ManageEngine

Estado de la Ciberseguridad para Latinoamérica 2024
ARGENTINA

manageengine.com/latam

Índice

Introducción

Este documento proporciona un breve resumen de una encuesta centrada en el estado de la ciberseguridad en Argentina. Un total de 150 ejecutivos calificados y profesionales de seguridad en pequeñas empresas y grandes corporaciones completaron la encuesta. Los participantes ocupaban cargos de alta jerarquía, a nivel de gerente y superior. Eran directamente responsables de la protección y estrategias de seguridad cibernética de sus organizaciones.

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

Aspectos Clave

ManageEngine

Aspectos Clave

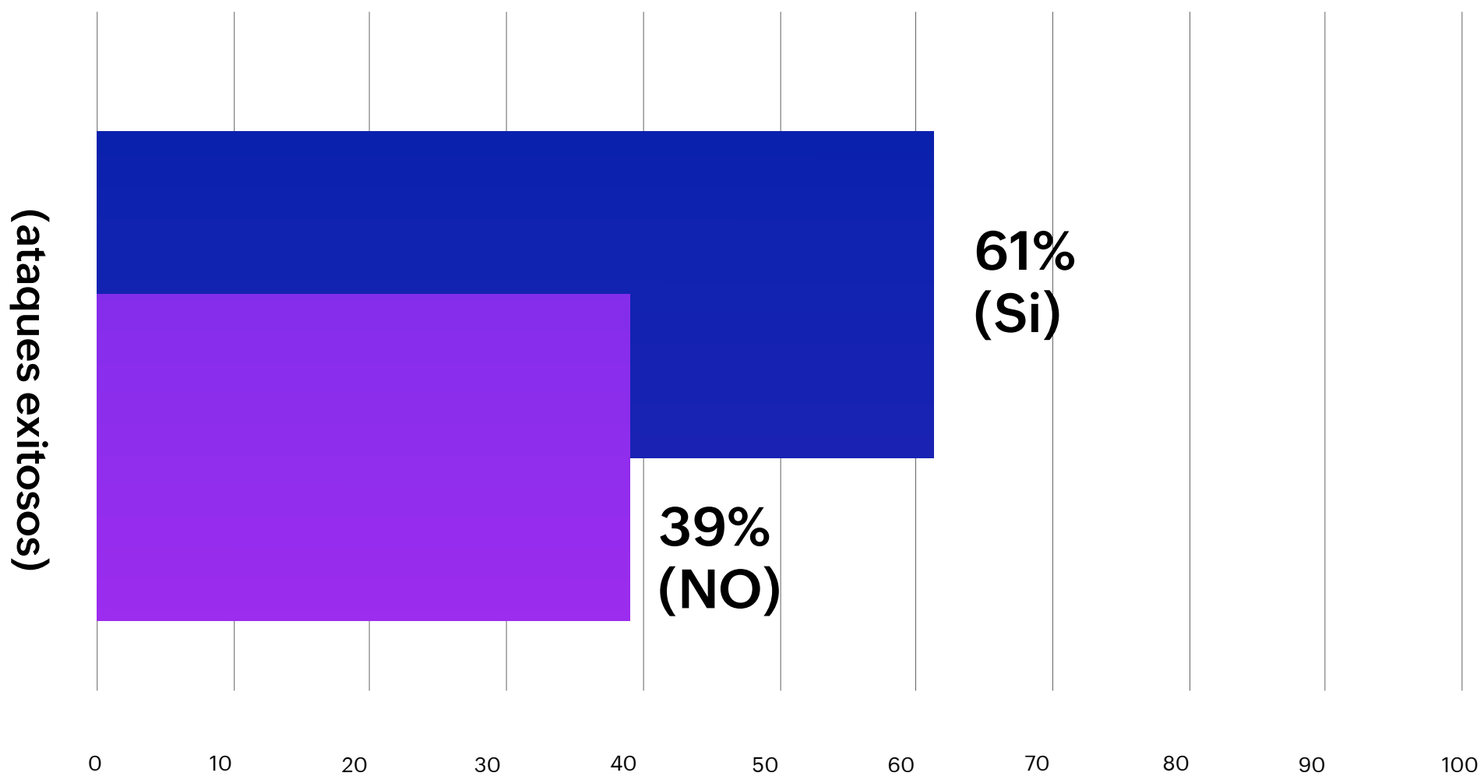
ManageEngine

Resumen de la Investigación

Sección 1: Amenazas e Impacto

