ManageEngine

Estado de la Ciberseguridad para Latinoamérica 2024
MÉXICO

manageengine.com/latam

Índice

Introducción

Este artículo proporciona una breve sinópsis de una encuesta de investigación centrada en el estado de la ciberseguridad en México. Un total de 200 ejecutivos calificados y profesionales de la seguridad de pequeñas y grandes empresas completaron la encuesta. Los participantes ocupan puestos de alto nivel, nivel directivo y superior, y son directamente responsables de las estrategias y la seguridad informática de sus organizaciones. Esta investigación investigó las tendencias en todo tipo de industrias.

La investigación evaluó el impacto de la IA en la defensa de la ciberseguridad y en los miembros del equipo de seguridad, el uso de seguros de ciberseguridad y la capacidad de cumplir con los requisitos de gestión de datos.

Puntos clave

47%

En 2023, poco menos de la mitad (47%) de las empresas mexicanas afirmaron que la IA generativa jugó un papel importante en los ciberataques contra sus empresas.

84%

El 84% de los encuestados confirmó su confianza en la IA para implementar cambios adecuados, manejar respuestas a ataques y realizar otras tareas sin la necesidad de una revisión manual antes de la implementación.

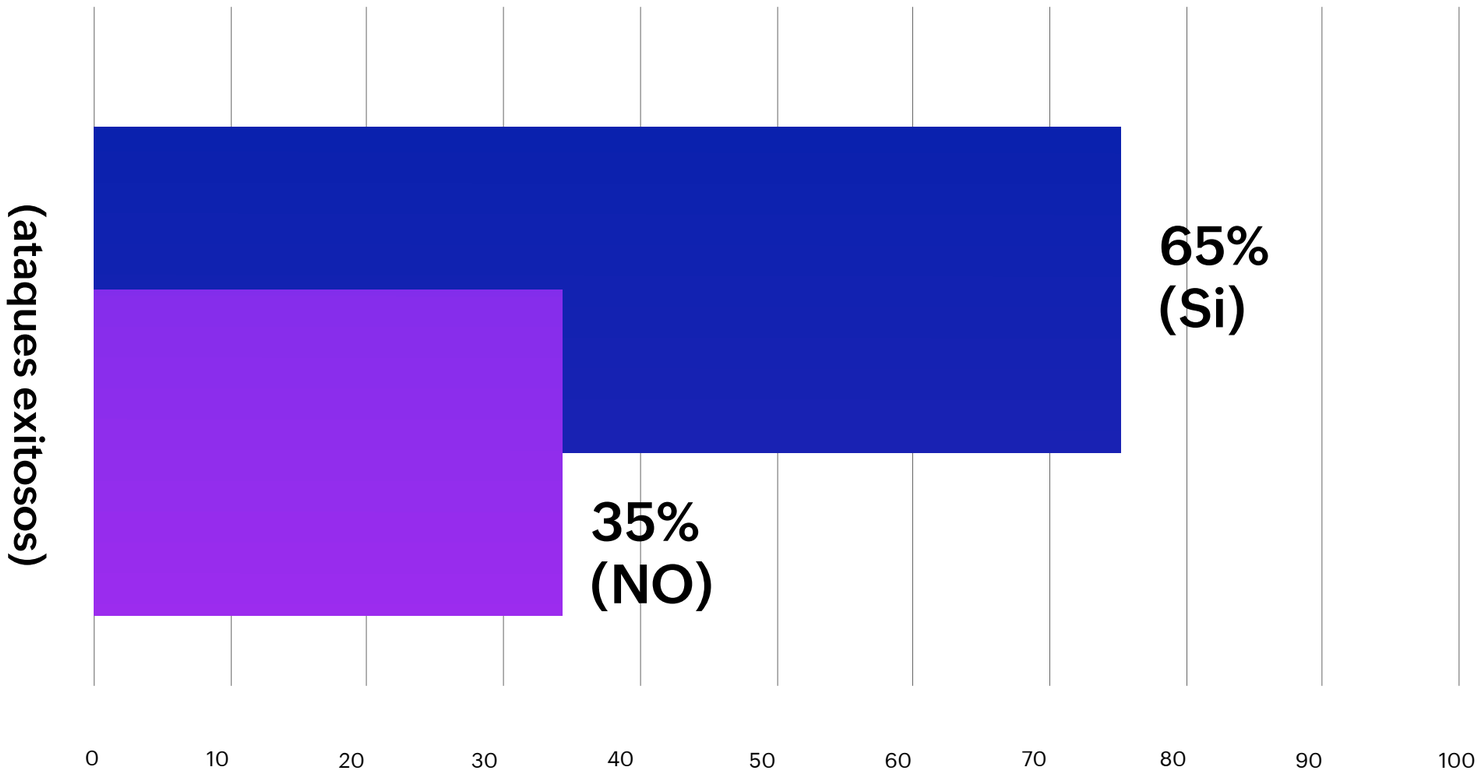
Puntos clave

Resumen de la investigación

Sección 1: Amenazas e impacto

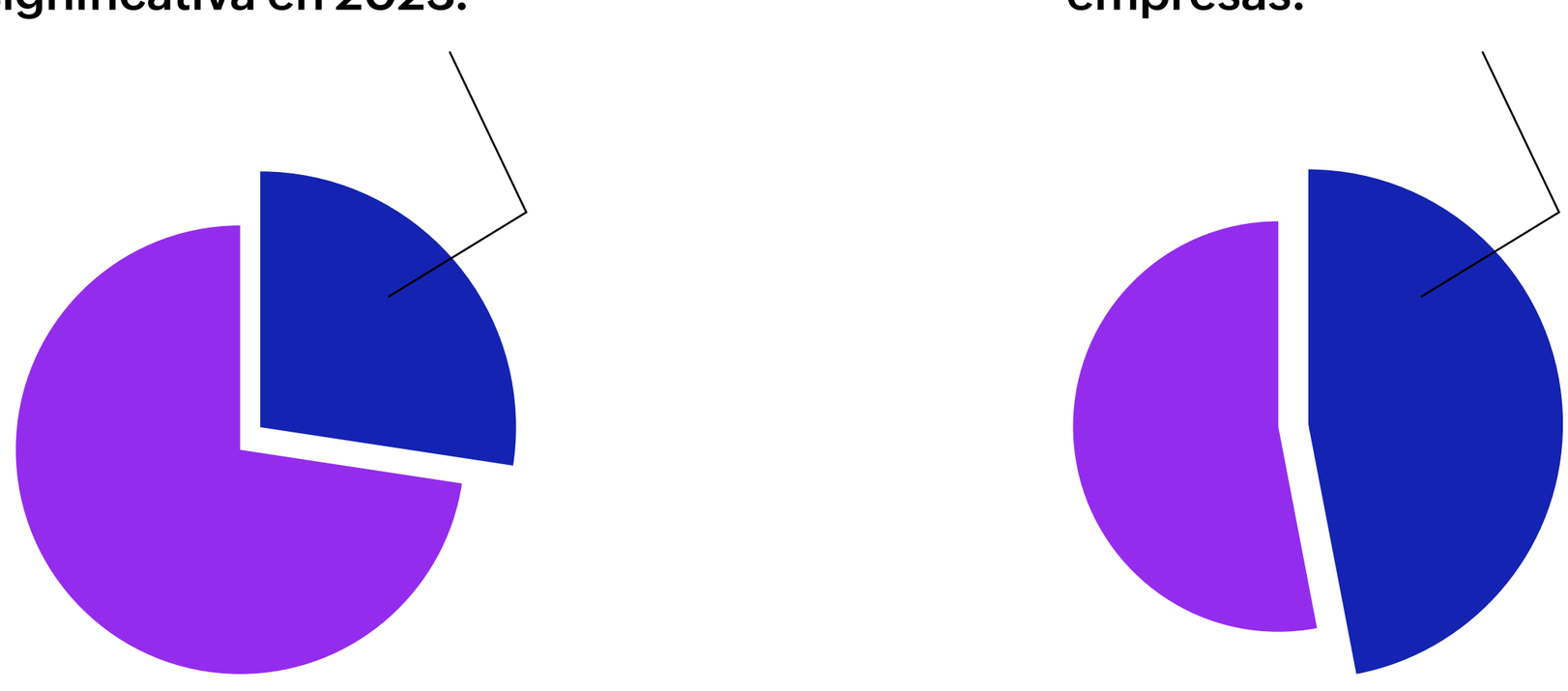
Los encuestados reconocieron que sus empresas encontraron un aumento en las violaciones de ciberseguridad en comparación con años anteriores. Entre las regiones estudiadas (Brasil, Colombia y Argentina), México registró el mayor número de incidencias. Sin embargo, los ataques que provocaron pérdidas financieras importantes siguieron siendo relativamente pocos.

¿Su empresa experimentó más violaciones de ciberseguridad (ataques exitosos) en 2023 en comparación con años anteriores? Sí: 65%



Solo el 27% 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 47% de los encuestados, la IA generativa jugó un papel importante en los ciberataques contra sus empresas.



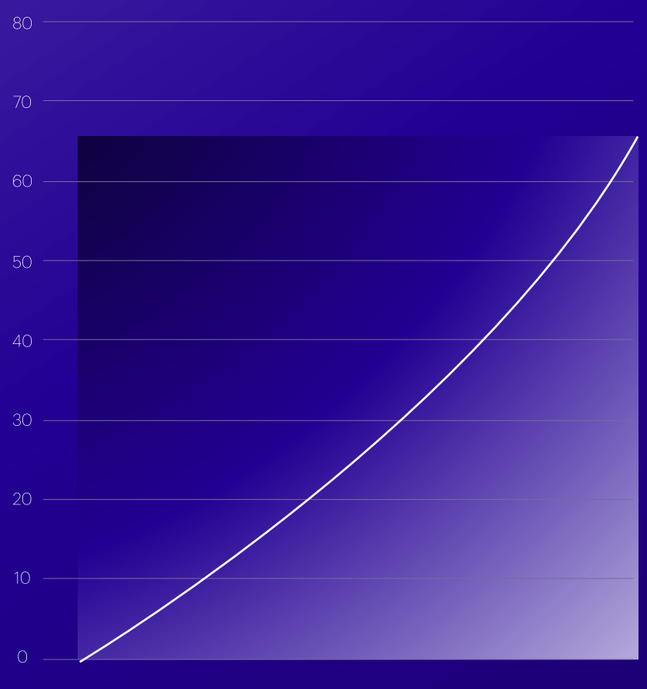
Sección 2: Seguro de ciberseguridad

La necesidad de asegurar la ciberseguridad y cumplir con sus requisitos está generando un efecto positivo en las empresas mexicanas

