A Lynchpin Media BRAND

CXO priorities

INFORME DE PRIORIDADES DE CXO LATAM 2024:

Principales tendencias, desafíos y prioridades de ciberseguridad para los CIOs en América Latina

Un informe de prioridades de CXO en colaboración con paloalto NETWORKS

Contenido

Introducción

Los cambios en el panorama tecnológico nunca han ocurrido tan rápidamente. Las herramientas digitales se están adoptando en todos los sectores para transformar la forma en que operan las empresas. Sin embargo, este entorno digital en rápida evolución trae consigo desafíos, especialmente en términos de ciberseguridad. Desde la necesidad de cumplimiento (compliance, en inglés) hasta la aparición de nuevas amenazas, los líderes tecnológicos deben enfrentar un panorama complejo para proteger sus organizaciones mientras impulsan la innovación y el crecimiento.

En este informe, exploramos las principales percepciones, conocimientos y prioridades de los Chief Information Officers (CIOs) en América Latina, revelando una amplia gama de preocupaciones. La gobernanza, el cumplimiento y la demostración del Retorno Sobre la Inversión (ROI, por sus siglas en inglés) surgen como las principales prioridades de los encuestados, mientras que la colaboración y la comunicación entre los ejecutivos se identifican como elementos cruciales para una estrategia eficaz de ciberseguridad. A medida que las organizaciones buscan herramientas digitales para aumentar la rentabilidad y la eficiencia, el papel del CIO en la toma de decisiones y la planificación estratégica se vuelve cada vez más importante.

Nuestros datos destacan las principales prioridades para los CIOs en 2024, incluyendo el fortalecimiento de la resiliencia de TI, la comprensión y priorización de los riesgos, y la adopción de tecnologías en la nube y automatización para mejorar las medidas de seguridad. Estas prioridades subrayan la necesidad estratégica de que las organizaciones se adapten a un mundo cada vez más digital e interconectado, mientras se protegen contra nuevas amenazas.

El informe ofrece valiosos conocimientos sobre el panorama de la ciberseguridad para los CIOs en 2024, destacando las prioridades, desafíos y oportunidades que enfrentarán los líderes tecnológicos. Al comprender y abordar estas tendencias, las organizaciones estarán mejor preparadas para navegar las complejidades de la ciberseguridad y posicionarse para el éxito en un entorno digital en constante evolución.

Visión general de la encuesta

Para descubrir más sobre los desafíos actuales de ciberseguridad y Tecnología de la Información que enfrentan los CIOs en organizaciones en América Latina, realizamos una encuesta con CIOs y Líderes Tecnológicos sobre sus experiencias y planes en relación con los principales desafíos y tendencias. Este informe tiene como objetivo presentar una visión general del panorama actual de amenazas, además de explorar tecnologías avanzadas y revelar cómo las organizaciones planean priorizar e invertir.

A través de esta encuesta, buscamos descubrir

La correlación entre el papel de los líderes tecnológicos dentro de una organización, sus patrones de comunicación, principales preocupaciones y la tasa de colaboración.

Cómo los CIOs esperan que su papel y sus prioridades cambien para el área de negocios en general.

Prácticas rutinarias y la adopción de tecnologías avanzadas dentro de las organizaciones.

Metodología

La encuesta contó con la participación de 200 **CIOs y Líderes Tecnológicos.**

Los tres países con mayor número de respuestas fueron **Brasil** (43%), **México** (23%) y **Argentina** (12%). Otros países que también participaron incluyen Chile, Colombia, Perú, Uruguay, Ecuador, Costa Rica y Bolivia.

Las empresas participantes se dividieron en tres principales categorías de tamaño: más de **50 mil empleados** (51%), de **10 mil a 50 mil empleados** (37%) y de **5 mil a 10 mil empleados** (6%).

Las cinco principales industrias representadas en la encuesta fueron **Manufactura** (25%), **Servicios Financieros** (15%), **Utilities y Energía** (10%), **Farmacéutica y Ciencias** (9%) y **Mayorista y Minorista** (6%).

Lo que se descubrió

EL PAPEL DEL CIO Y LA COMUNICACIÓN

Los CIOs creen que, en los próximos cinco años, enfrentarán una creciente presión para convertirse en una parte esencial en la generación de ingresos de la organización (33%), además de una necesidad de convertirse en una función más estratégica dentro de la empresa (33%)

La mayoría de los encuestados indicó que, en los próximos 12 meses, dará prioridad a la seguridad en la nube, a la resiliencia cibernética y a la gestión de riesgos de terceros.

Gobernanza y cumplimiento (18%) y la demostración de ROI (13%) son las principales preocupaciones profesionales para los CIOs en América Latina. Las organizaciones esperan centrarse en estas áreas para asegurar el éxito en 2024.

La mayoría de los encuestados indicó que, en los próximos 12 meses, dará prioridad a la seguridad en la nube, a la resiliencia cibernética y a la gestión de riesgos de terceros

CONTINUADA

LO QUE
SE DESCUBRIÓ CONTINUADA

PRIORIDADES DE NEGOCIOS Y CIBERSEGURIDAD DE LOS CIOS

Las tres principales prioridades de TI para los próximos 12 meses son: enfoque en la nube (21%), mejoras en ciberseguridad (21%) y expansión de la automatización (13%).

Más de un tercio de los encuestados (37%) ya está utilizando Inteligencia Artificial (IA) para simulación de amenazas y predicción de ataques, mientras que el 27% la utiliza para detección y análisis de malware.

El 26% de los encuestados están adoptando IA, mientras que el 22% tiene un entendimiento básico de esta tecnología.

Un cuarto de los encuestados afirmó que el papel más importante de la ciberseguridad es proteger a la empresa y garantizar su continuidad.

