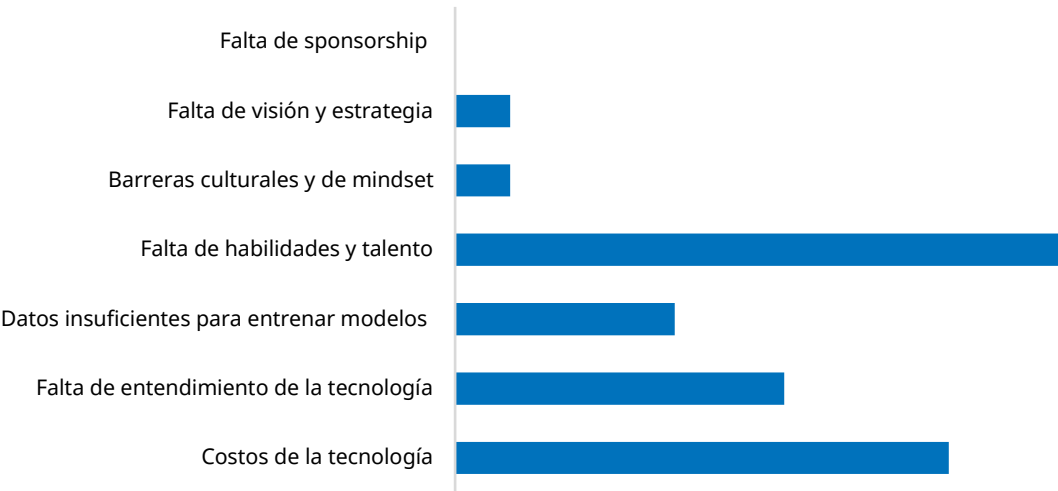


Estos beneficios derivan otros. Por ejemplo, si se logra una mayor automatización de tareas repetitivas, se conseguirá disminuir el gap de

talento necesario de personas con conocimientos en ciber a la par que las actuales reciben tareas a realizar de mayor valor. Y, de hecho, este

punto es el que se aprecia como la mayor barrera existente en la aplicación de la IA en las áreas de ciberseguridad hoy en día.

Barreras principales en el área de ciberseguridad para aplicar IA



Los costes y la falta de entendimiento de la IA son las siguientes barreras percibidas, tras la falta de talento.

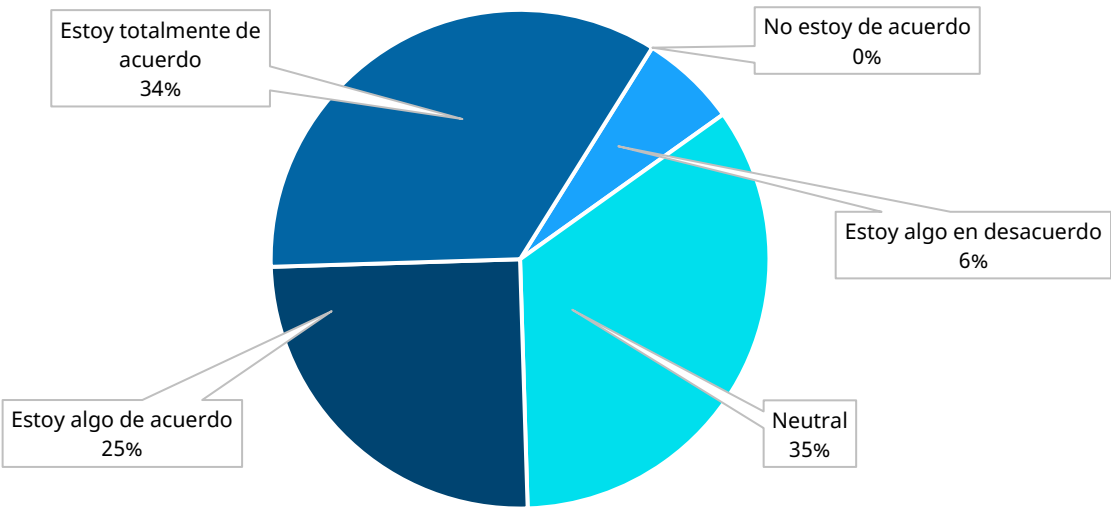
Beneficios y barreras para la implementación de la IA en ciberseguridad

Un tema clave para adoptar IA en cualquier área, incluyendo el área de ciberseguridad, es el soporte por parte de la organización. En este punto, hay un gran grupo que está

de acuerdo o algo de acuerdo con la afirmación “Tengo apoyo por parte de la organización para aplicar IA en el área de ciberseguridad”. Hay otro grupo que es neutral a esa

afirmación. En punto positivo a resaltar es que la opinión de no estar de acuerdo o algo en desacuerdo es minoritaria.

Tengo apoyo por parte de la organización para aplicar IA en el área de ciberseguridad.

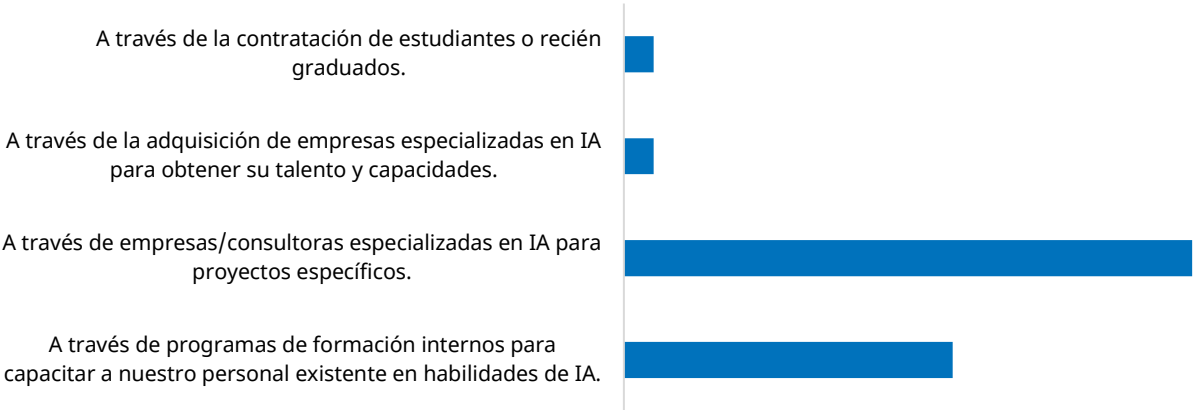


Para obtener las capacidades y el talento necesario para el trabajo relacionado con la IA, las