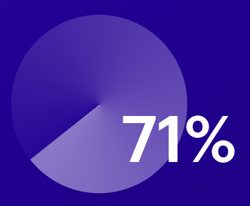
Mexico

65%

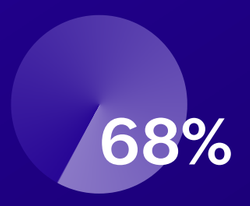
En México, el 65% de los encuestados afirmó que sus empresas realizaron exitosas reclamaciones de seguros de ciberseguridad.



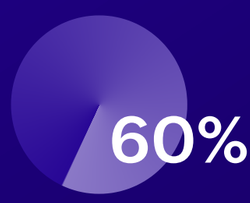
Los tres requisitos principales que las empresas debían cumplir para adquirir un seguro de ciberseguridad:



Adhesión a la normativa de protección de datos



Políticas de seguridad y control de acceso



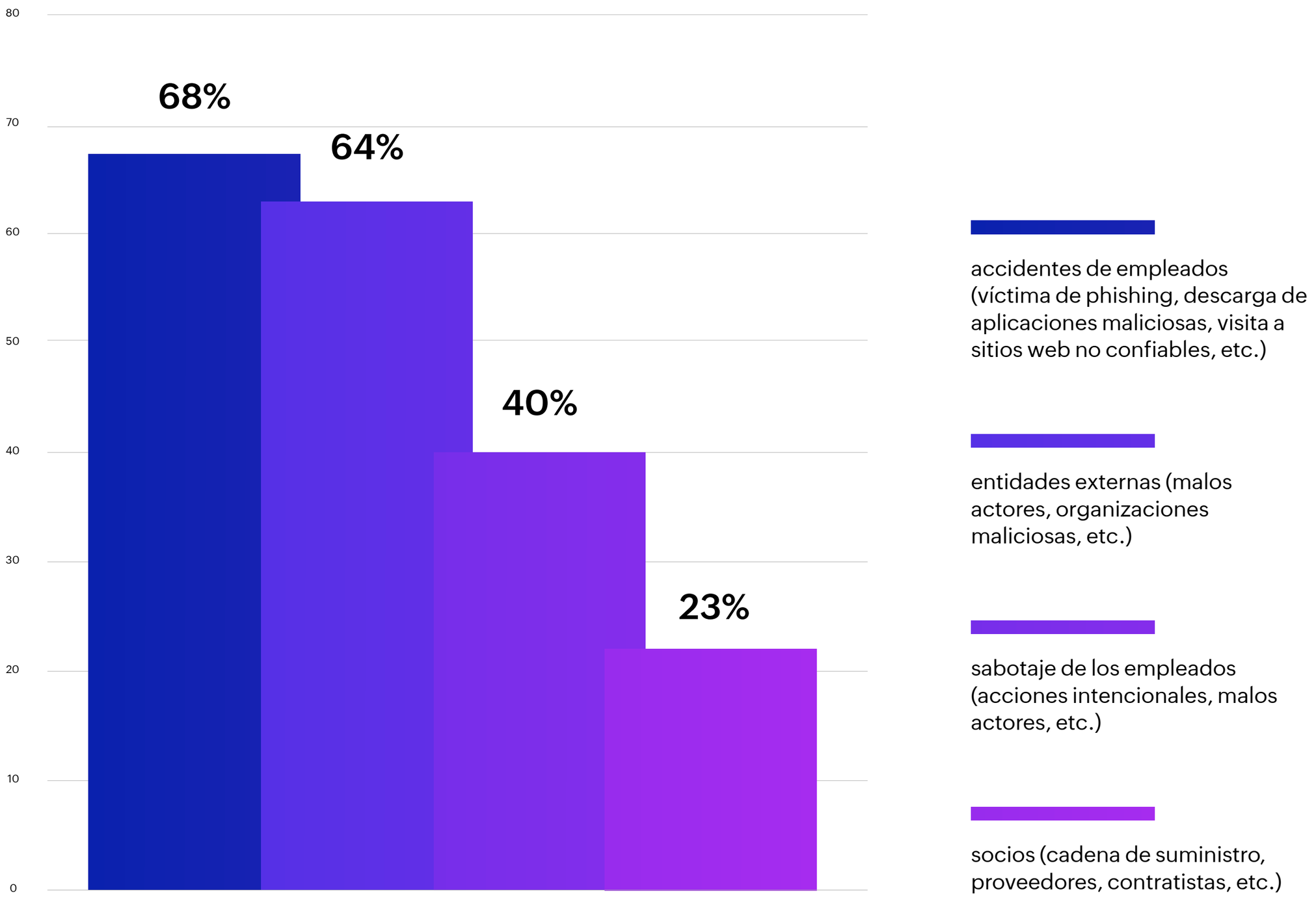
Evaluación y gestión de riesgos