paloalto NETWORKS

priorities

A Lynchpin Media BRAND

Parte 1

El papel del CIO y la comunicación

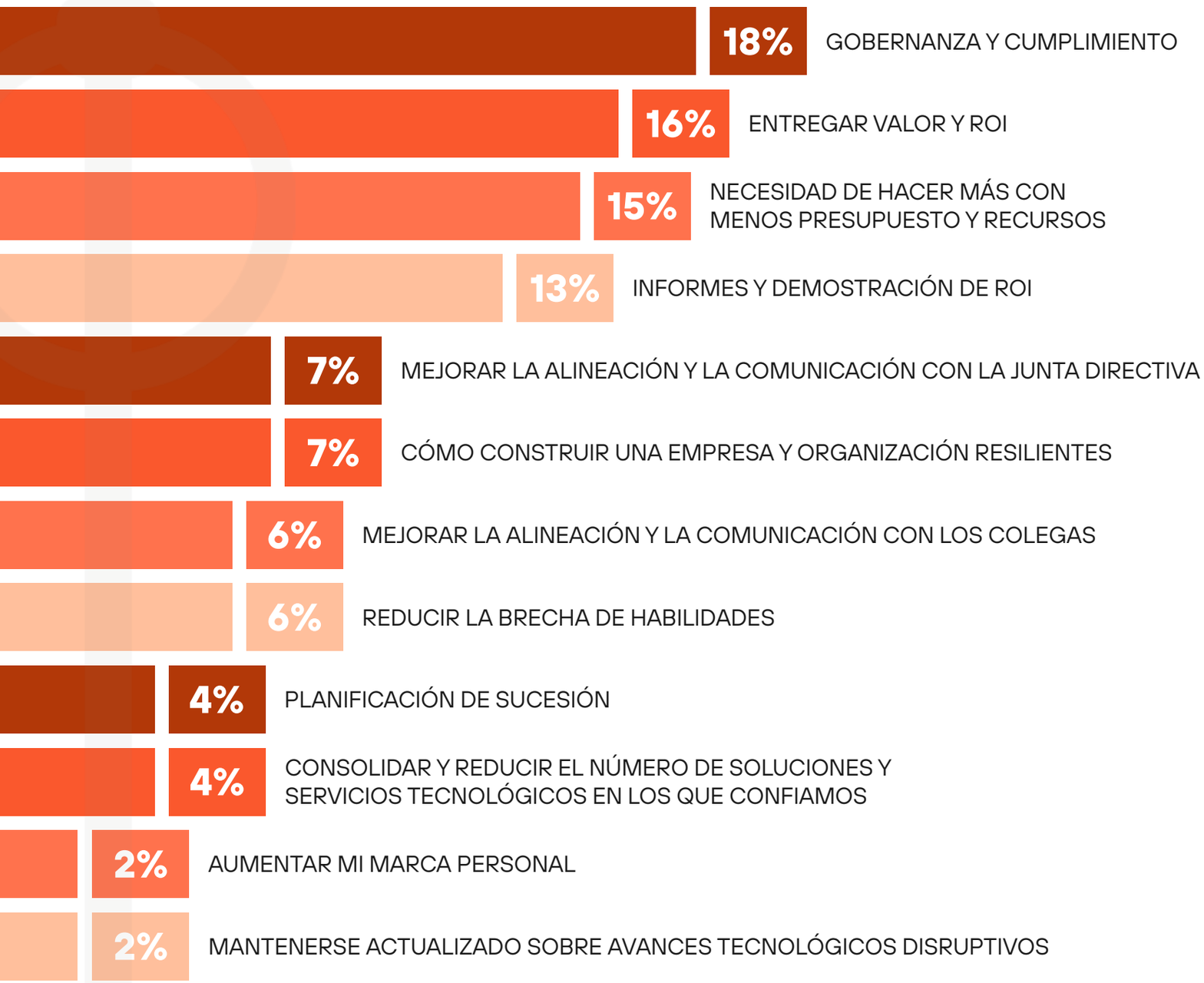
paloalto NETWORKS

priorities

A Lynchpin Media BRAND

1

¿Cuáles son sus principales preocupaciones profesionales en este momento?



Principales insights:

Las preocupaciones de los CIOs están distribuidas en varias áreas, pero gobernanza y cumplimiento recibieron la mayor parte de las respuestas, con un 18%. Luego, entregar valor y ROI (16%) y la necesidad de hacer más con menos presupuesto y recursos (15%) también se destacaron. El enfoque en el ROI refleja la presión que enfrentan los CIOs para garantizar que las inversiones en tecnología demuestren un valor real.

Gobernanza y cumplimiento están en la cima de las prioridades para los líderes tecnológicos, especialmente debido a directrices internacionales como el Digital Operational Resilience Act (DORA, por sus siglas en inglés), el Cyber Resilience Act (CRA, por sus siglas en inglés) y la Directiva NIS2, además de regulaciones locales que requieren atención para evitar posibles penalidades.

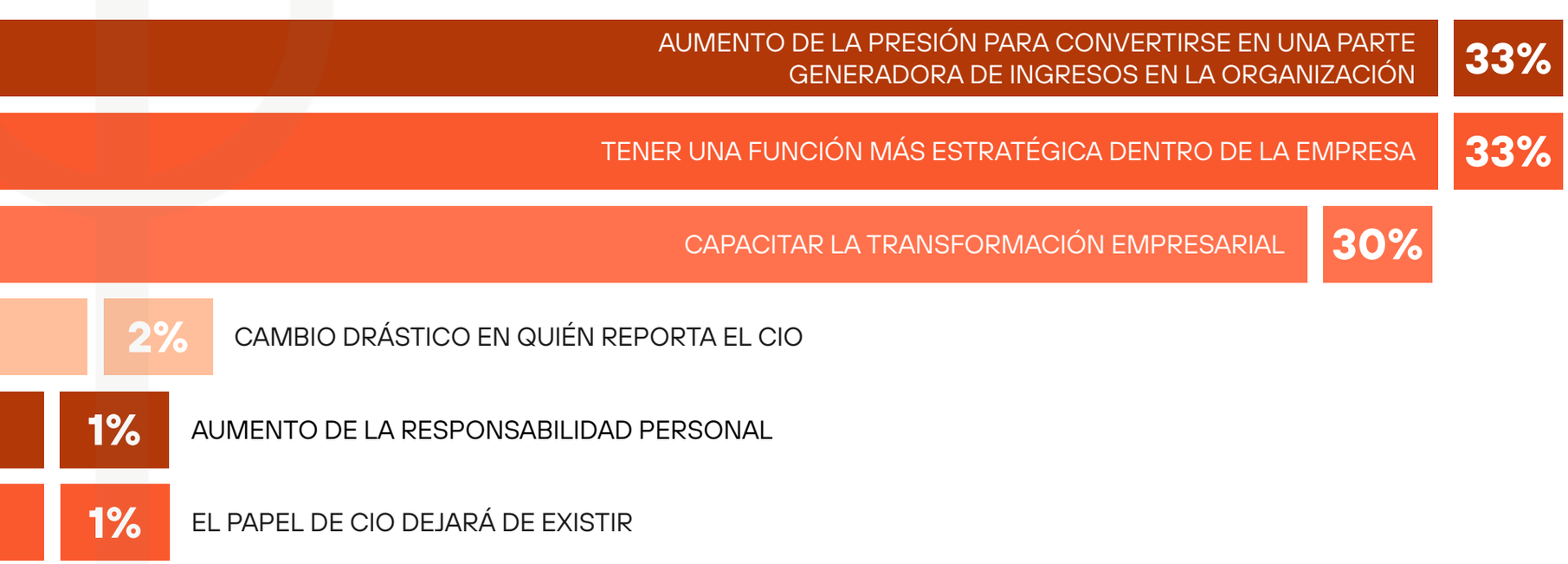
paloalto NETWORKS

priorities

A Lynchpin Media BRAND

2

¿Cómo cree que su papel podría cambiar en los próximos cinco años?