organizaciones están mayoritariamente apostando por la contratación de compañías

consultoras especializadas o la creación de capacidades internas.

Obtención de las capacidades y el talento necesario para el trabajo relacionado con IA



Conclusiones y retos

En esta última sección quisiéramos destacar los principales “take-aways” de este análisis realizado y qué retos van a suponer en los próximos meses.

Materialización del valor invertido en IA en ciberseguridad.

Más del 95% de las organizaciones cree que la IA tendrá un impacto medio o alto en las áreas de ciberseguridad. La IA está generando alta expectativa en ciberseguridad, y esto se traduce	en presupuesto invertido y en apoyo de la organización. Esto supone que los CISOs deben materializar y cuantificar el valor invertido en IA en su área, demostrando que se han logrado alguno de los beneficios	esperados. Especial importancia tiene este reto en las organizaciones que declaran llevar usando IA en las áreas de ciberseguridad más de 3 años.
---	---	---

Definición de casos de uso de IA en ciberseguridad concretos

El SOC se percibe como el área donde más apoya la IA, y si nos vamos a los dominios de la NIST, hay una opinión muy general de que los dominios identificar proteger, detectar, responder se pueden ver	muy beneficiados de con la IA. La definición de casos de uso permitirá explicar cómo se está adoptando la IA en ciberseguridad, a la vez que limita el alcance a valorar y cuantificar. Actualmente se puede	comenzar por la definición de casos de uso de SOC para ir extendiéndolo a dominios del NIST y otros ámbitos como gobierno o riesgos.
---	--	--

Ideas o aplicaciones de IA donde tendrá alto impacto en el corto o mediano plazo:

1. Detección de amenazas y anomalías: Utilizando el aprendizaje automático y el análisis de datos, la IA puede identificar patrones inusuales o comportamientos sospechosos en una red, que podrían indicar una intrusión, un malware, o cualquier otro tipo de amenaza cibernética. Esta capacidad de detección rápida y precisa es fundamental para prevenir ataques o limitar el daño que pueden causar.
2. Respuesta a incidentes de ciberseguridad: Una vez que se identifica una amenaza, la capacidad de responder rápidamente es crucial. La IA puede automatizar respuestas a incidentes de ciberseguridad, como aislar sistemas comprometidos o aplicar parches a vulnerabilidades. Esto no solo mejora la velocidad de respuesta, sino que también reduce la carga sobre los equipos de ciberseguridad cibernética, permitiéndoles concentrarse en problemas más complejos.

CISO Banca LATAM

Cuidado del talento en IA y Ciberseguridad

El talento, o más bien, la falta de él es la principal barrera de adopción de la IA. Las organizaciones deben pensar qué carrera van a dar a los	profesionales expertos en IA y ciberseguridad. Estas personas buscan nuevos retos y si no los encuentran en una organización, cambiarán a otra.	Buscar la resiliencia en la rotación de este personal clave debe ser también parte de la estrategia de adopción de la IA
---	---	--

María Pilar Torres Bruna

Responsable del área de ciberseguridad en Iberia y LATAM

maria.pilar.torres.bruna@nttdata.com

Carla Passos Schwarzer

Responsable del área de ciberseguridad en Brasil

carla.passosschwarzer@emeal.nttdata.com

Jose Uzcategui

Responsable del área de ciberseguridad en Chile

jose.uzcategui@emeal.nttdata.com

Miguel Angel Garzón Ramirez

Responsable del área de ciberseguridad en Colombia

miguel.angel.garzon.ramirez@emeal.nttdata.com

Andrea Isabel Muñoz Parreño

Responsable del área de ciberseguridad en Ecuador

andraisabel.munozparreno@emeal.nttdata.com

Cristhian Israel Atristain Garcia

Responsable del área de ciberseguridad en Mexico

cristhianisrael.atristaingarcia@emeal.nttdata.com

Néstor Gerardo Ordoñez

Responsable del área de ciberseguridad en USA

nestorgerardo.ordonez@emeal.nttdata.com

Andrea Araujo Braga

Manager de Marketing and Communication Americas

andrea.araujo.braga@nttdata.com

Gabriela Gutiérrez Sánchez

Leader de Marketing and Communications Americas

dulcegabriela.gutierrezsanchez@nttdata.com

Sobre NTT DATA

NTT DATA, parte del Grupo NTT, es una compañía innovadora global de servicios empresariales y de IT con sede en Tokio. La empresa ayuda a los clientes en su proceso de transformación a través de consultoría, soluciones industriales, servicios de procesos comerciales, modernización digital y de IT y servicios administrados. NTT DATA les permite a ellos, así como a la sociedad, avanzar con confianza hacia el futuro digital. La compañía demuestra su compromiso con el éxito a largo plazo de sus clientes, combinando el alcance global con la atención local, para trabajar con ellos en más de 50 países de todo el mundo. Para saber más, visita nttdata.com.