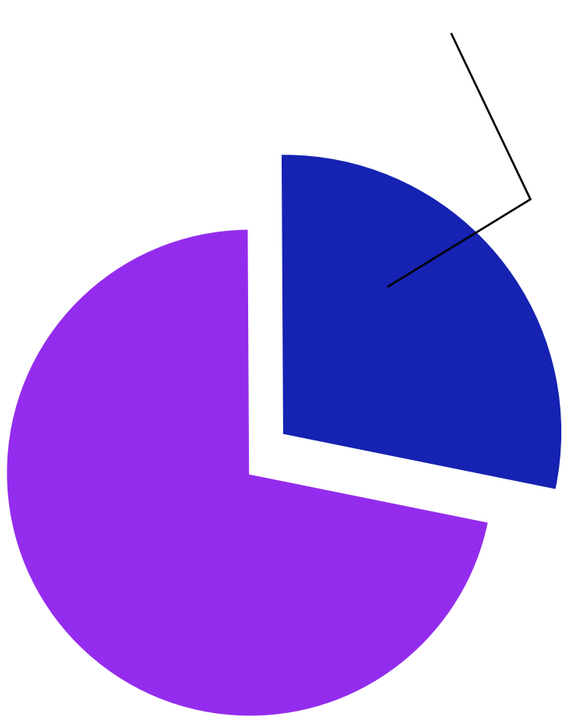
Los encuestados reconocieron que sus empresas experimentaron un aumento en las violaciones de ciberseguridad en comparación con años anteriores. Sin embargo, los ataques que resultaron en pérdidas financieras significativas siguieron siendo relativamente bajos.

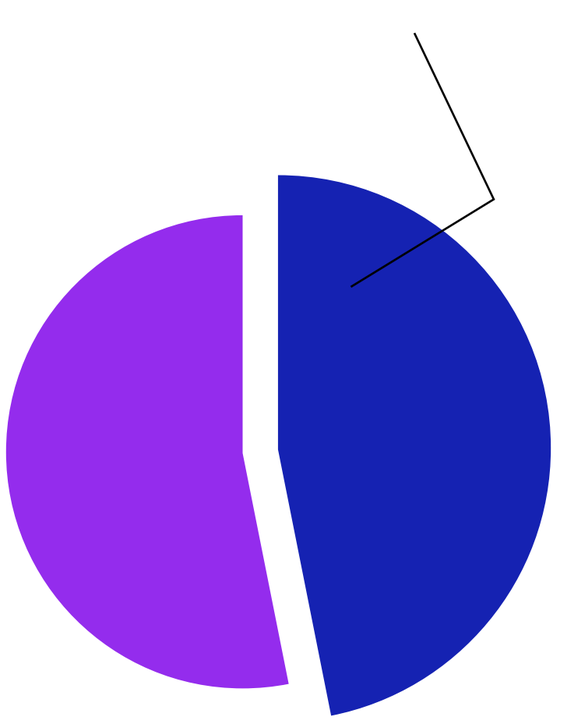
¿Tu empresa experimentó más violaciones de ciberseguridad (ataques exitosos) en 2023 en comparación con años anteriores?



El 29% de los encuestados aseguró que sus empresas experimentaron un ataque de ciberseguridad que resultó en una pérdida financiera significativa en 2023.

Según el 47% de los encuestados, la inteligencia artificial generativa jugó un papel significativo en los ciberataques contra sus empresas en 2023.