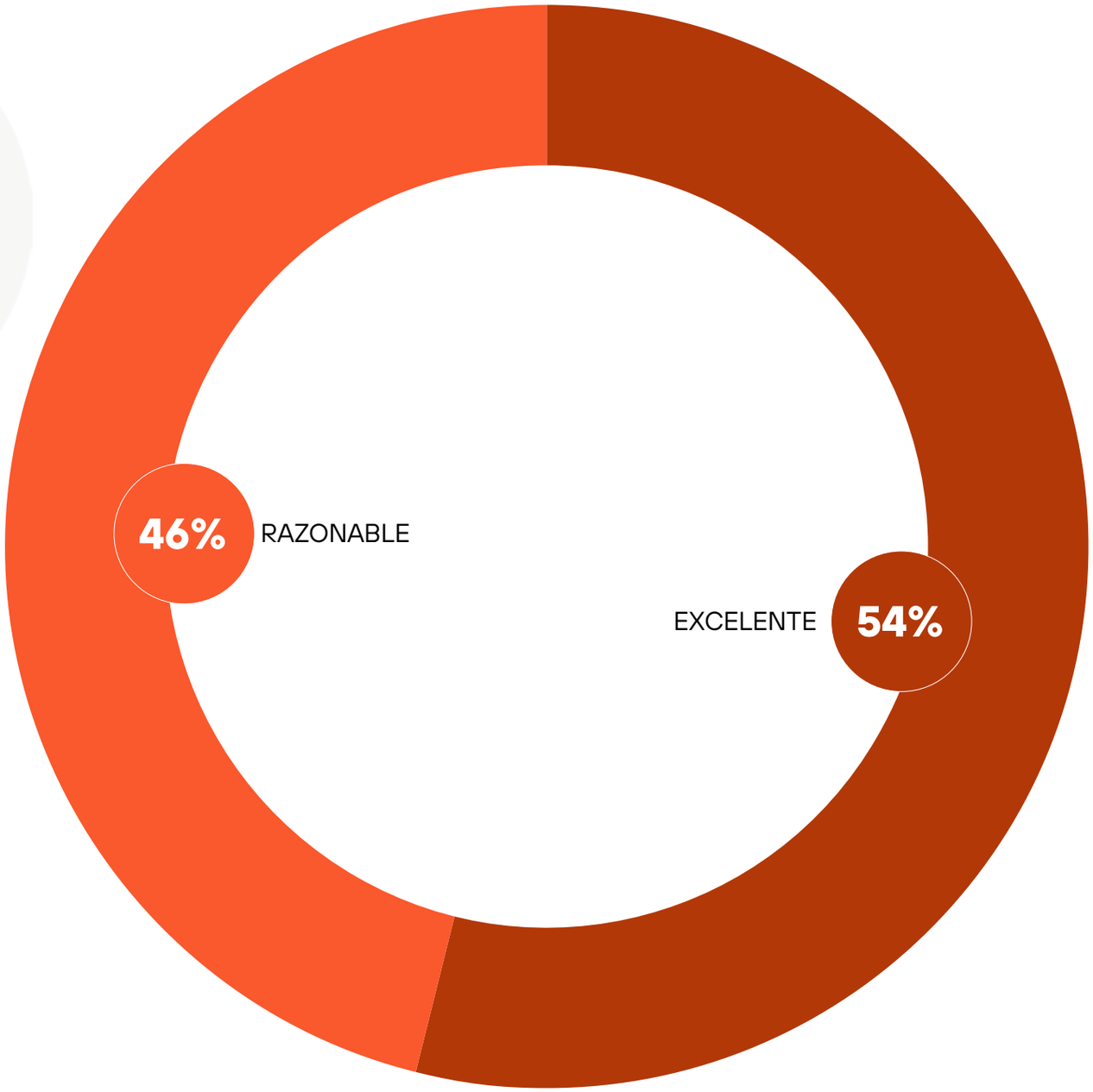
Principales insights:

Los CIOs creen que, en los próximos cinco años, enfrentarán una presión creciente para convertirse en una parte esencial en la generación de ingresos de la organización (33%), además de una necesidad de convertirse en una función más estratégica dentro de la empresa (33%). También esperan ser responsables de impulsar la transformación de los negocios.

A medida que las empresas se enfocan cada vez más en herramientas digitales para aumentar la rentabilidad y mejorar los procesos, los CIOs esperan estar en el centro de las decisiones de inversión en tecnología.

3

¿Cómo evaluaría la colaboración entre su papel y el resto de la alta dirección (C-Suite) en su organización?



SIGUIENTE

paloalto NETWORKS

priorities

A Lynchpin Media BRAND

4

¿Cuáles son algunas maneras de mejorar la colaboración con el resto de la alta dirección?

Aquí están las palabras más mencionadas en las respuestas:

"Aprovechando la tecnología para la eficiencia operativa."

Principales insights:

La comunicación y la colaboración son fundamentales para la cohesión del C-suite, pero no siempre están garantizadas. El éxito en esta área generalmente depende de una buena cultura organizacional. Esto es especialmente importante cuando se trata de ciberseguridad.

Nuestros datos sugieren que esto es ampliamente reconocido, con más de la mitad de los participantes calificando la colaboración entre su función y el resto de la alta dirección como "excelente". Sin embargo, el 46% cree que esta colaboración aún puede mejorar. Algunas sugerencias incluyen:

- Garantizar que las medidas de ciberseguridad apoyen el crecimiento de los negocios y las iniciativas de sostenibilidad;
- Mejorar la comunicación y la alineación para apoyar los esfuerzos de digitalización;
- Aprovechar la tecnología para aumentar la eficiencia operacional;
- Facilitar la colaboración entre diferentes áreas para fortalecer la defensa cibernética y proteger activos críticos;
- Mejorar la comunicación y la coordinación para impulsar la Transformación Digital.

