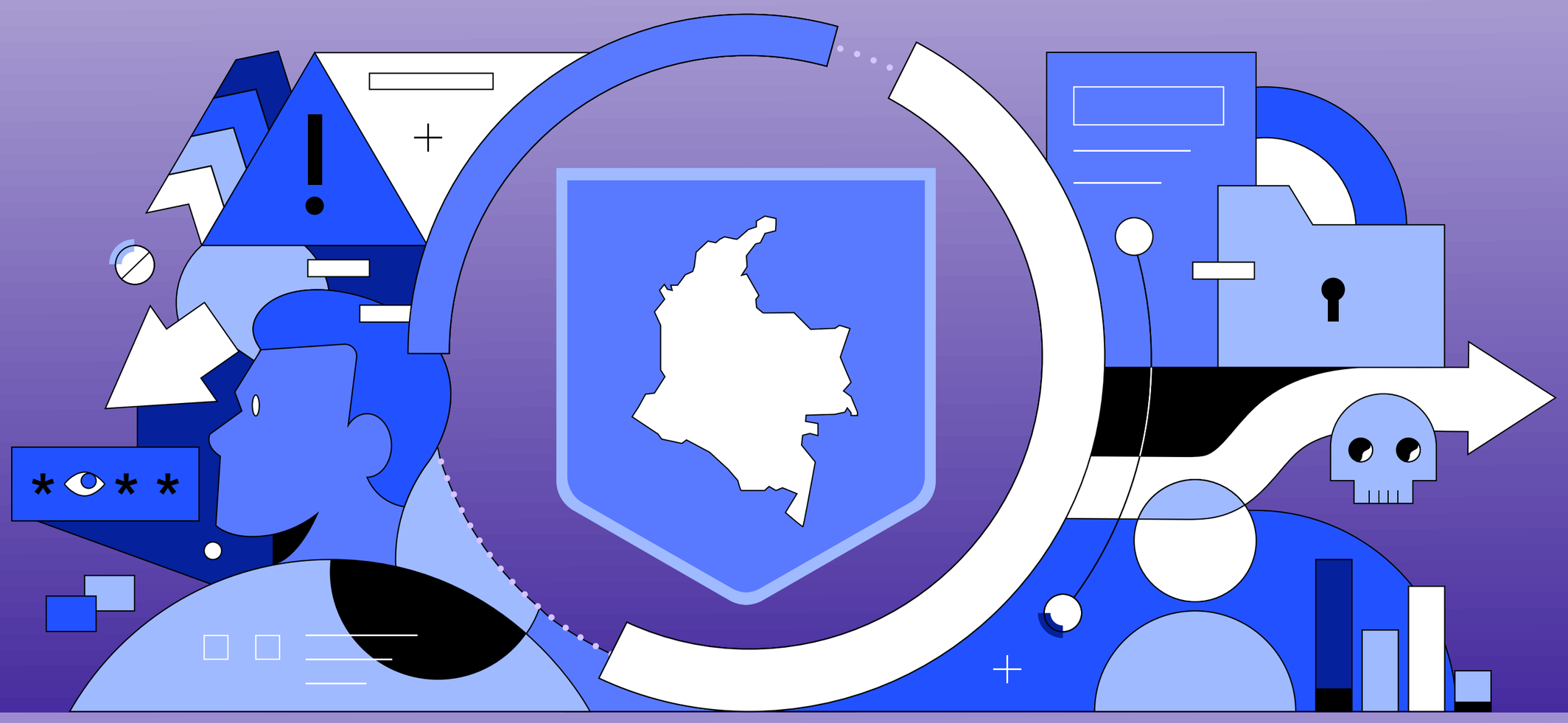
ManageEngine

El estado de la ciberseguridad en Latinoamérica para 2024

manageengine.com/latam



Índice

Introducción

Este documento proporciona un breve resumen de una encuesta centrada en el estado de la ciberseguridad en Colombia. Un total de 150 ejecutivos calificados y profesionales de seguridad de pequeñas, medianas y grandes corporaciones completaron la encuesta. Los participantes ocupaban cargos de alta jerarquía, a nivel de gerente y superior, y eran directamente responsables de la defensa y estrategias de seguridad de sus organizaciones. Esta investigación examinó tendencias en todos los tipos de industrias.