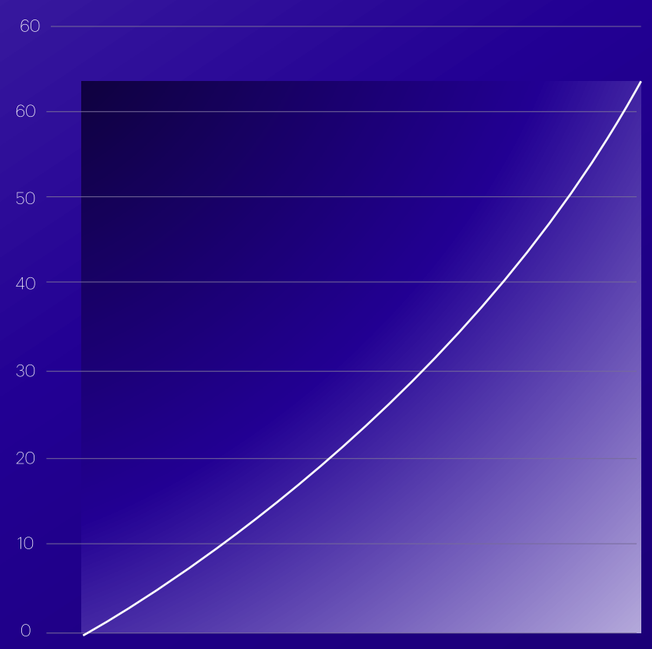
ManageEngine

Sección 2: Seguro de Ciberseguridad

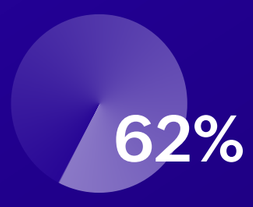
La necesidad de seguros de ciberseguridad y cumplir con sus requisitos está generando un efecto positivo en las empresas argentinas.

63%

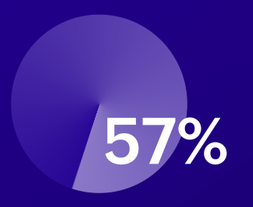
En Argentina, el 63% de los encuestados afirmó que sus empresas realizaron reclamaciones exitosas de seguros de ciberseguridad.



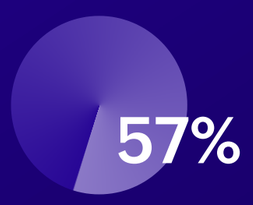
Los tres requisitos principales que las empresas tuvieron que cumplir para adquirir un seguro de ciberseguridad fueron:



Políticas de seguridad y control de acceso



Capacitación regular de empleados



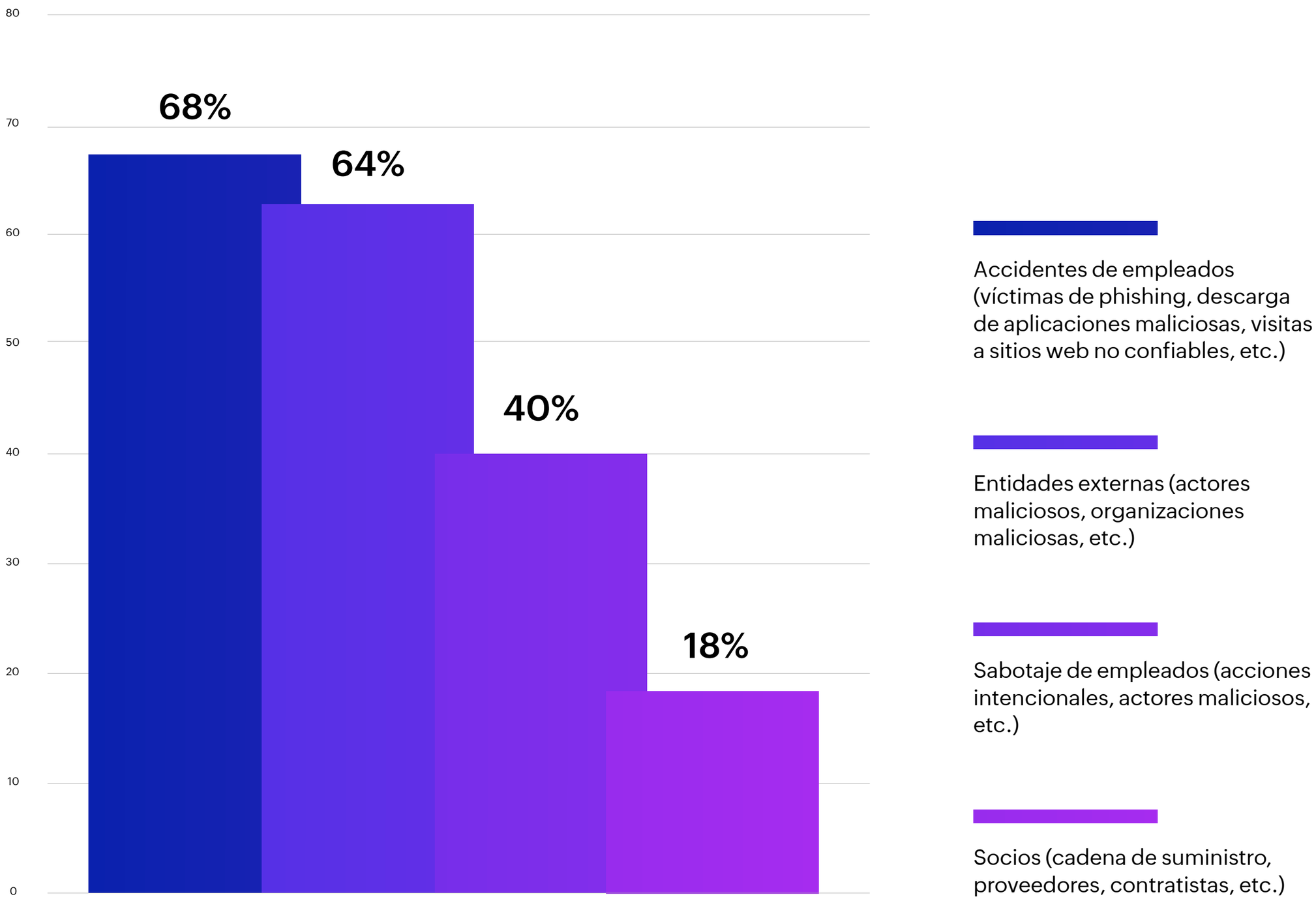
Adherencia a las regulaciones de protección de datos