ManageEngine

Sección 3: Papel de los empleados

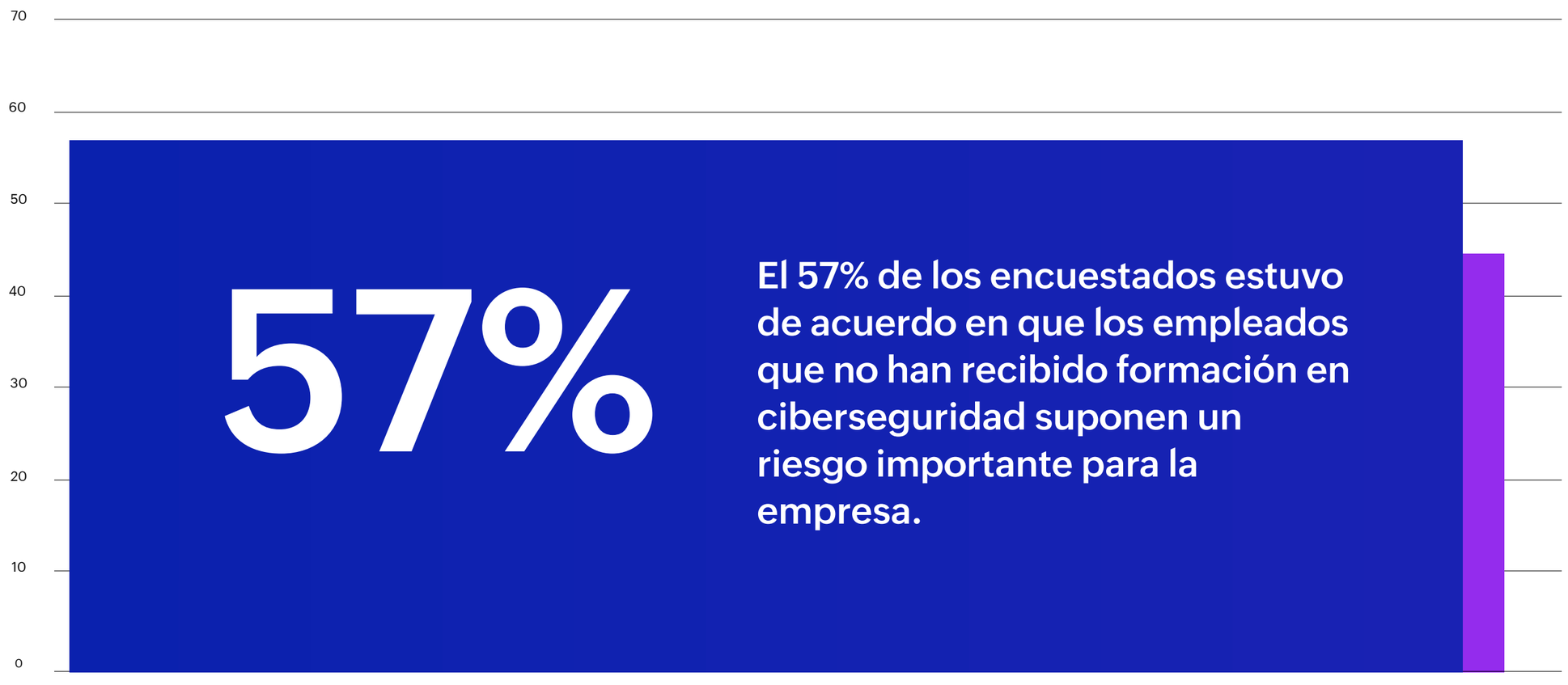
En México, las amenazas internas parecen representar un riesgo significativo para las organizaciones. Estas amenazas generalmente provienen de personas con acceso autorizado a los sistemas, datos o instalaciones de una organización que, consciente o accidentalmente, explotan sus privilegios con fines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

Según su experiencia, ¿cómo se producen la mayoría de las amenazas a la seguridad?