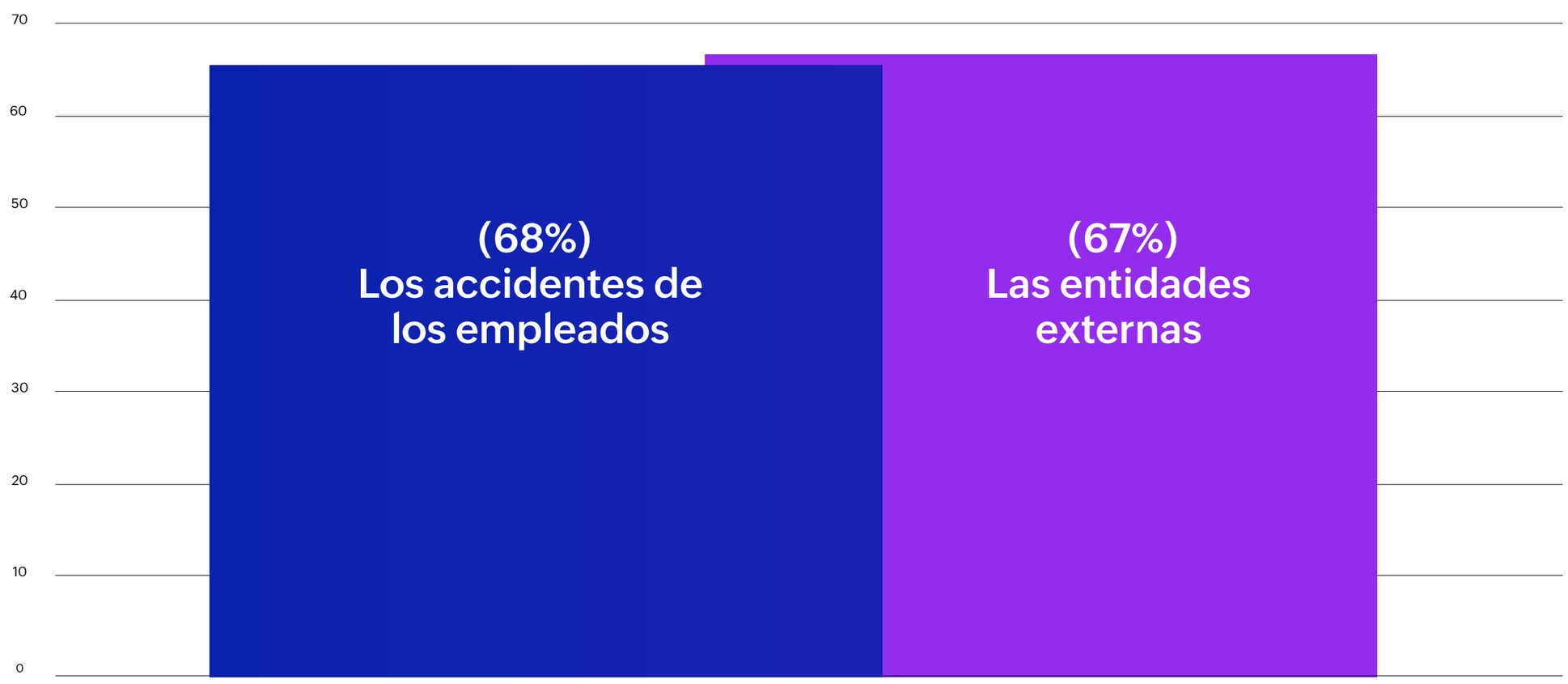
La investigación analizó el impacto de la inteligencia artificial en la defensa de la ciberseguridad y en los miembros de los equipos de seguridad, el uso de seguros de seguridad cibernética y la capacidad para cumplir con los requisitos de gestión de datos.

Aspectos clave destacados:

Esto es comparativamente más bajo que el resto de América Latina (92%).

Aspectos clave destacados:

Los accidentes de los empleados (68%) y las entidades externas (67%) fueron las principales razones detrás de la mayoría de las amenazas de seguridad.