ManageEngine

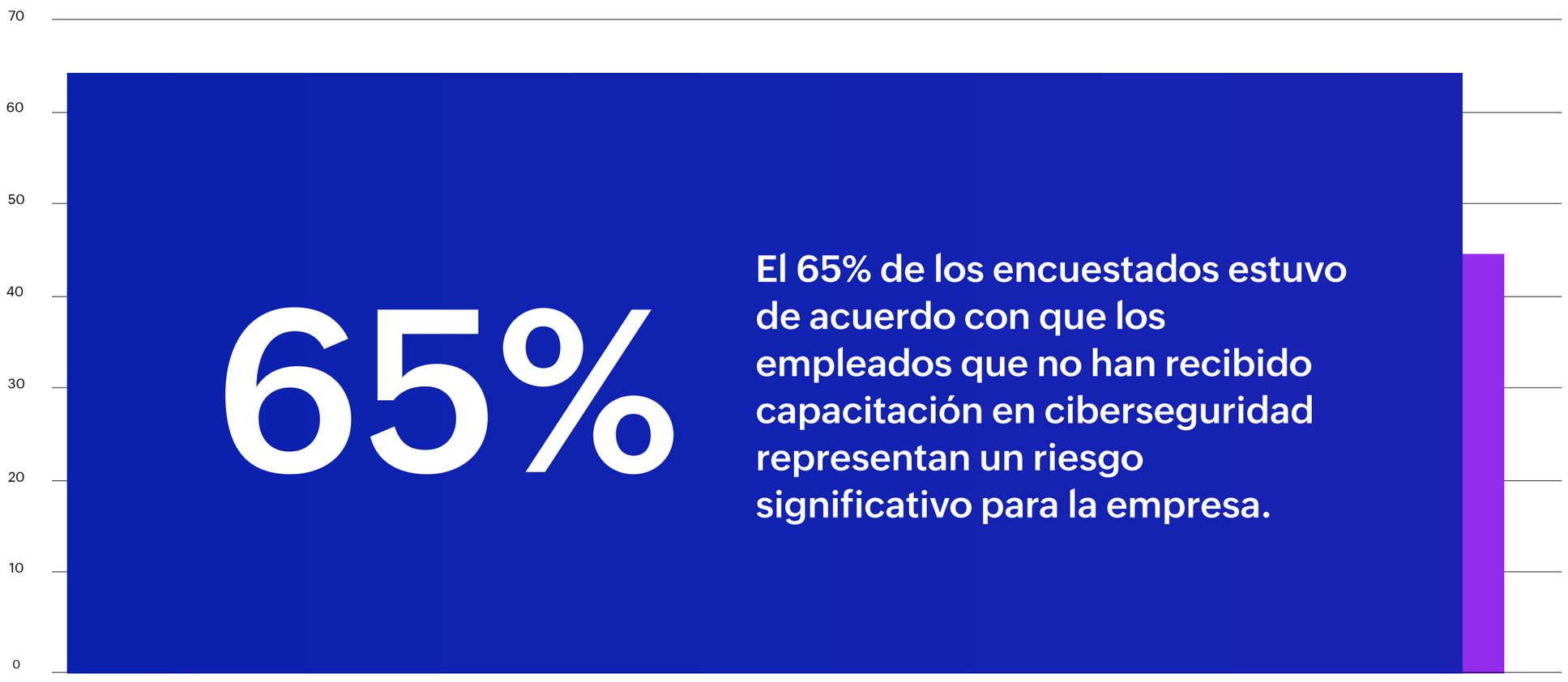
Sección 3: Rol de los empleados

En Argentina, las amenazas internas parecen representar un riesgo significativo para las organizaciones. Estos riesgos generalmente provienen de individuos con acceso autorizado a los sistemas, datos o instalaciones de una organización. De manera consciente o accidental, ellos explotan sus privilegios con fines maliciosos. Las implicaciones de tales amenazas pueden ser graves: pérdidas financieras, responsabilidades