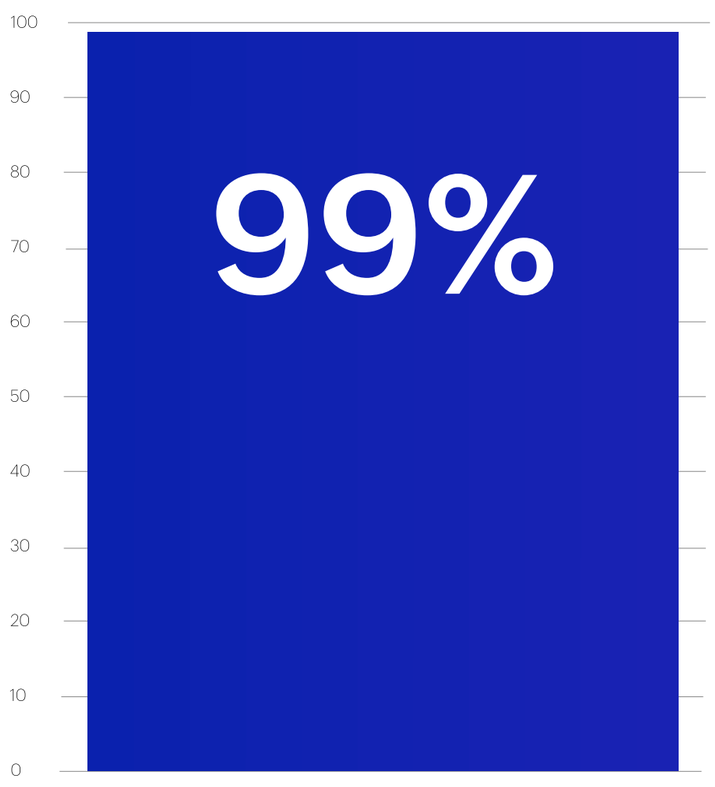


ManageEngine

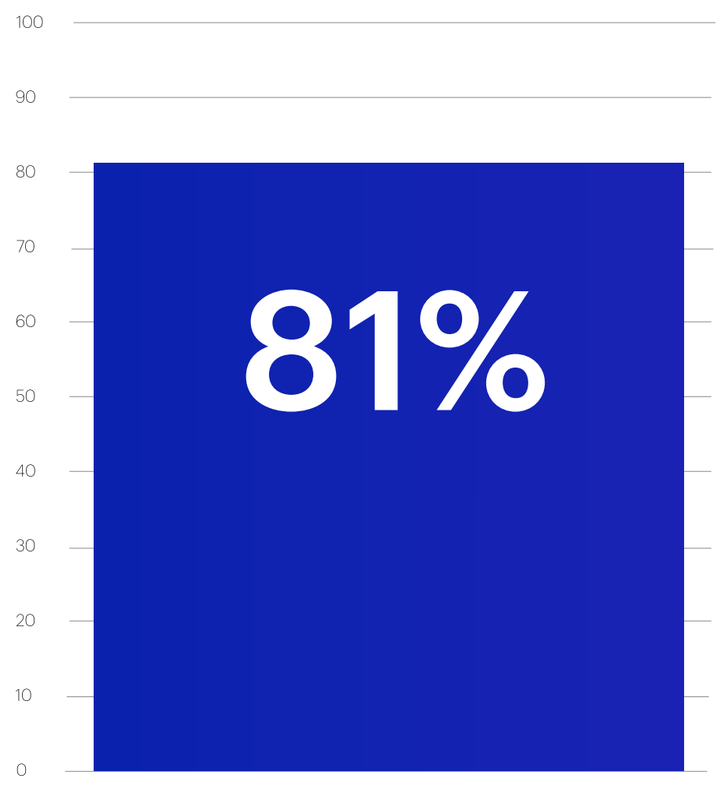
Las empresas comprenden la amenaza, dados los numerosos riesgos internos que enfrentan, y existe preocupación por la calidad de la capacitación de los empleados. Esto hace que la formación de los empleados, especialmente de aquellos que se han incorporado recientemente a la organización, sea una necesidad absoluta.



Casi todos los encuestados (99%) afirmaron que su empresa proporcionaba formación en ciberseguridad a sus empleados.



La mayoría de los encuestados (81%) afirmó que esta formación se ofrece dentro del mes siguiente a la contratación.