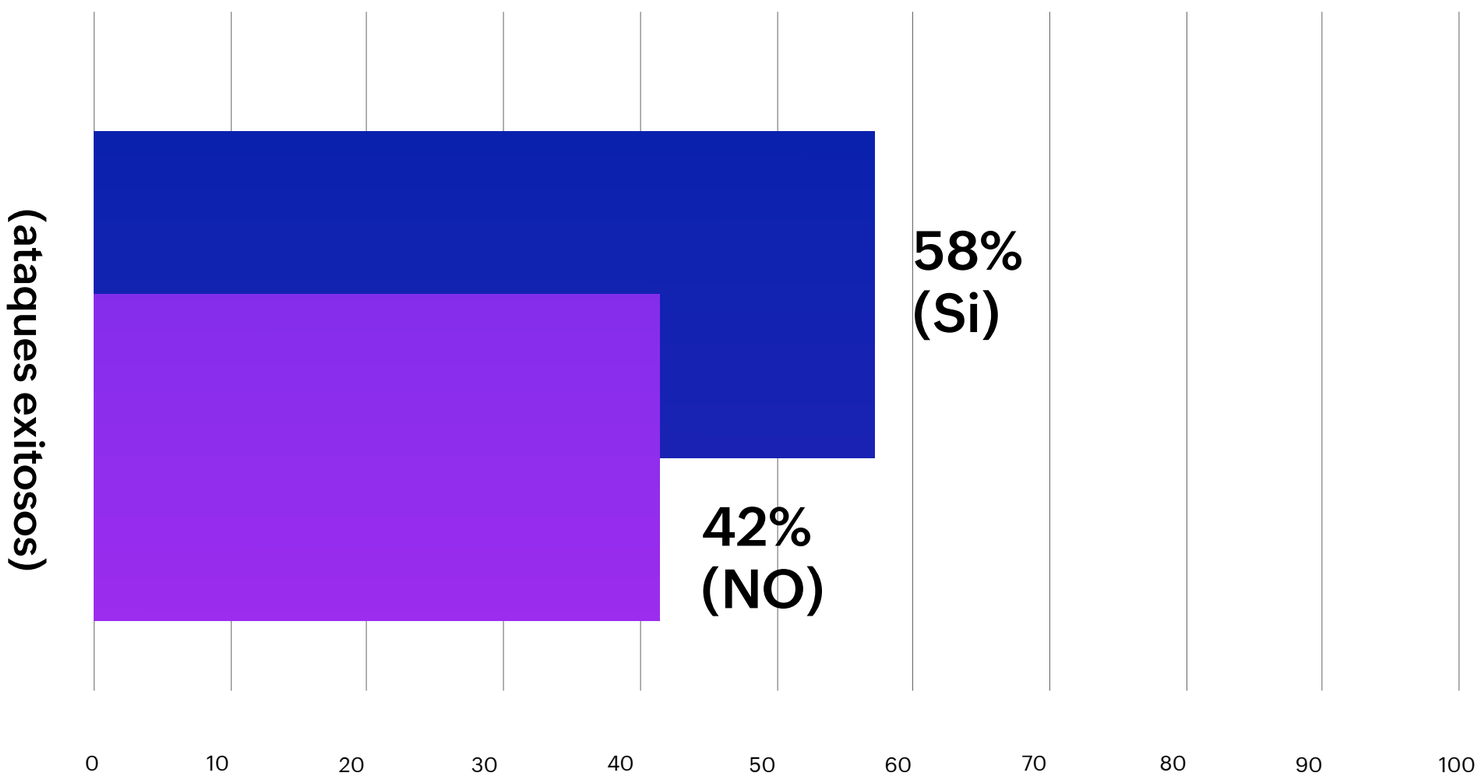


Resumen de la investigación

Sección 1: Amenazas e impacto

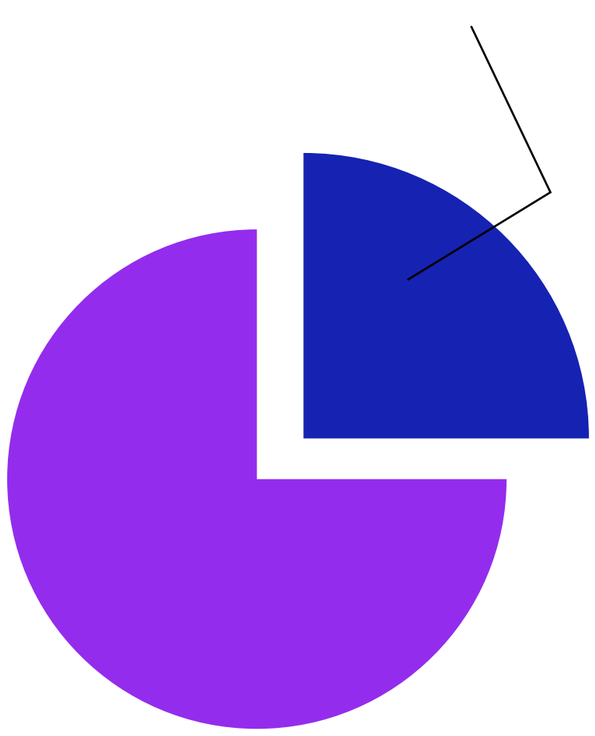
Los encuestados reconocieron que sus empresas experimentaron un aumento en las violaciones de ciberseguridad en comparación con años anteriores. Sin embargo, los ataques que resultaron en pérdidas financieras significativas siguieron siendo relativamente bajos.

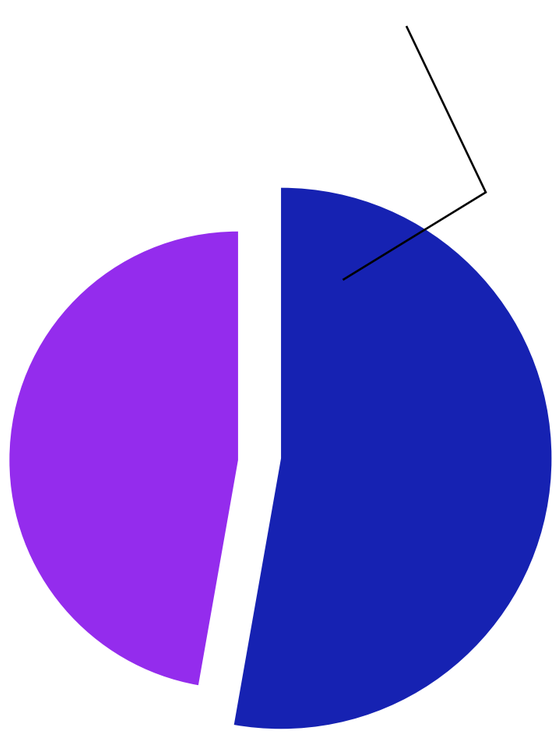
¿Su empresa experimentó más violaciones de ciberseguridad (ataques exitosos) en 2023 en comparación con años anteriores?



Solo el 25% de los encuestados dijo que sus empresas experimentaron un ataque de ciberseguridad que resultó en una pérdida financiera significativa en 2023.

En 2023, según el 53% de los encuestados, la inteligencia artificial generativa desempeñó un papel importante en los ciberataques contra sus empresas.





ManageEngine

Sección 2: Seguro de ciberseguridad

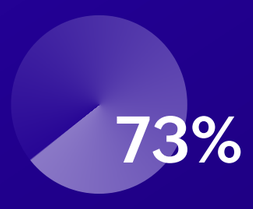
La necesidad de seguros de ciberseguridad y el cumplimiento con sus requisitos está generando un efecto positivo en las empresas colombianas.

54%

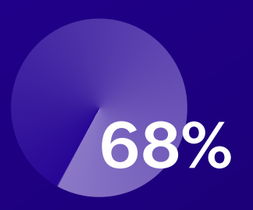
En Colombia, el 54% de los encuestados afirmó que sus empresas realizaron reclamaciones exitosas de seguros de ciberseguridad.

En comparación con el resto de los países encuestados, Colombia registró el menor índice.

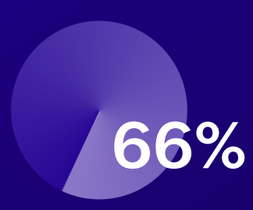
Los tres principales requisitos que las empresas tuvieron que cumplir para adquirir un seguro de ciberseguridad fueron:



Adherencia a las regulaciones de protección de datos



Políticas de seguridad y control de acceso



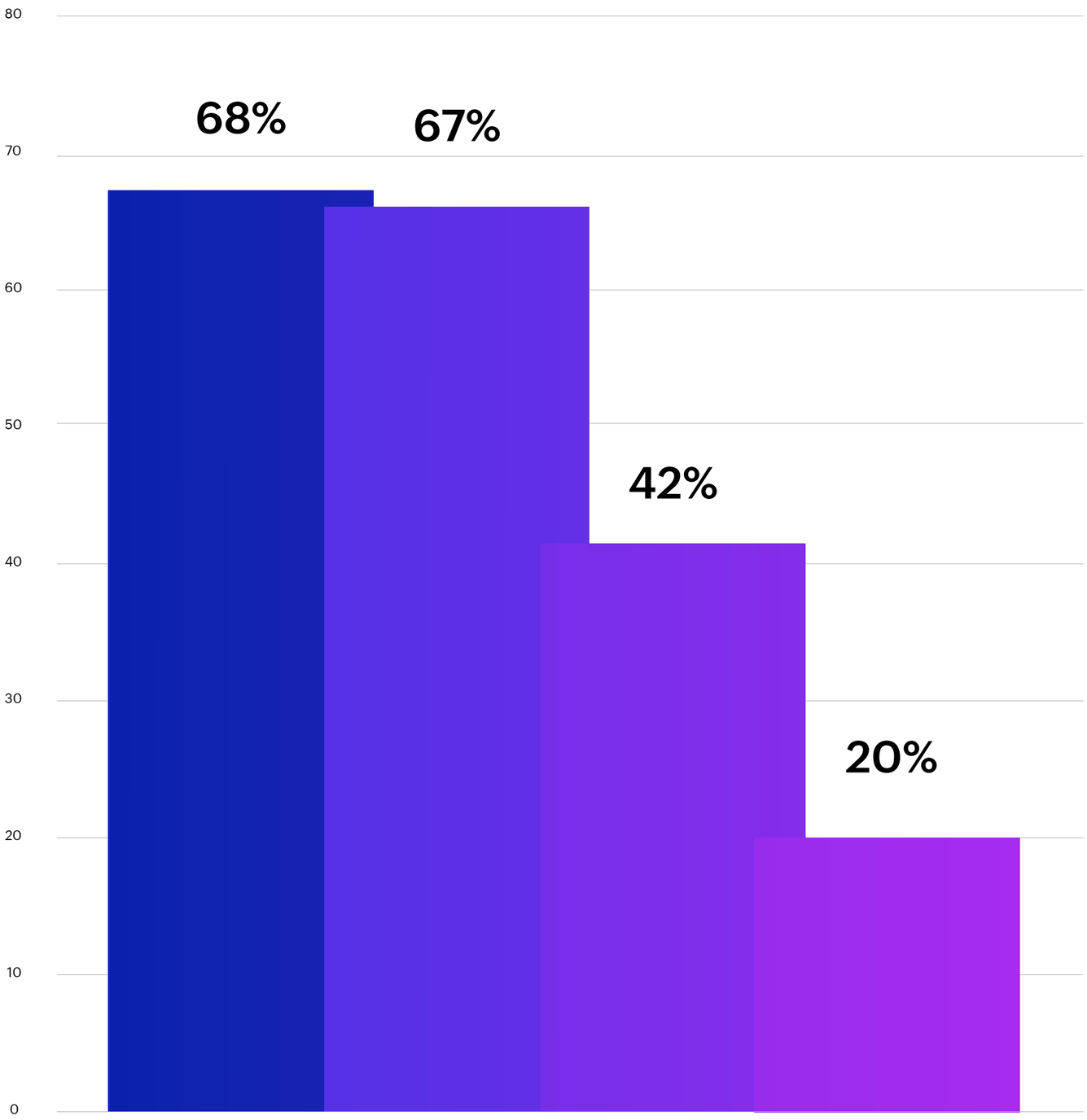
Evaluación y gestión de riesgos

ManageEngine

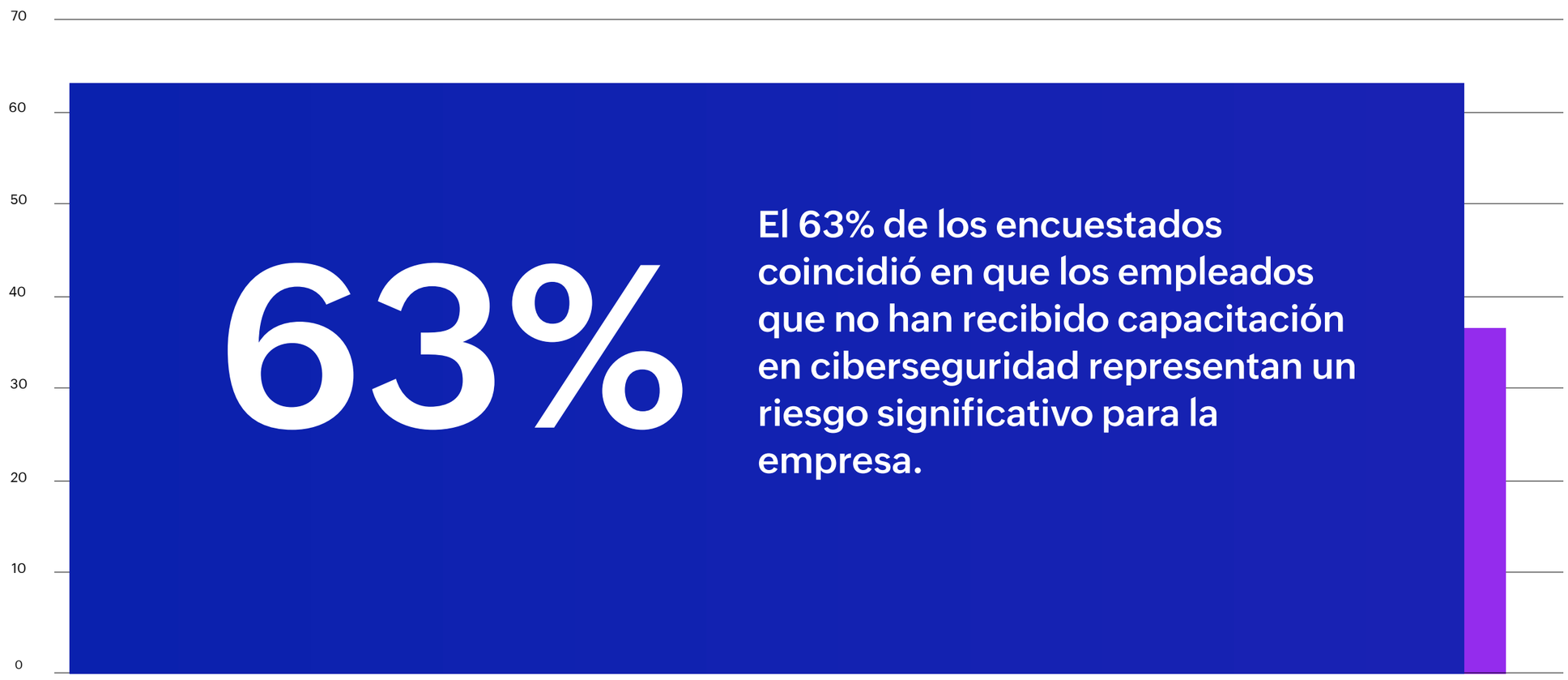
Sección 3: Rol de los empleados

En Colombia, las amenazas internas parecen representar un riesgo significativo para las organizaciones. Generalmente provienen de individuos con acceso autorizado a los sistemas, datos o instalaciones de una organización, quienes, de manera consciente o accidental, explotan sus privilegios con fines maliciosos. Las implicaciones de tales amenazas pueden ser graves, desde pérdidas financieras, responsabilidades legales y daños a la reputación hasta la pérdida de la confianza del cliente.