legales, daños a la reputación e incluso 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 experimentan, y hay 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 (95%) afirmaron que su empresa proporcionaba capacitación en ciberseguridad a sus empleados.

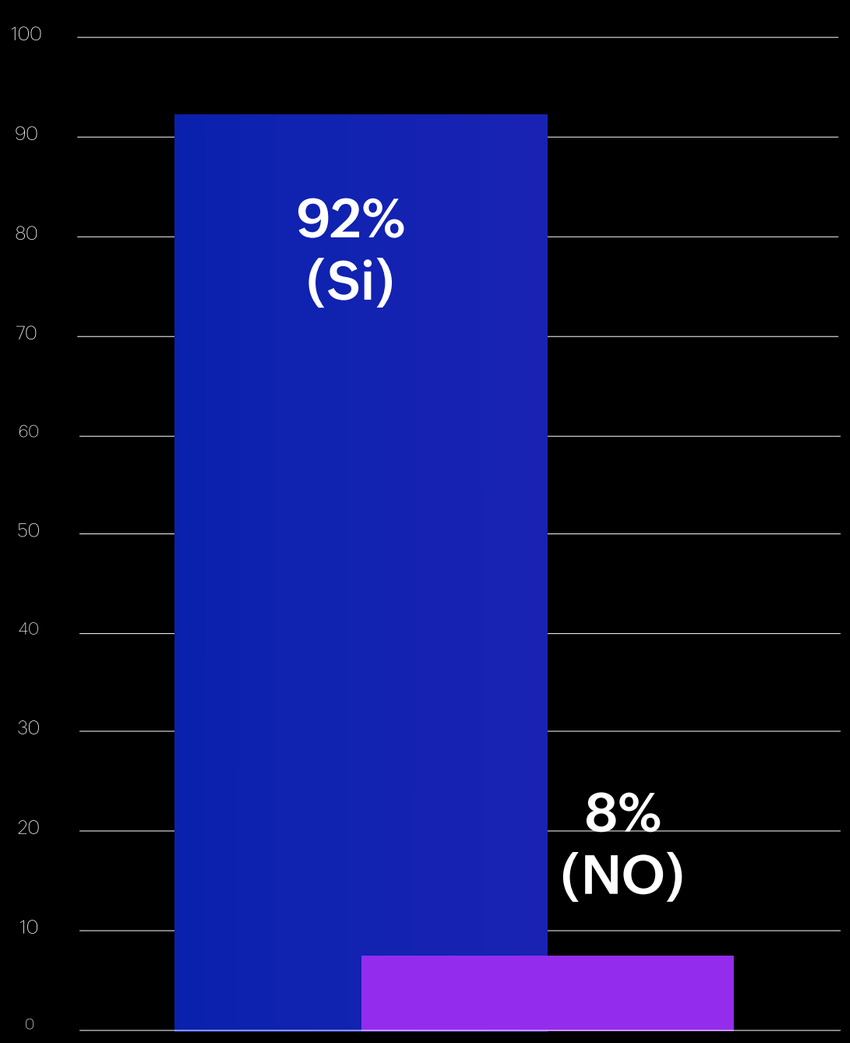
El 60% de los encuestados afirmó que esta capacitación se ofrecía dentro del primer mes de contratación. Argentina obtuvo un índice más bajo en este aspecto, en comparación con el resto de los países encuestados.