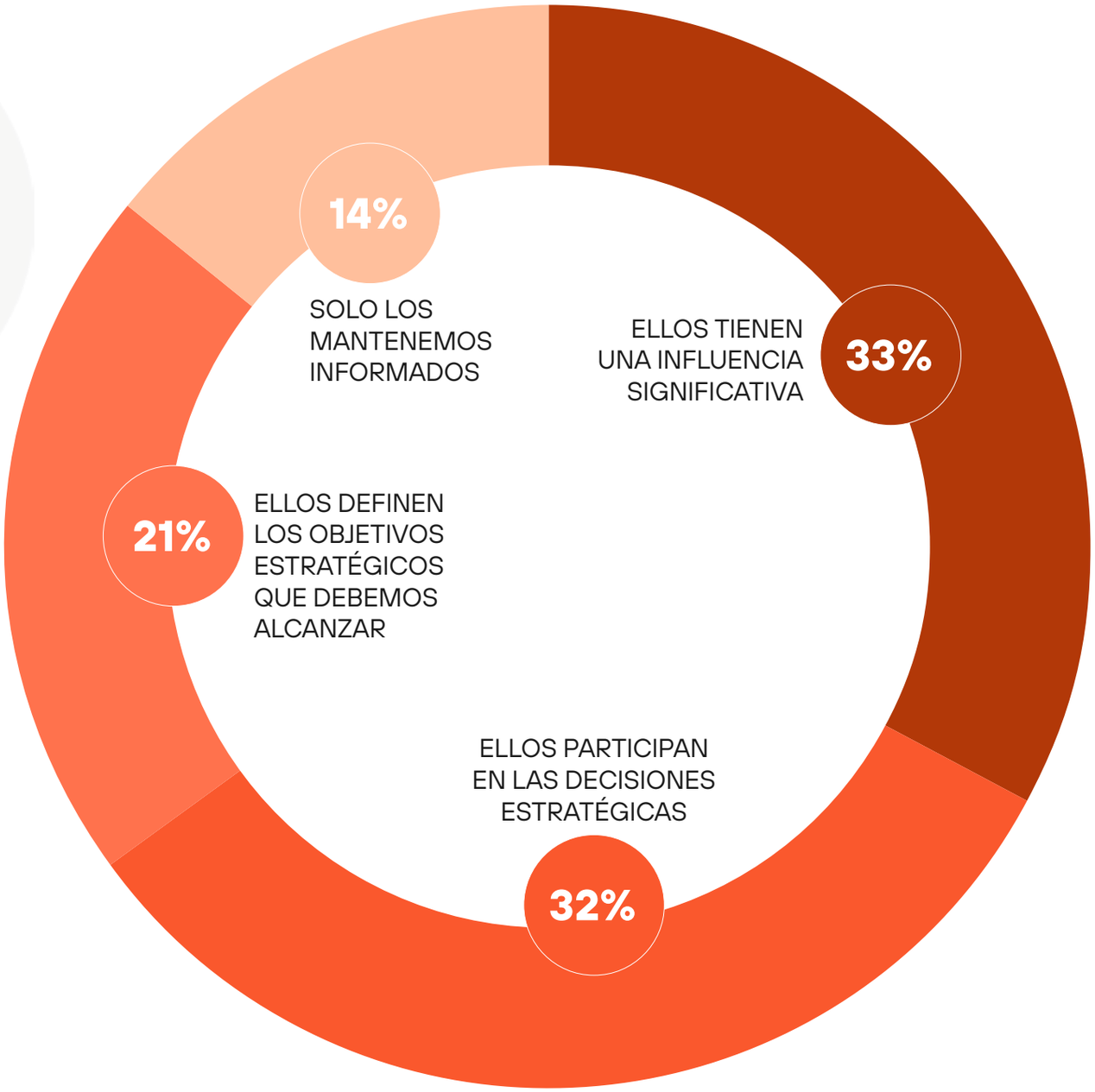
paloalto NETWORKS

priorities

A Lynchpin Media BRAND

5

¿Cuánto influye y dirige la junta directiva la estrategia de ciberseguridad de su organización?



SIGUIENTE

paloalto NETWORKS

priorities

A Lynchpin Media BRAND

6

¿Cuáles son algunos de los desafíos que esto te trae?

Aquí están las palabras más mencionadas en las respuestas:

"Presionado por requisitos de cumplimiento y regulación, necesitando ajustes continuos en las políticas y prácticas de seguridad."

Principales insights:

Los hallazgos revelan que la junta directiva desempeña un papel importante en la definición de las estrategias de ciberseguridad de las organizaciones. Solo el 14% de los participantes informó que la junta directiva tiene un papel pasivo, siendo solo informada sin necesariamente involucrarse en los objetivos estratégicos.

Para el 33% de los participantes, la junta directiva ejerce "influencia significativa".

Para el 32%, la junta está involucrada en las decisiones estratégicas. El 21% restante afirmó que la junta define los objetivos estratégicos. Esto indica que la ciberseguridad se ha convertido en una función esencial del negocio, profundamente integrada en la estructura organizacional. Sin embargo, los encuestados mencionaron algunos desafíos, incluidos:

- Lidiar con la escasez de habilidades y la brecha de especialización, lo que perjudica la implementación eficaz de la estrategia de ciberseguridad;
- Falta de conciencia y capacitación adecuada en ciberseguridad en toda la organización;
- Dificultades con la saturación de alertas y falsos positivos, dificultando la respuesta eficaz a las amenazas;
- Resistencia a la adopción de nuevas tecnologías en industrias tradicionales;
- Recursos limitados y asignación insuficiente de presupuesto para iniciativas de TI;
- Presión de los requisitos de cumplimiento y regulación, exigiendo ajustes continuos en las políticas y prácticas de seguridad.