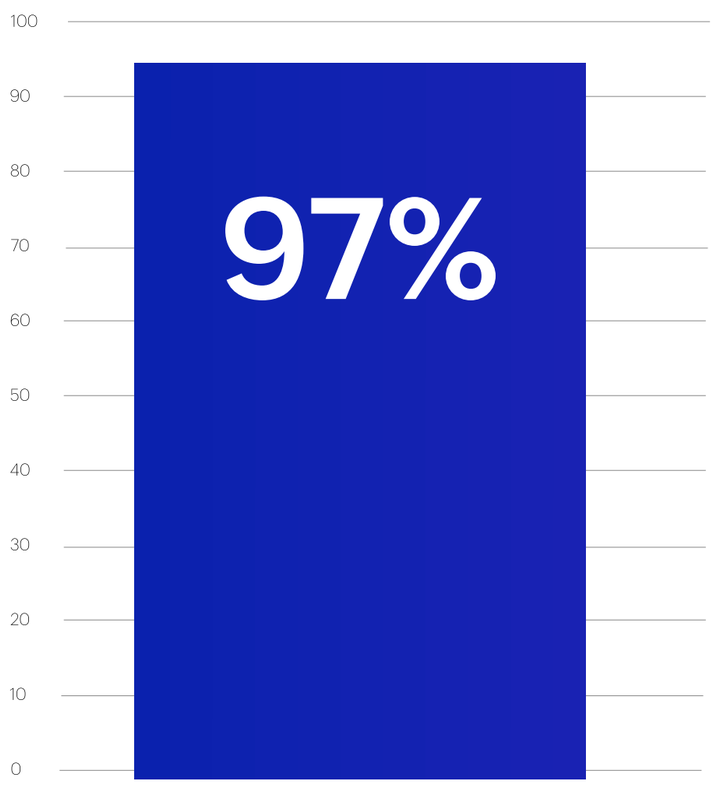
En su experiencia, ¿cómo suelen ocurrir la mayoría de las amenazas de seguridad?



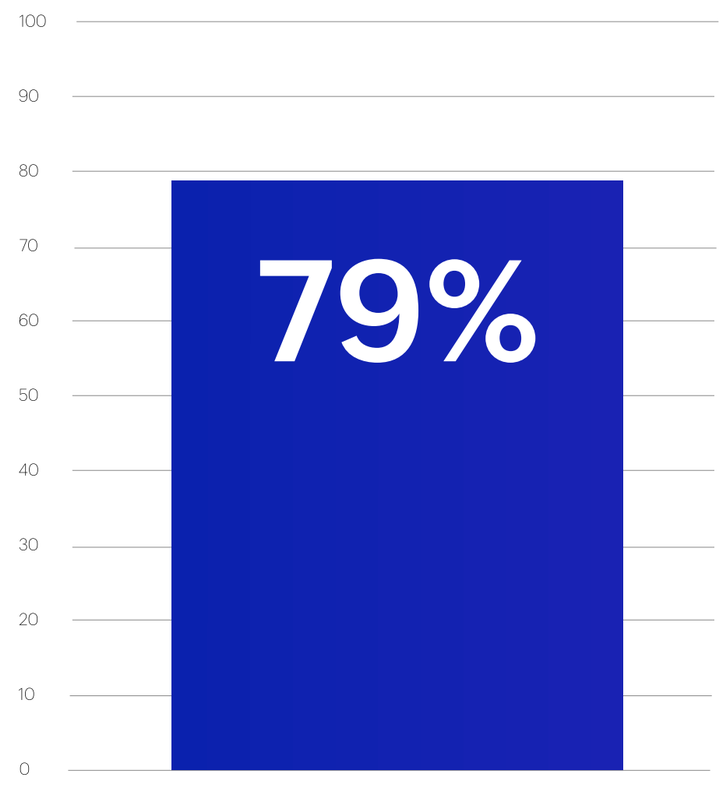
Las empresas comprenden el riesgo, dada la gran cantidad de amenazas internas que enfrentan, y existe una preocupación sobre la calidad de la capacitación de los empleados. Esto hace que la formación del talento humano (especialmente para aquellos que recientemente se han unido a la organización), sea una necesidad absoluta.



Casi todos los encuestados (97%) indicaron que sus empresas proporcionan capacitación en ciberseguridad a sus empleados.