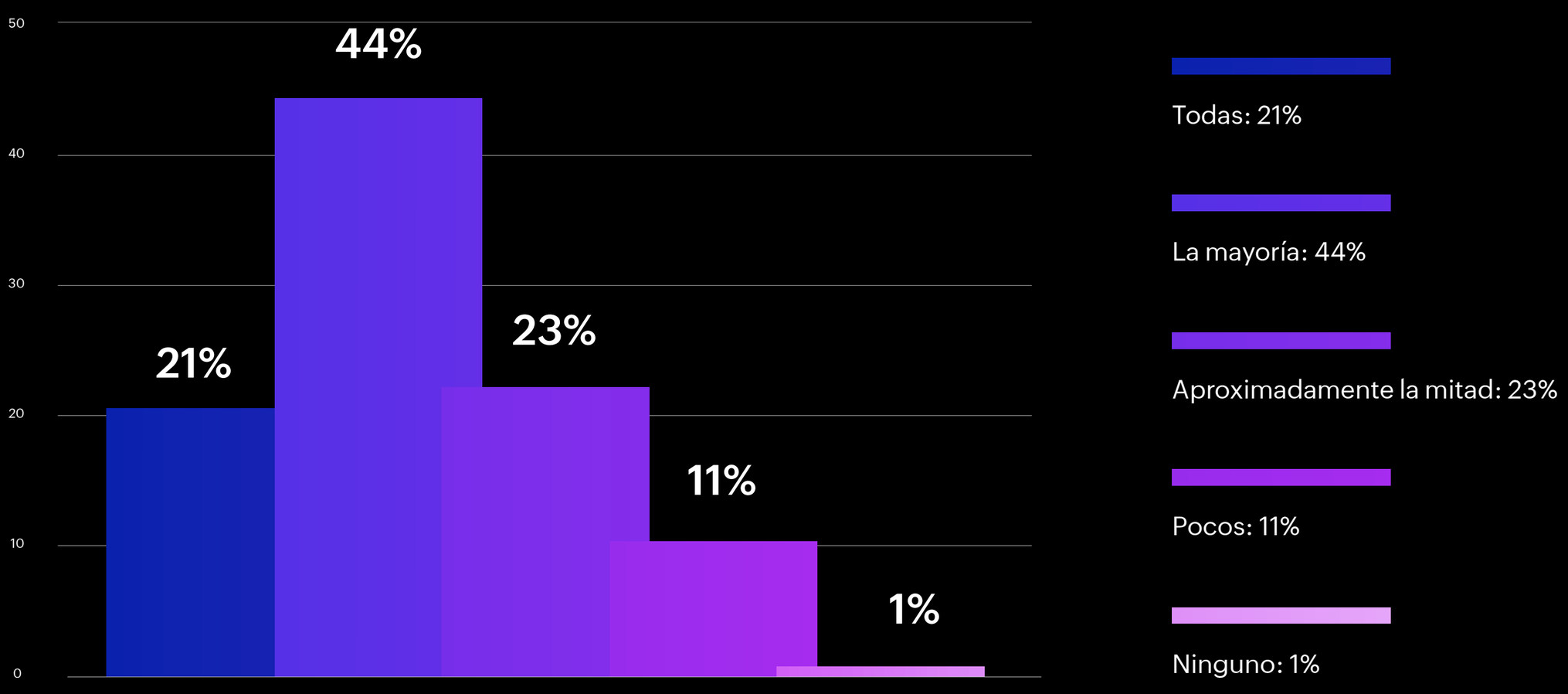


ManageEngine

Sección 4: Papel de la IA

Los profesionales de la seguridad afirman que se necesitan soluciones de seguridad basadas en IA, y el 92% afirma que IA fueron fundamentales para defender su empresa este año. Esto llevó a que el 88% indicara que la mitad o más de todas sus soluciones de seguridad estarán impulsadas por IA para fines de 2024.

Hasta donde usted sabe, ¿cuántas de las soluciones de ciberseguridad de su empresa utilizarán IA en 2024?



La investigación encontró algunos hallazgos significativos: el 84% expresó una confianza inquebrantable en las herramientas de seguridad habilitadas por IA para implementar cambios y ejecutar acciones sin ninguna intervención humana. Esto puede deberse a la falta de profesionales con experiencia en ciberseguridad que se señala en la sección posterior. No obstante, los profesionales de la seguridad reconocen los riesgos y el 85% aboga por una organización independiente para verificar la confiabilidad de las soluciones de seguridad habilitadas por IA.

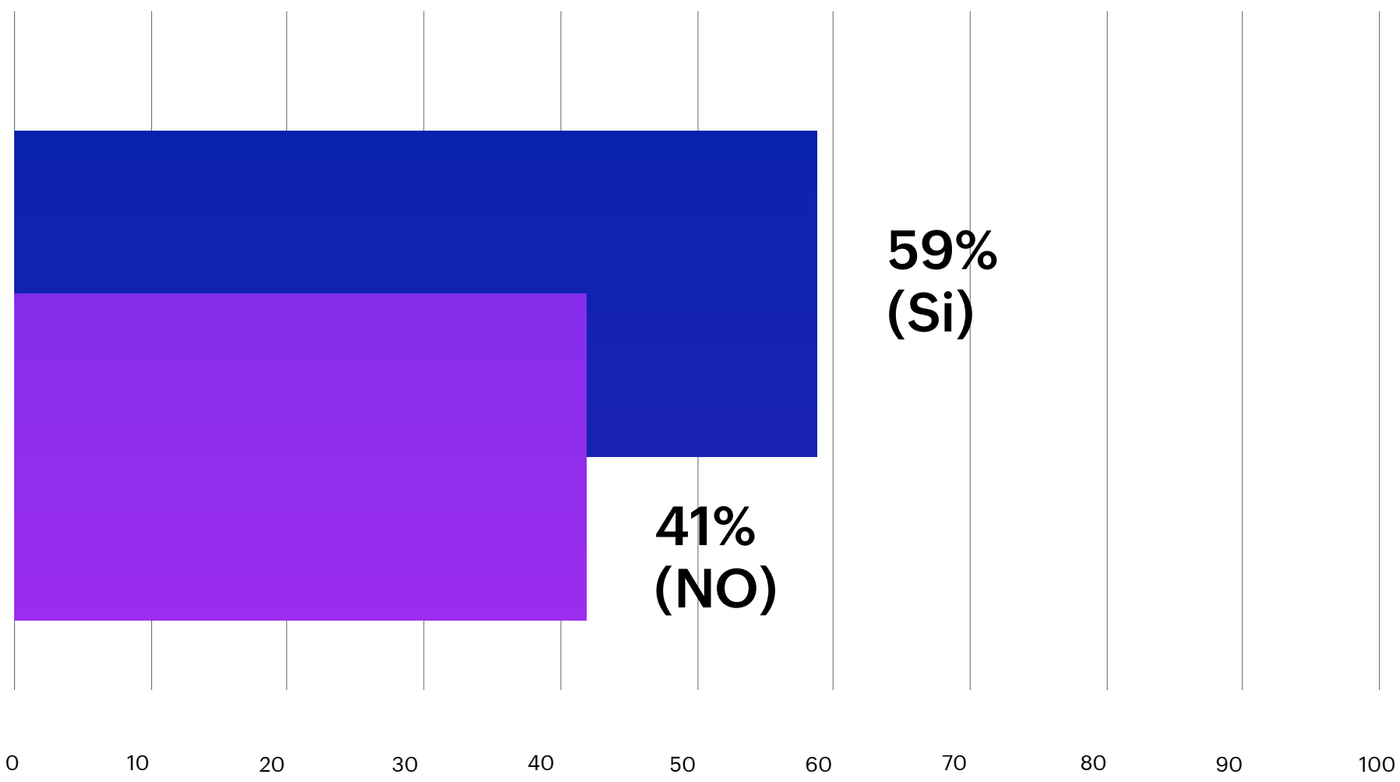
El hecho es que los ataques impulsados por IA son más efectivos, crean dificultades financieras y aumentan el estrés en los equipos de seguridad. En 2024, las empresas necesitarán herramientas habilitadas para IA y profesionales experimentados para defender el negocio y proteger sus datos contra las crecientes amenazas de la IA.