Sección 4: Rol de la IA

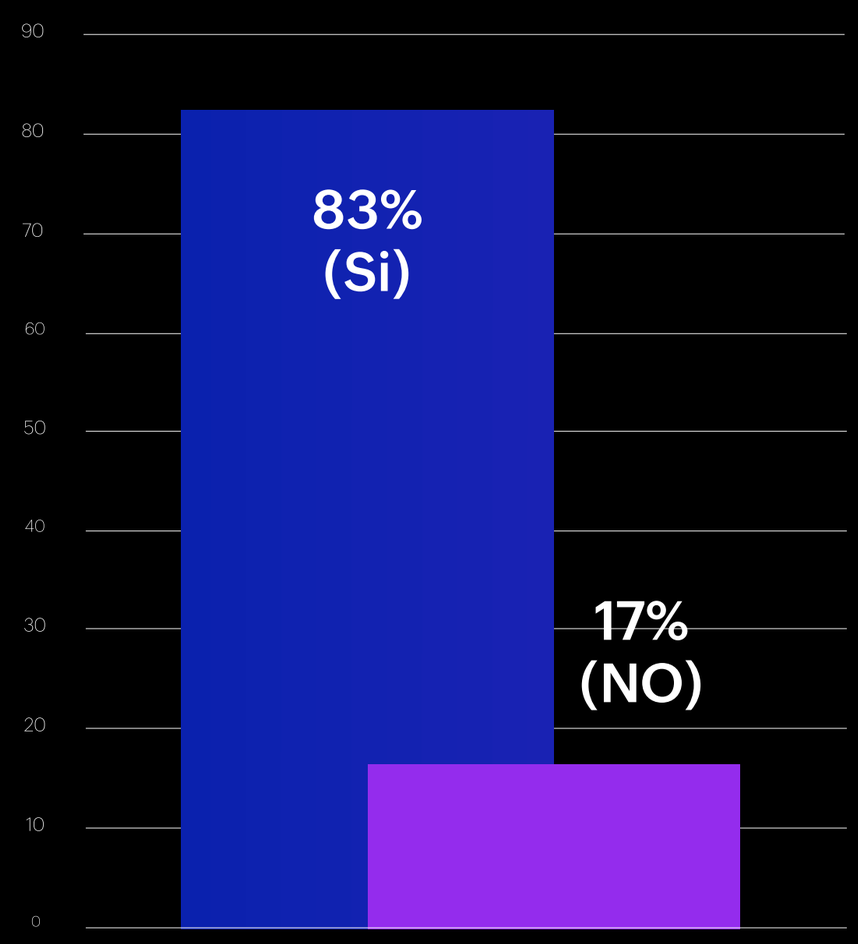
Los ataques impulsados por inteligencia artificial son más efectivos, creando dificultades financieras y aumentando el estrés en los equipos de seguridad. En 2024, las empresas necesitarán herramientas habilitadas para la inteligencia artificial y profesionales experimentados para defender el negocio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

El 92% afirmó que la inteligencia artificial será fundamental para defenderse contra los ciberataques en 2024 en Argentina.