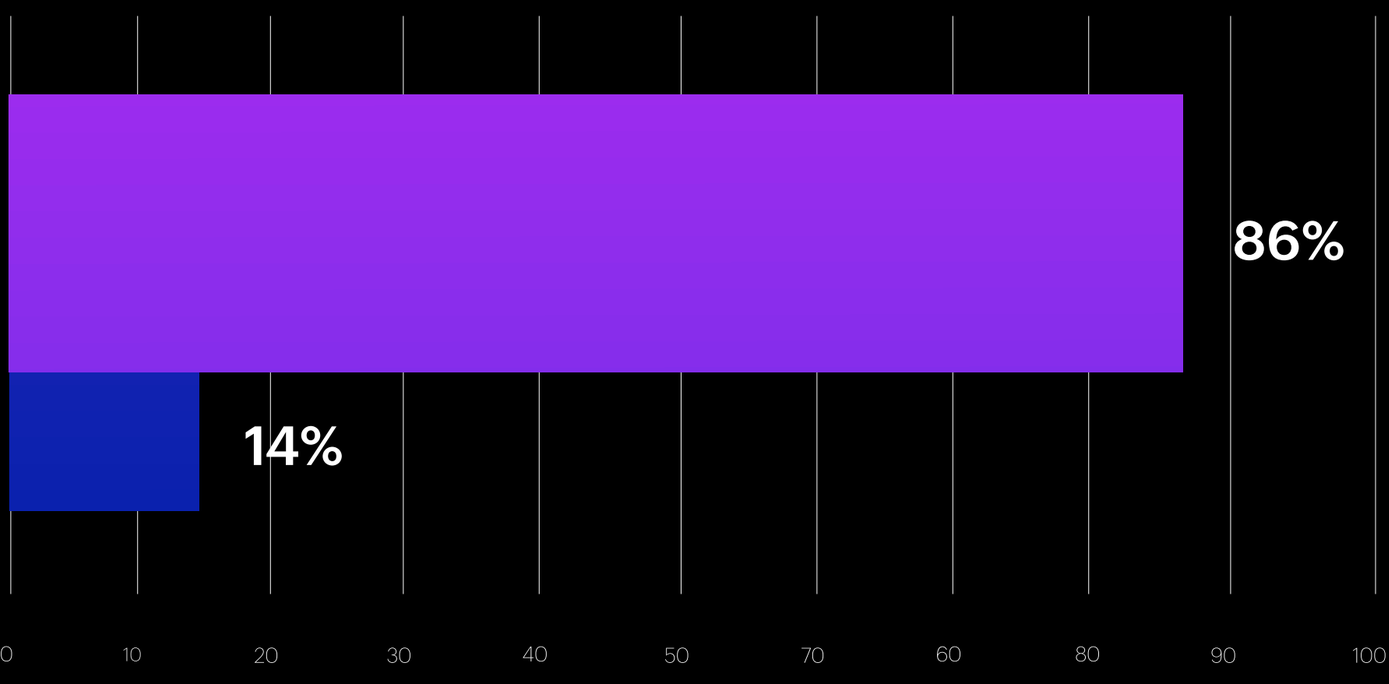
La mayoría de los encuestados (79%) aseguró que esta capacitación se ofrece dentro del primer mes de contratación.



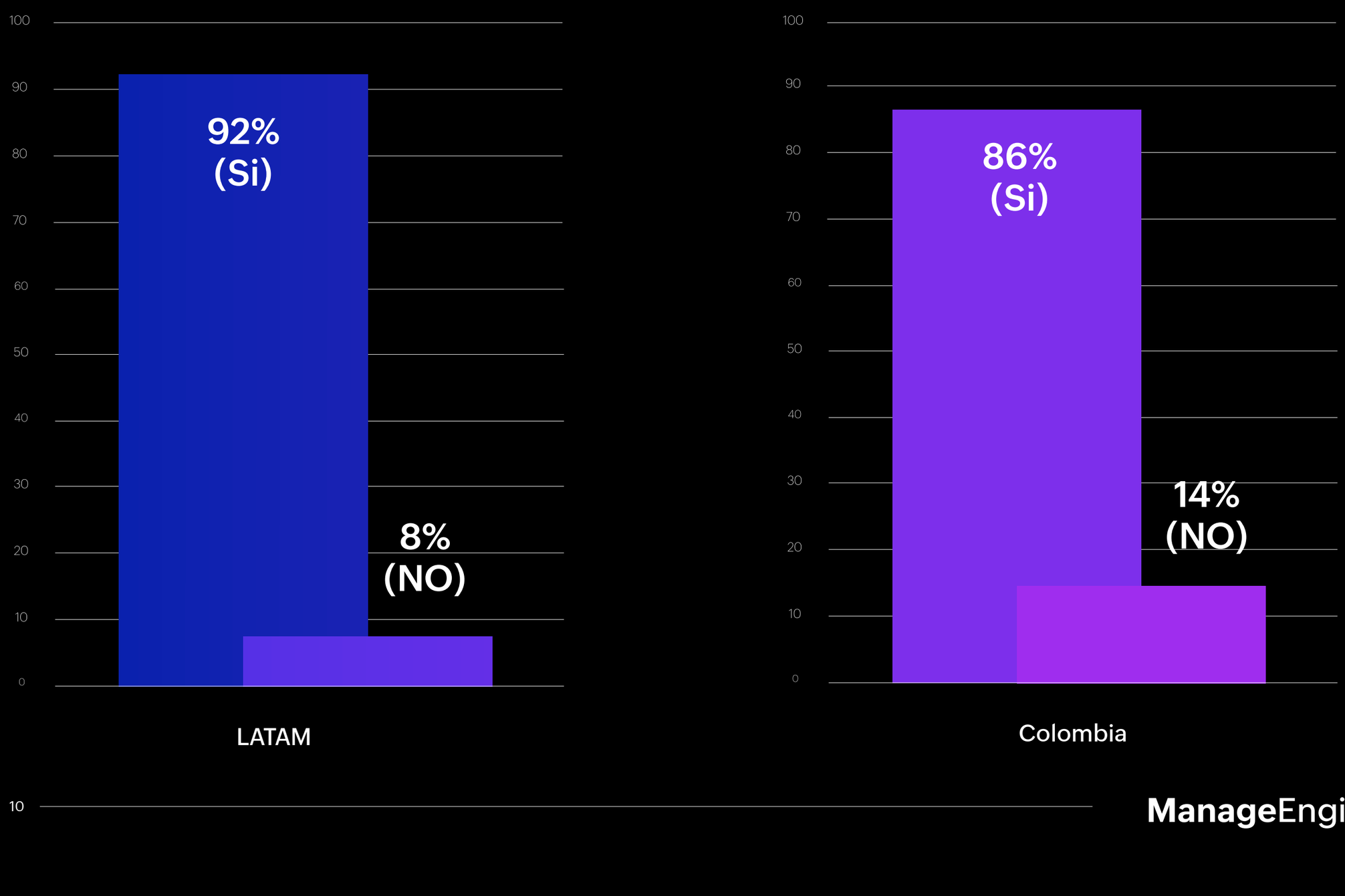
Sección 4: Rol de la IA

Los ataques impulsados por inteligencia artificial son más efectivos, creando dificultades financieras y aumentando el estrés en los equipos de seguridad. En 2024, las empresas necesitarán herramientas habilitadas para la inteligencia artificial y profesionales experimentados para defender el negocio y proteger sus datos contra las crecientes amenazas.