Sección 5: Aumento del estrés en los equipos de ciberseguridad

Con la creciente frecuencia de los ataques a la ciberseguridad amplificada aún más por GenAI, la carga para los profesionales de la ciberseguridad se ha intensificado.

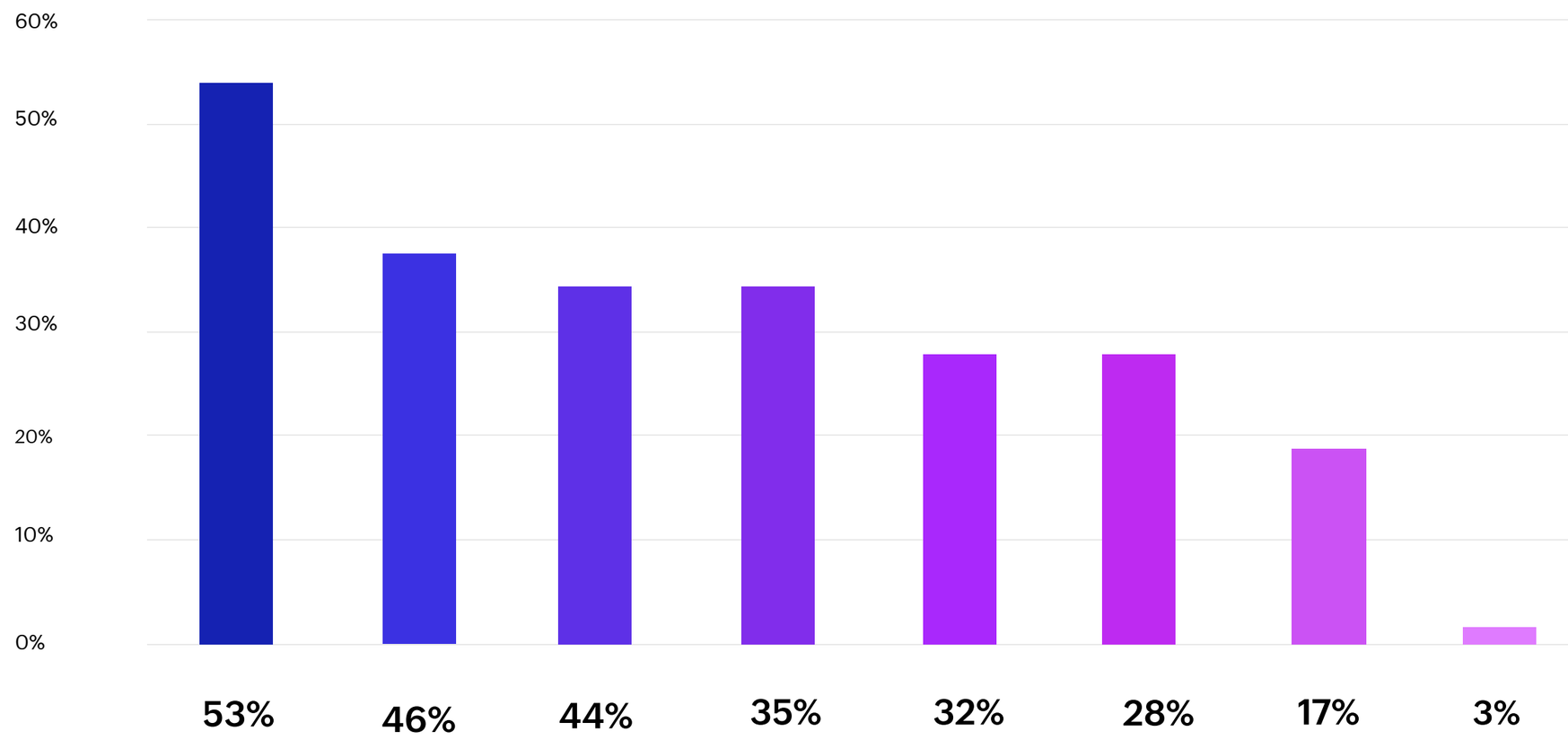
El 59% de los encuestados reveló que sus niveles de estrés han aumentado debido al trabajo en los últimos años. Curiosamente, en comparación con otros países encuestados (Brasil, Colombia, Argentina), México mostró el menor aumento en los niveles de estrés.