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

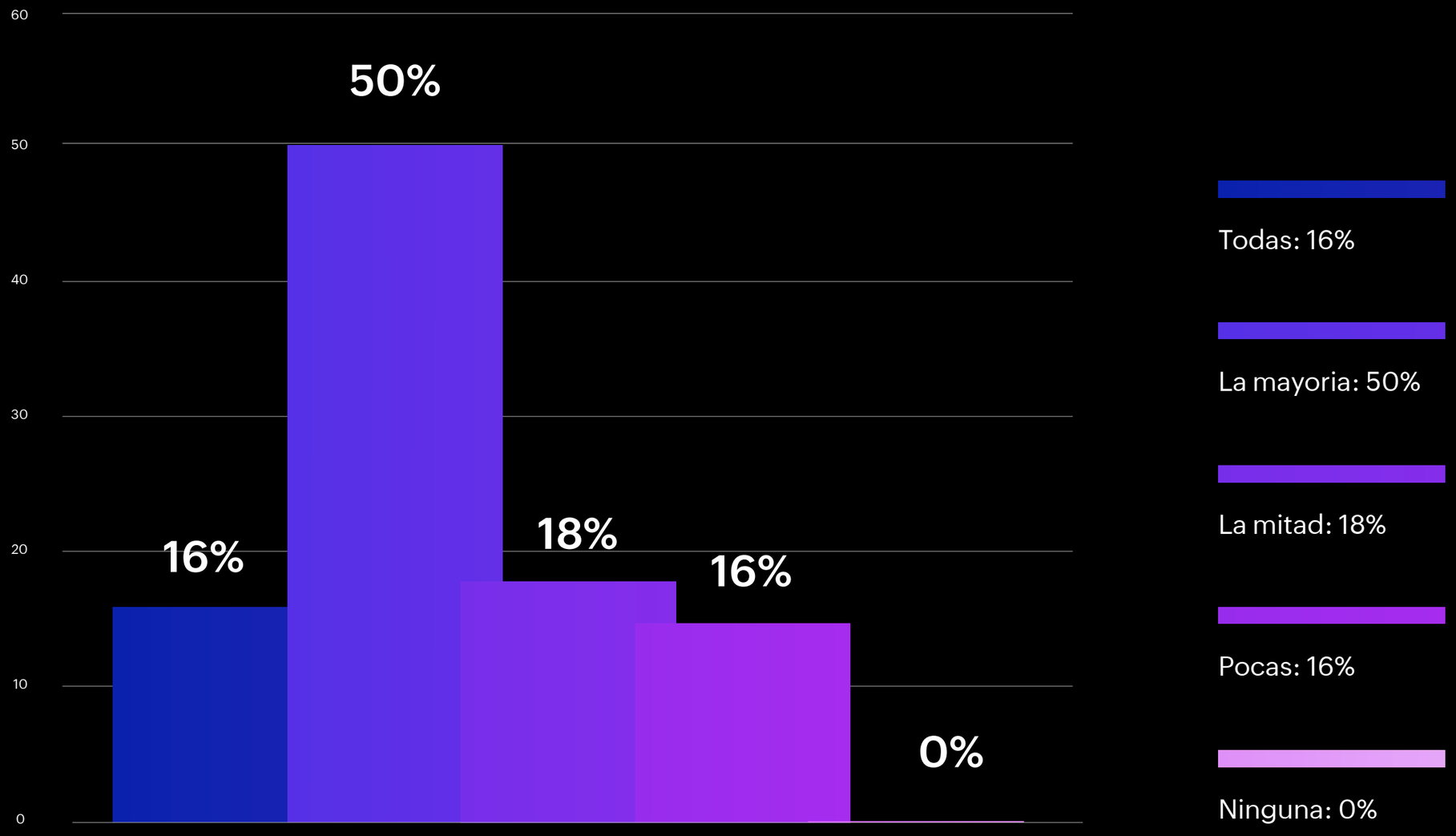


Esto llevó al 83% a indicar que la mitad o más de todas sus soluciones de seguridad estarán impulsadas por inteligencia artificial para fines de 2024.



ManageEngine

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



La investigación descubrió algunos hallazgos controvertidos, con un 82% expresando una confianza inquebrantable en las herramientas de seguridad habilitadas para la inteligencia artificial para realizar cambios y ejecutar acciones sin ninguna intervención humana. Esto puede haber surgido de la falta de profesionales experimentados en ciberseguridad.

Sin embargo, los profesionales de seguridad reconocen los riesgos. Un 82% aboga por una organización independiente para verificar la confiabilidad de las soluciones de seguridad habilitadas para la inteligencia artificial.