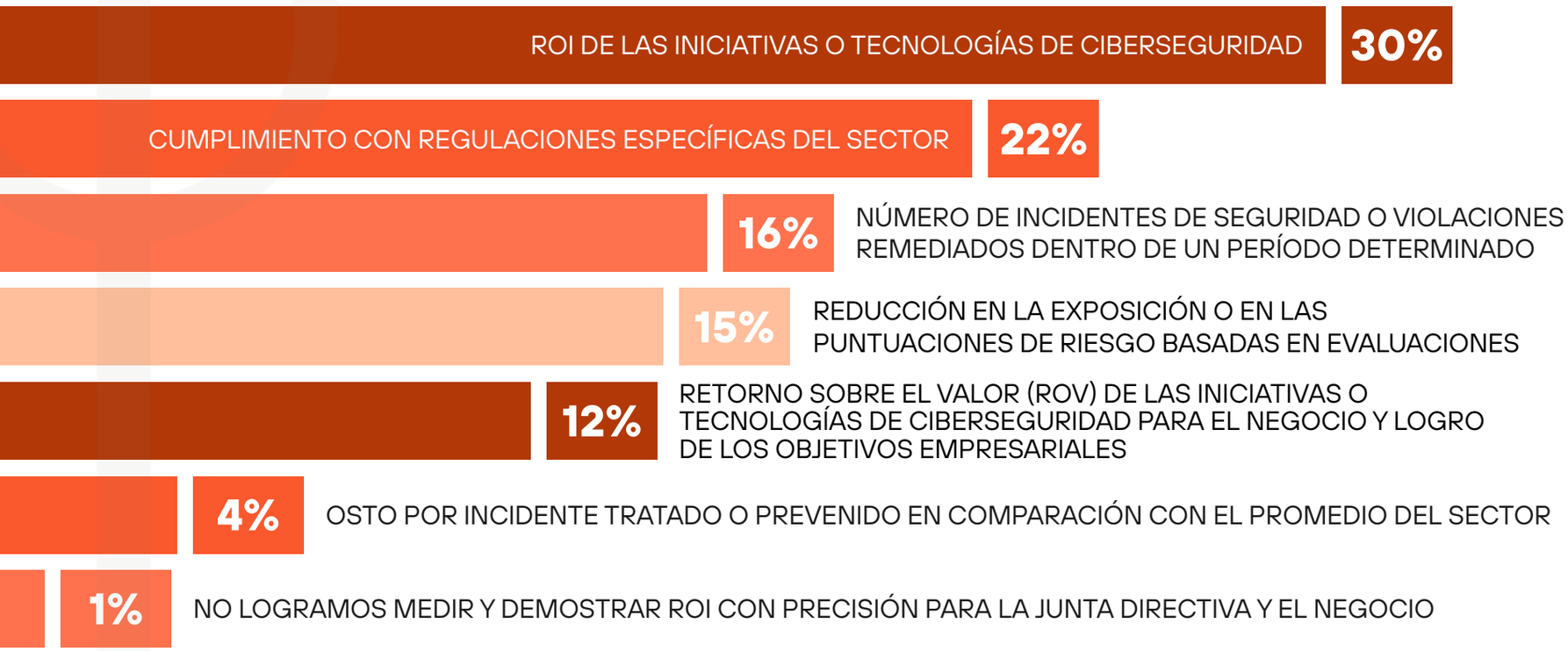
paloalto NETWORKS

priorities

A Lynchpin Media BRAND

7

¿Cuáles son algunas de las métricas de éxito que usas actualmente para evaluar tu postura de seguridad y demostrar valor para el negocio y para la junta directiva?



Principales insights:

Sobre las métricas de éxito utilizadas para evaluar la postura de seguridad y demostrar valor al negocio y a la junta directiva, el 22% de los encuestados utiliza el cumplimiento con regulaciones específicas del sector, lo que indica una fuerte adhesión a las normas regulatorias. Un total del 30% mide el éxito por el ROI de las iniciativas o tecnologías de ciberseguridad, destacando el aspecto financiero de las decisiones de seguridad. La reducción en la exposición o en las puntuaciones de riesgo basadas en evaluaciones es una métrica de éxito para el 15% de los encuestados, lo que evidencia un enfoque proactivo en la gestión de riesgos.

Otras métricas consideradas, aunque en menor escala, incluyen el costo por incidente tratado o prevenido en comparación con el promedio del sector, el número de incidentes de seguridad o violaciones resueltos en un período determinado, y el ROV de las iniciativas o tecnologías de ciberseguridad para el negocio y el cumplimiento de los objetivos empresariales.

paloalto NETWORKS

priorities

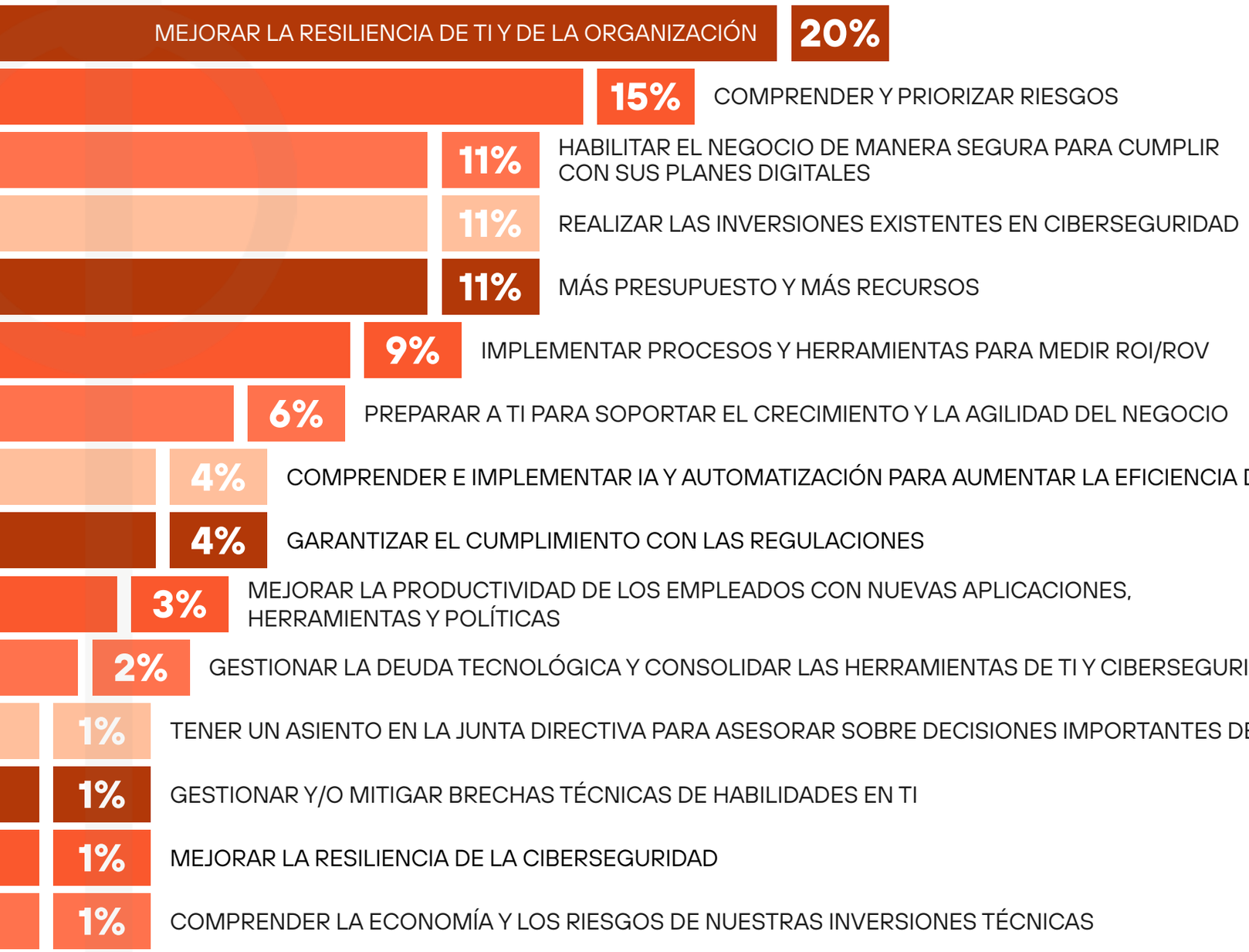
A Lynchpin Media BRAND

Parte 2

Prioridades de negocios del CIO

8

¿Cuáles son las 5 principales cosas que necesitas para garantizar el éxito de tu negocio en 2024?