El 86% afirmó que la inteligencia artificial será fundamental para defenderse contra los ciberataques en 2024, mientras que el 14% aseguró que no. Colombia obtuvo un índice menor en comparación con el resto de los países encuestados en este aspecto.

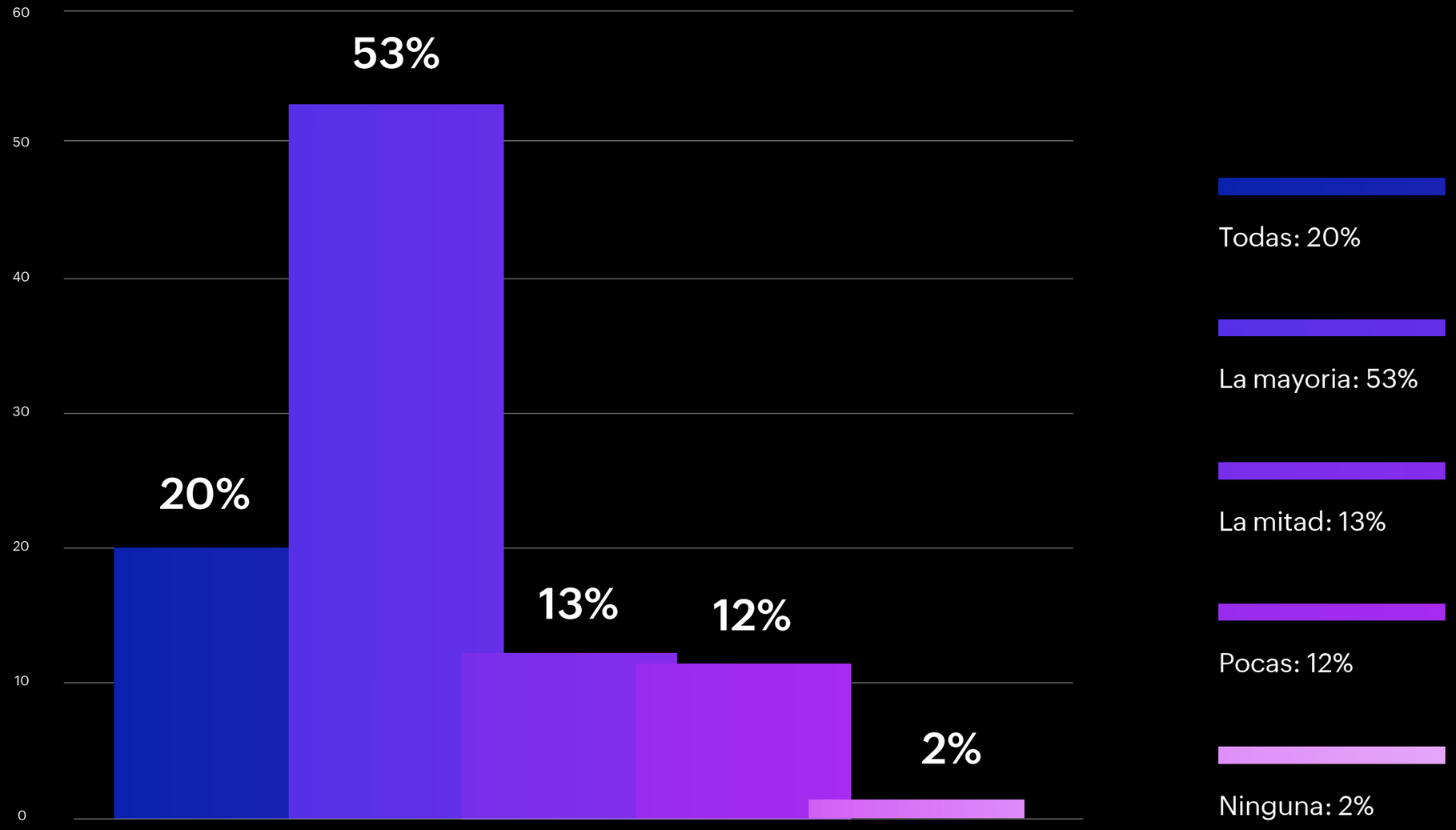


En su opinión, ¿será crítica la inteligencia artificial para defenderse contra los ataques de ciberseguridad en 2024?



ManageEngine

Según su mejor conocimiento, ¿cuántas de las soluciones de ciberseguridad de su empresa utilizarán inteligencia artificial en 2024?



La investigación descubrió algunos hallazgos controvertidos, con un 85% expresando una confianza inquebrantable en las herramientas de seguridad habilitadas para la inteligencia artificial para implementar cambios y ejecutar acciones sin ninguna intervención humana.

Esto puede haber surgido de la falta de profesionales experimentados en ciberseguridad señalados en la sección anterior. Sin embargo, los profesionales de seguridad reconocen los riesgos, con un 89% abogando por una organización independiente para verificar la confiabilidad de las soluciones de seguridad habilitadas para la inteligencia artificial.

Sección 5: El aumento del estrés en los equipos de ciberseguridad

Con la creciente frecuencia de los ataques cibernéticos -que se ven aún más amplificados por GenAI-, la carga sobre los profesionales de la ciberseguridad se ha intensificado.

El 65% de los encuestados reveló que sus niveles de estrés han aumentado debido al trabajo en los últimos años.

¿Ha aumentado su nivel de estrés debido al trabajo en los últimos años?

¿Qué está causando que aumente su nivel de estrés?