¿En los últimos años ha aumentado su nivel de estrés debido al trabajo ?



Sección 5: Aumento del estrés en los equipos de ciberseguridad

¿Qué está provocando que su nivel de estrés aumente?

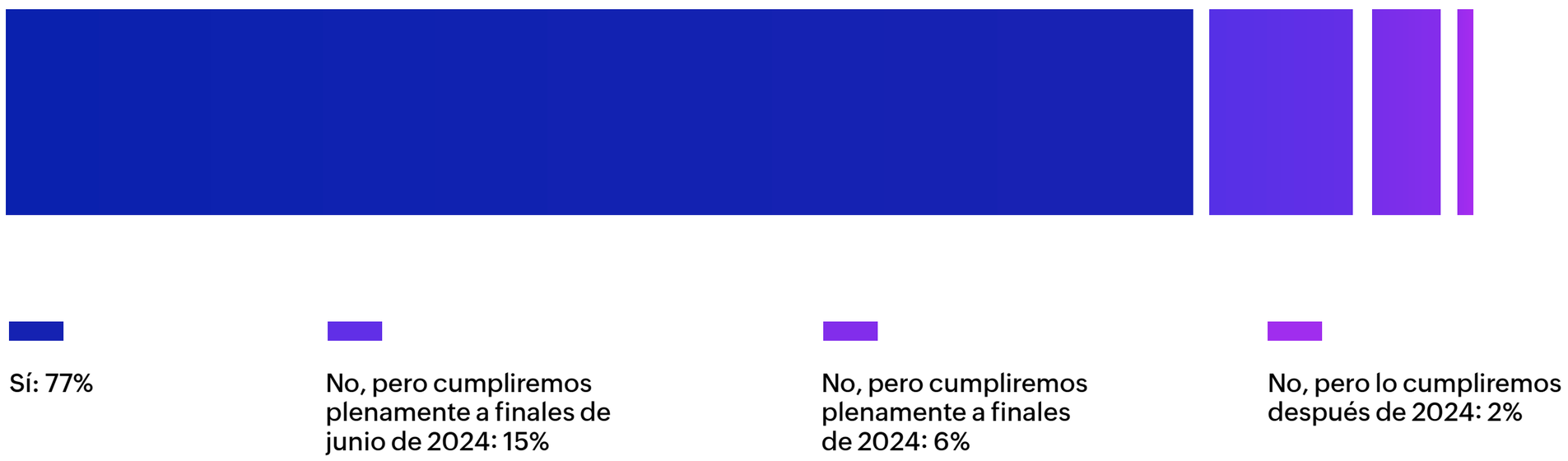


Los encuestados mexicanos revelaron que sus empresas frecuentemente (42%) o constantemente (38%) brindaban oportunidades para mejorar sus habilidades en ciberseguridad.

Sección 6: Cumplimiento

Como se mencionó anteriormente, la necesidad de contar con un seguro de ciberseguridad y cumplir con sus requisitos está generando un efecto positivo en las empresas mexicanas, ya que el 77% afirma que actualmente cumple con todas las normas de protección de datos. Un 21% adicional afirma que cumplirá las normas a finales de 2024.

Hasta donde usted sabe, ¿su empresa cumple plenamente con las normas de protección de datos locales e internacionales?



Conclusión

Los resultados de la encuesta resaltan las preocupaciones apremiantes que enfrentan los profesionales de la seguridad en México, con un número cada vez mayor de problemas de seguridad que emergen como el principal factor estresante. A esto le sigue de cerca el desafío que presenta la falta de miembros experimentados en el equipo, particularmente a medida que el panorama de amenazas evoluciona con el aumento de los ataques habilitados por IA. A esto 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 hace que los empleados se conviertan en una amenaza importante para la seguridad.

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

Acerca de ManageEngine

ManageEngine es una división de Zoho Corporation que ofrece soluciones integrales de gestión de operaciones de TI, on premises y en la nube, para organizaciones globales y proveedores de servicios gestionados. Las empresas establecidas y emergentes, incluidas 9 de cada 10 organizaciones Fortune 100, confían en las herramientas de administración de TI en tiempo real de ManageEngine para garantizar el rendimiento óptimo de su infraestructura de TI, incluidas redes, servidores, aplicaciones, endpoints y más. ManageEngine tiene 18 data centers, 20 oficinas y más de 200 partners en todo el mundo para ayudar a las organizaciones a alinear estrechamente sus negocios con TI. Para obtener más información, visite nuestro sitio web.

ManageEngine

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