Principales insights:

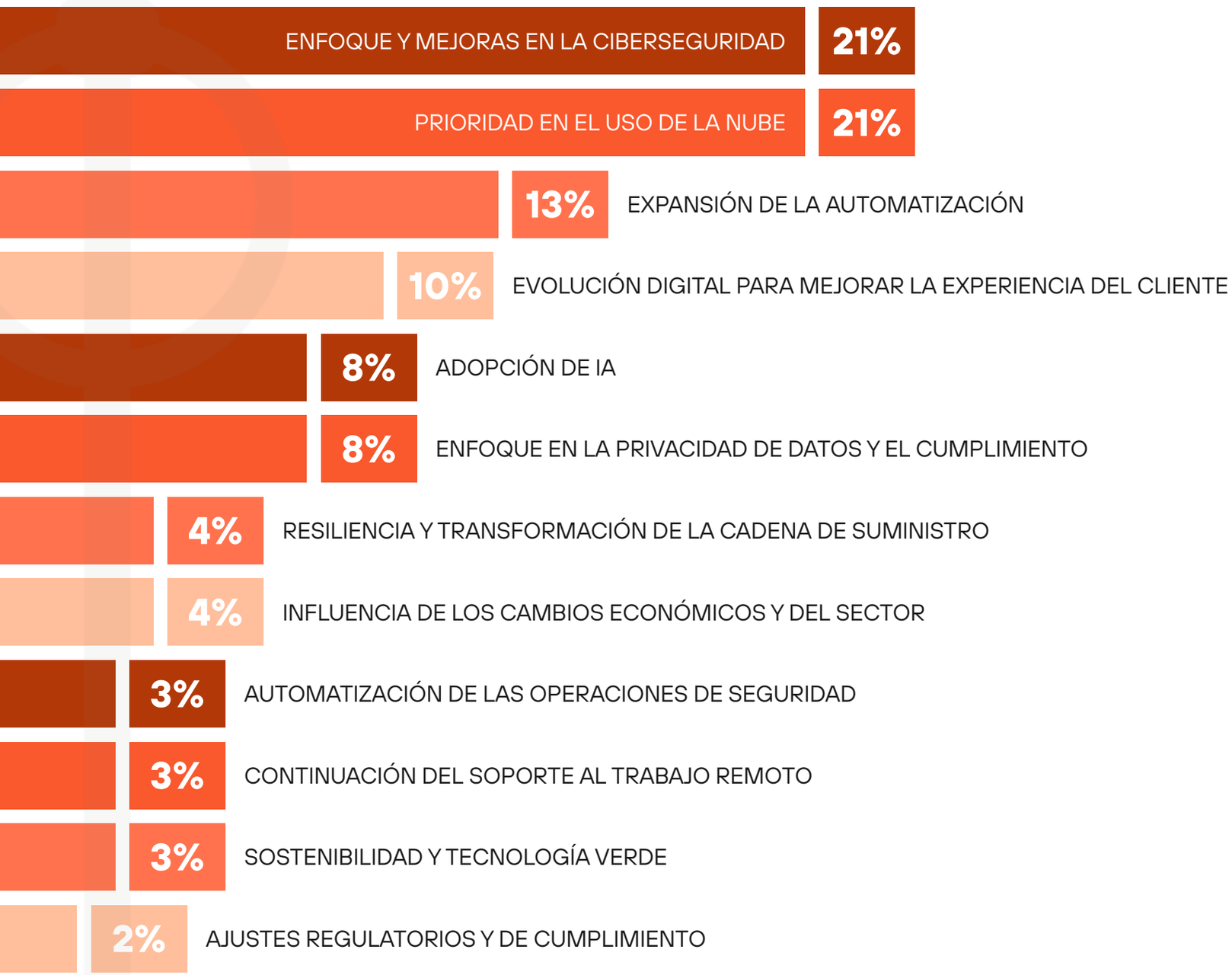
Las cinco principales áreas de enfoque para garantizar el éxito en 2024 son:

- Mejorar la resiliencia de TI y de la organización (20%);
- Comprender y priorizar riesgos (15%);
- Habilitar el negocio de manera segura para cumplir con sus planes digitales (11%);
- Realizar las inversiones existentes en ciberseguridad (11%);
- Más presupuesto y más recursos (11%).

Estas prioridades indican un fuerte énfasis en la resiliencia, la Transformación Digital, la gestión de riesgos, la ciberseguridad y la asignación de recursos como factores críticos para el éxito en 2024.

9

¿Cuáles son las tres principales prioridades de TI de tu organización para los próximos 12 meses?



Principales insights:

Las tres principales prioridades de TI para los próximos 12 meses son: uso de la nube (21%); enfoque y mejoras en la ciberseguridad (21%); y expansión de la automatización (13%). Estas prioridades reflejan un enfoque estratégico en mejorar las medidas de seguridad, aprovechar tecnologías de nube y expandir las iniciativas de automatización para impulsar el crecimiento y la resiliencia del negocio en el escenario tecnológico en constante evolución.

paloalto NETWORKS

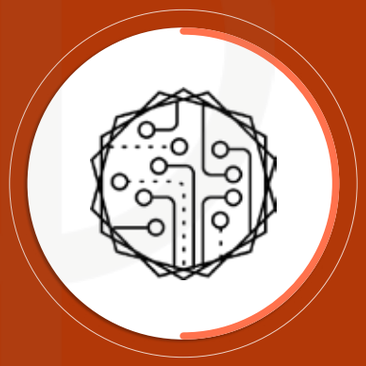
priorities

A Lynchpin Media BRAND

10

¿Qué tendencias tecnológicas cree que tendrán el mayor impacto en sus futuras prioridades empresariales y qué tan preparado está para adoptarlas?