- Pocos miembros en el equipo de seguridad: 23%
- Falta de personal experimentado en el equipo: 43%
- Falta de capacitación: 19%
- Soluciones de ciberseguridad inadecuadas: 37%
- Aumento en la cantidad de problemas de seguridad (ataques, alertas, parches, etc.): 58%
- Falta de apoyo dentro de la empresa (otros empleados, departamentos, etc.): 37%
- Mala dirección (estrategia, apoyo, etc.): 21%
- Otros: 1%

ManageEngine

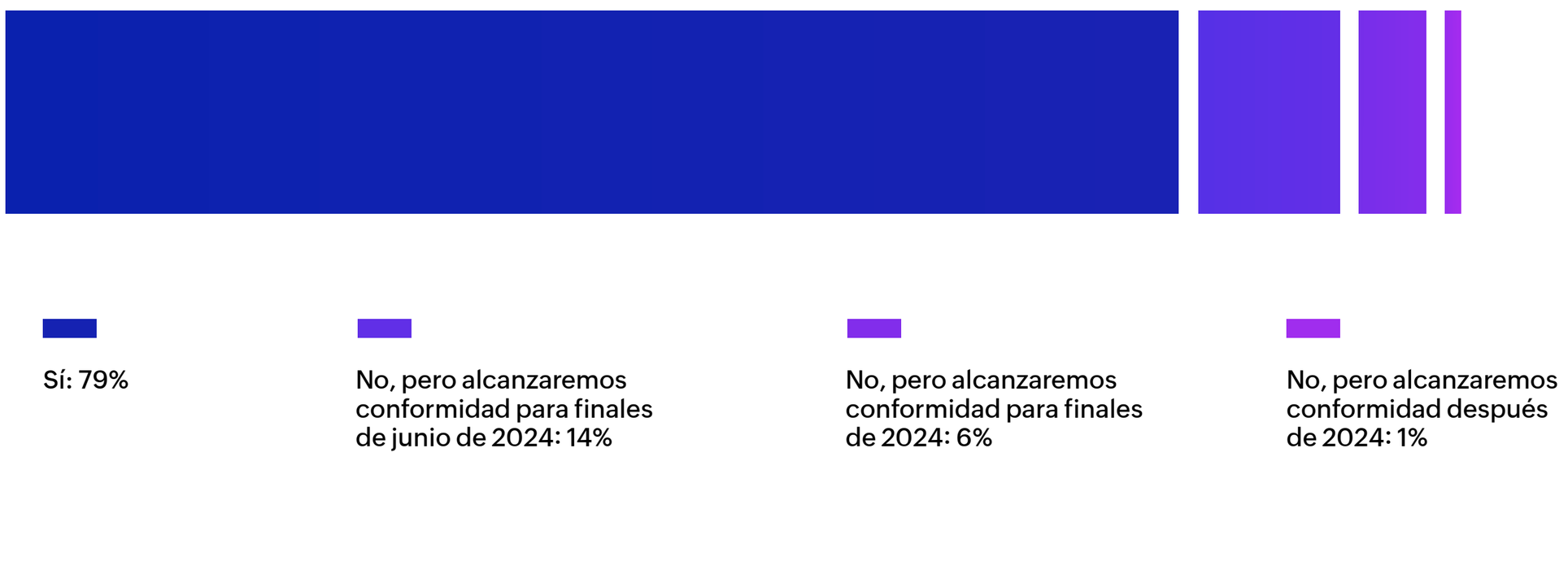
Resumen de la investigación (Sección 5: El aumento del estrés en los equipos de ciberseguridad.)

Los encuestados colombianos revelaron que sus empresas frecuentemente (42%) o constantemente (36%) brindaban oportunidades para mejorar sus habilidades en ciberseguridad.

Sección 6: Cumplimiento

Como se mencionó anteriormente, la necesidad de seguros de ciberseguridad y el cumplimiento con sus requisitos está generando un efecto positivo en las empresas colombianas, con un 79% afirmando que actualmente cumple con todas las regulaciones de protección de datos. El 20% afirma que cumplirá con estos elementos para fines del 2024.

Según su conocimiento, ¿su empresa cumple completamente con las regulaciones locales e internacionales de protección de datos?



Conclusión

Los hallazgos de la encuesta resaltan las preocupaciones apremiantes que enfrentan los profesionales de la seguridad en Colombia, con una cantidad creciente de problemas de seguridad emergiendo como el principal factor estresante. Esto es seguido de cerca por el desafío que presenta la falta de miembros experimentados en el equipo, especialmente a medida que el panorama de amenazas evoluciona con el aumento de los ataques habilitados por IA. Además, se suma la falta de apoyo de otros equipos dentro de la organización, que a menudo ignoran las reglas y políticas de seguridad, lo que resulta en que los empleados se conviertan en una amenaza significativa para la seguridad.

Si bien el liderazgo en seguridad reconoce la escasez de miembros experimentados en el equipo y se esfuerza por abordarla a través de opciones de capacitación regular, sigue existiendo una brecha entre el panorama de amenazas en evolución y la experiencia necesaria para combatirlo de manera efectiva, lo que confirma los desafíos continuos enfrentados por los equipos de seguridad.

Acerca de ManageEngine

ManageEngine es una división de Zoho Corporation que proporciona una solución integral de gestión de TI local y en la nube para una amplia gama de organizaciones, MSPs y MSSPs. Empresas establecidas y emergentes, incluidas 9 de cada 10 organizaciones Fortune 100, confían en las herramientas de gestión de TI en tiempo real de ManageEngine para garantizar el rendimiento óptimo de su infraestructura de TI, incluidas redes, servidores, aplicaciones, puntos finales y más. ManageEngine tiene oficinas en todo el mundo, incluidos Estados Unidos, Emiratos Árabes Unidos, Países Bajos, India, Colombia, México, Brasil, Singapur, Japón, China, Australia y Reino Unido, así como más de 200 socios globales para ayudar a las organizaciones a alinear estrechamente su negocio y TI.

ManageEngine

Para obtener más información, visite nuestro sitio web, el blog de la empresa o síganos en