Sección 5: Aumento del Estrés en los equipos de ciberseguridad

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

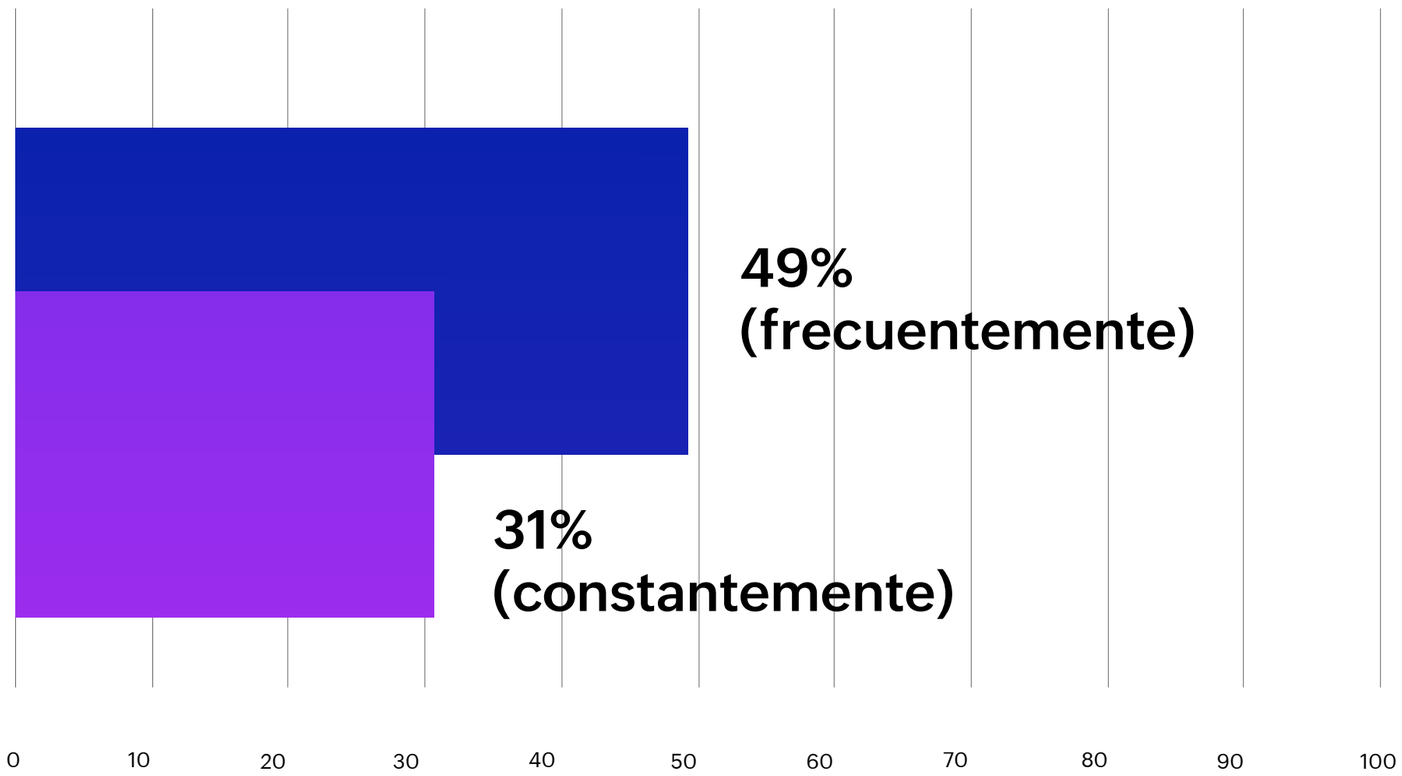
El 65% de los encuestados reveló que sus niveles de estrés han aumentado debido al trabajo en los últimos años.

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

¿Qué está causando que aumente su nivel de estrés?

ManageEngine

Los encuestados argentinos revelaron que sus empresas frecuentemente (49%) o constantemente (31%) brindan oportunidades para mejorar sus habilidades en ciberseguridad.



Sección 6: Conformidad

Como se mencionó, la necesidad de seguros de ciberseguridad y cumplir con sus requisitos está generando un efecto positivo en las empresas argentinas. Un **82%** afirma que actualmente cumplen con todas las regulaciones de protección de datos. En comparación con el resto de los países encuestados, Argentina obtuvo una calificación más alta. Un **16%** adicional afirma que cumplirán para fines de 2024.

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

Sí: 82%

No, pero alcanzaremos conformidad para finales de junio de 2024: 10%

No, pero alcanzaremos conformidad para finales de 2024: 6%

No, pero alcanzaremos conformidad después de 2024: 2%

Conclusión

Los hallazgos de la encuesta resaltan las preocupaciones urgentes que enfrentan los profesionales de la ciberseguridad en Argentina, con una cantidad creciente de problemas que emergen 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. 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. Esto resulta en que los empleados se conviertan en una amenaza significativa.

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, todavía existe una brecha entre el panorama de amenazas en evolución y la experiencia necesaria para combatirla de manera efectiva. Esto resalta los desafíos continuos enfrentados por los equipos de seguridad cibernética.

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, MSP y MSSP. 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. Lo anterior incluye redes, servidores, aplicaciones, puntos finales y más. ManageEngine tiene oficinas en todo el mundo: Estados Unidos, Emiratos Árabes Unidos, Países Bajos, India, Colombia, México, Brasil, Singapur, Japón, China, Australia y Reino Unido. Cuenta con 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