IA



26% de los encuestados están adoptando IA

22% tienen un conocimiento básico de IA

Automatización de Ciberseguridad

17% tienen un conocimiento básico

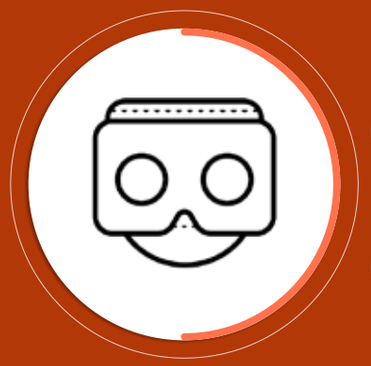
23% necesitan más información

Sustentabilidad

28% tienen un conocimiento básico

26% necesitan más información

Realidad Aumentada y Realidad Virtual

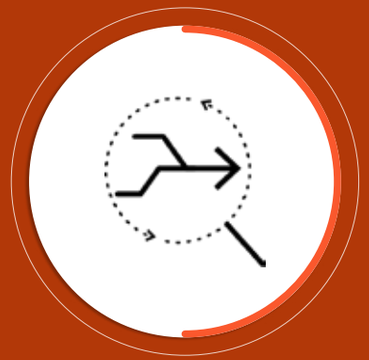


16% están adoptando estas tecnologías

10% tienen un conocimiento básico

SIGUIENTE

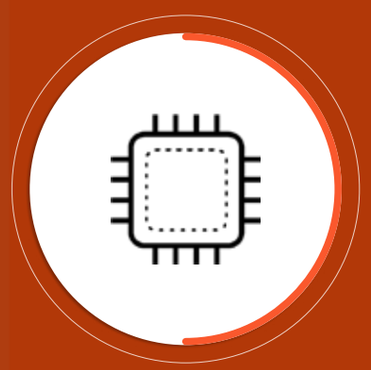
Sistemas Autónomos



25% están adoptando Sistemas Autónomos

23% necesitan más habilidades

Computación Cuántica



12% están adoptando Computación Cuántica

15% necesitan más información

Ofertas basadas en servicios

16% necesitan más información

15% tienen un conocimiento básico

paloalto NETWORKS

priorities

A Lynchpin Media BRAND

Parte 3

Prioridades de Ciberseguridad del CIO

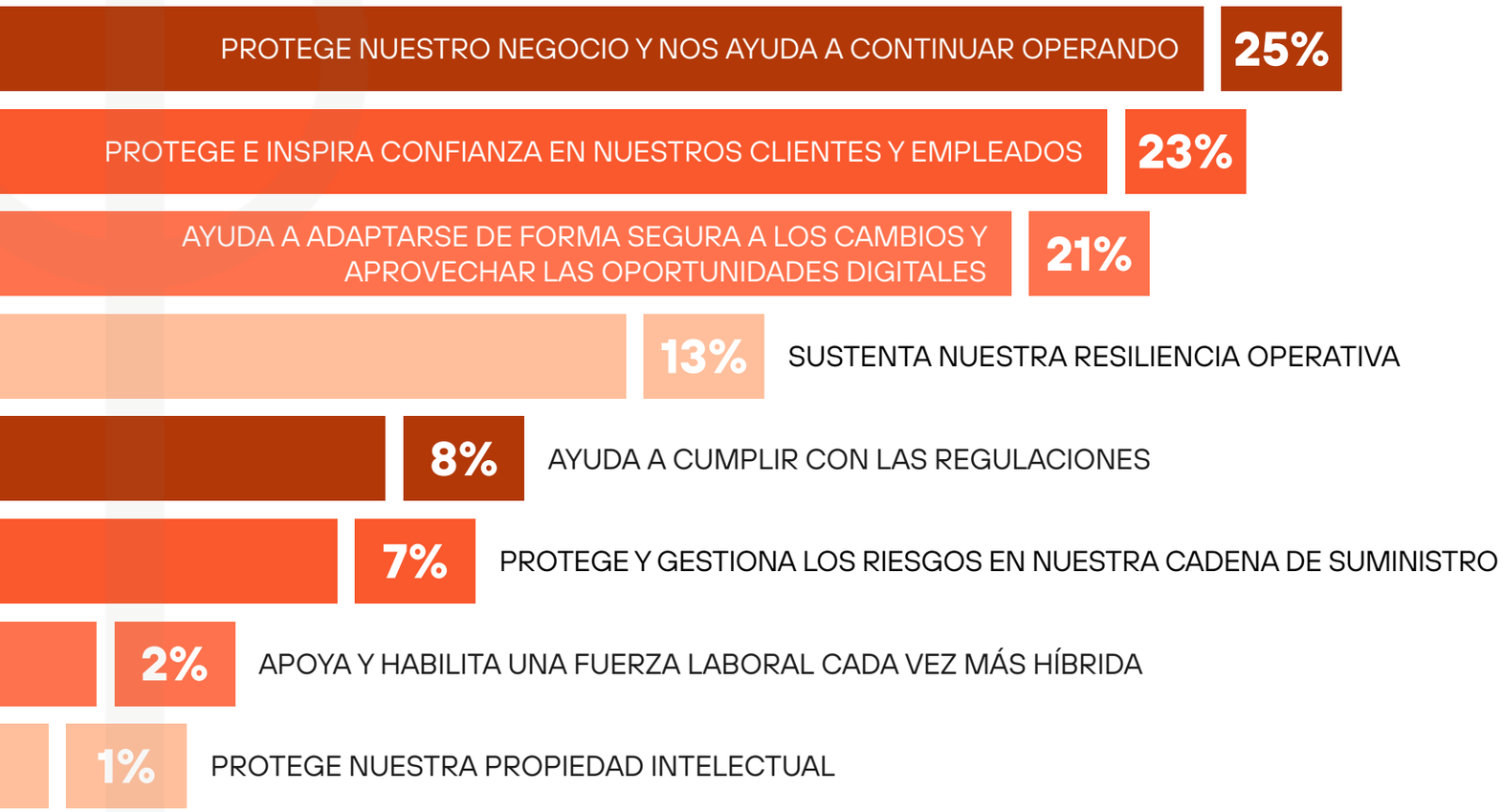
paloalto NETWORKS

priorities

A Lynchpin Media BRAND

11

¿Cuál es el papel más importante que desempeña la ciberseguridad para el éxito de su organización?



Principales insights:

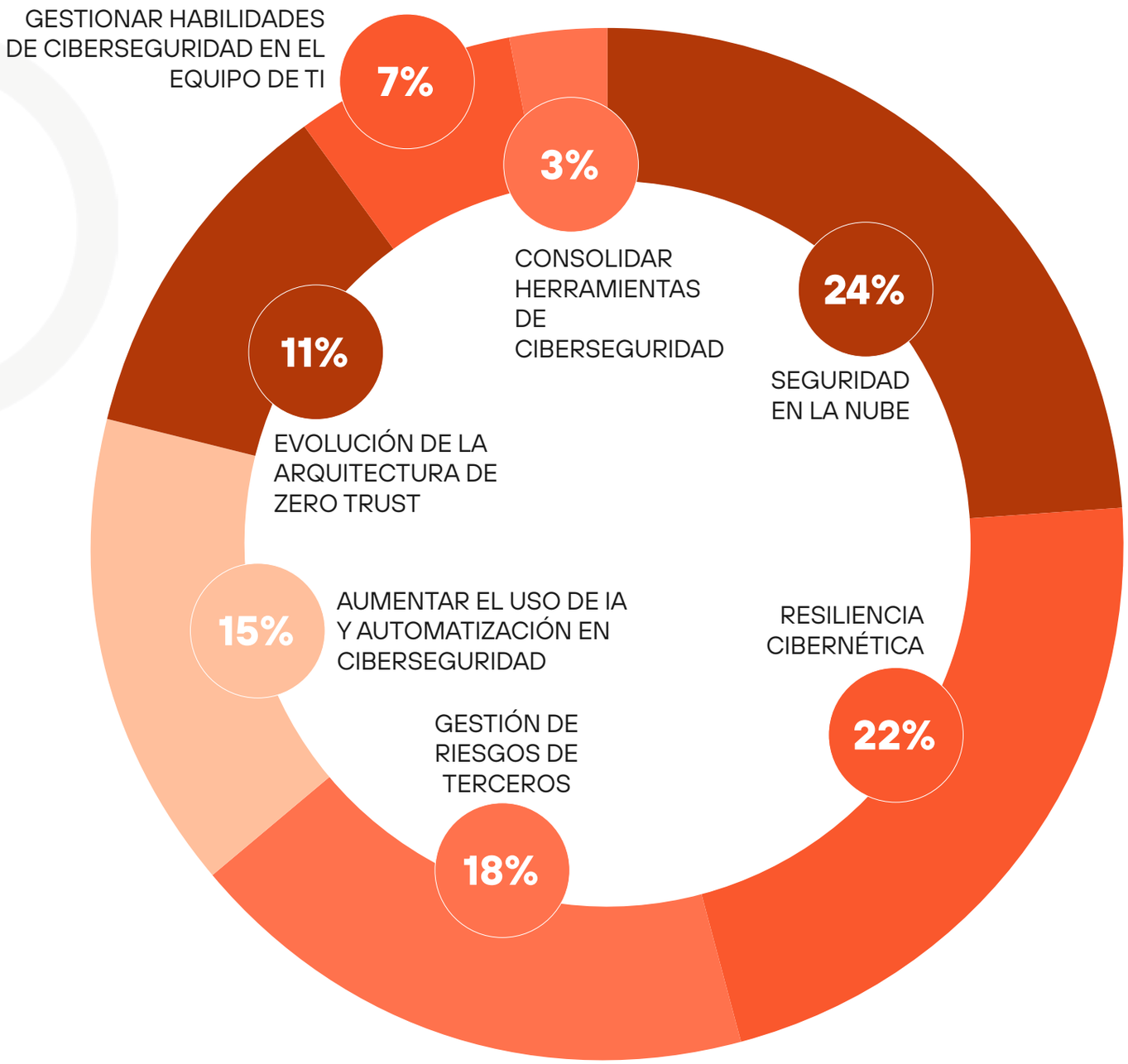
Una cuarta parte de los encuestados destacó que el papel más importante de la ciberseguridad es proteger el negocio y garantizar su continuidad. Esto refleja la comprensión de que una ciberseguridad robusta es crucial para el éxito empresarial, no solo para los CISOs, sino para toda la alta dirección.

"Proteger e inspirar confianza en clientes y empleados" fue la elección de 23% de los encuestados, lo que evidencia la responsabilidad que se le atribuye a la ciberseguridad en este aspecto. Además, 21% creen que la ciberseguridad ayuda a las organizaciones a adaptarse de manera segura a los cambios y a aprovechar oportunidades digitales.

El mensaje principal aquí es que, sin una postura de ciberseguridad resiliente y firme, la confianza de los clientes se verá afectada, y las organizaciones tendrán poca o ninguna oportunidad de invertir y aprovechar las oportunidades digitales, además de correr el riesgo de salir del mercado.

12

¿Cuáles son sus tres principales prioridades de ciberseguridad para los próximos 12 meses?



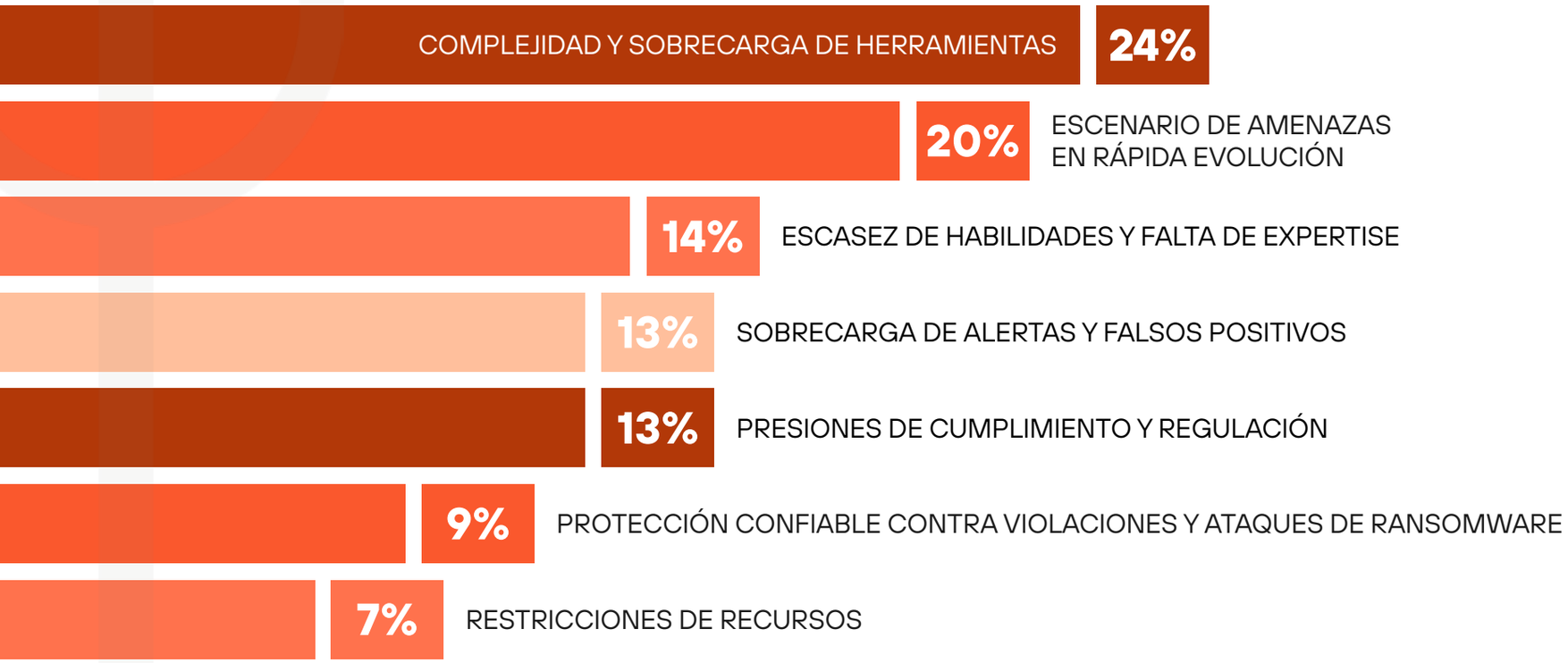
Principales insights:

La mayoría de los encuestados planea priorizar la seguridad en la nube, la resiliencia cibernética y la gestión de riesgos de terceros en los próximos 12 meses. Solo 7% dijeron que priorizarán la gestión de habilidades de ciberseguridad dentro del equipo de TI, lo que sugiere un mayor enfoque en el negocio en sí que en las personas.

Esto puede generar un debate interesante, considerando que las habilidades y la educación en ciberseguridad son fundamentales para el funcionamiento de una organización, siendo crucial que esta área de inversión no se descuide mientras se abordan otras prioridades.

13

¿Cuáles son los desafíos más comunes que enfrenta en la gestión de sus herramientas y soluciones de ciberseguridad?

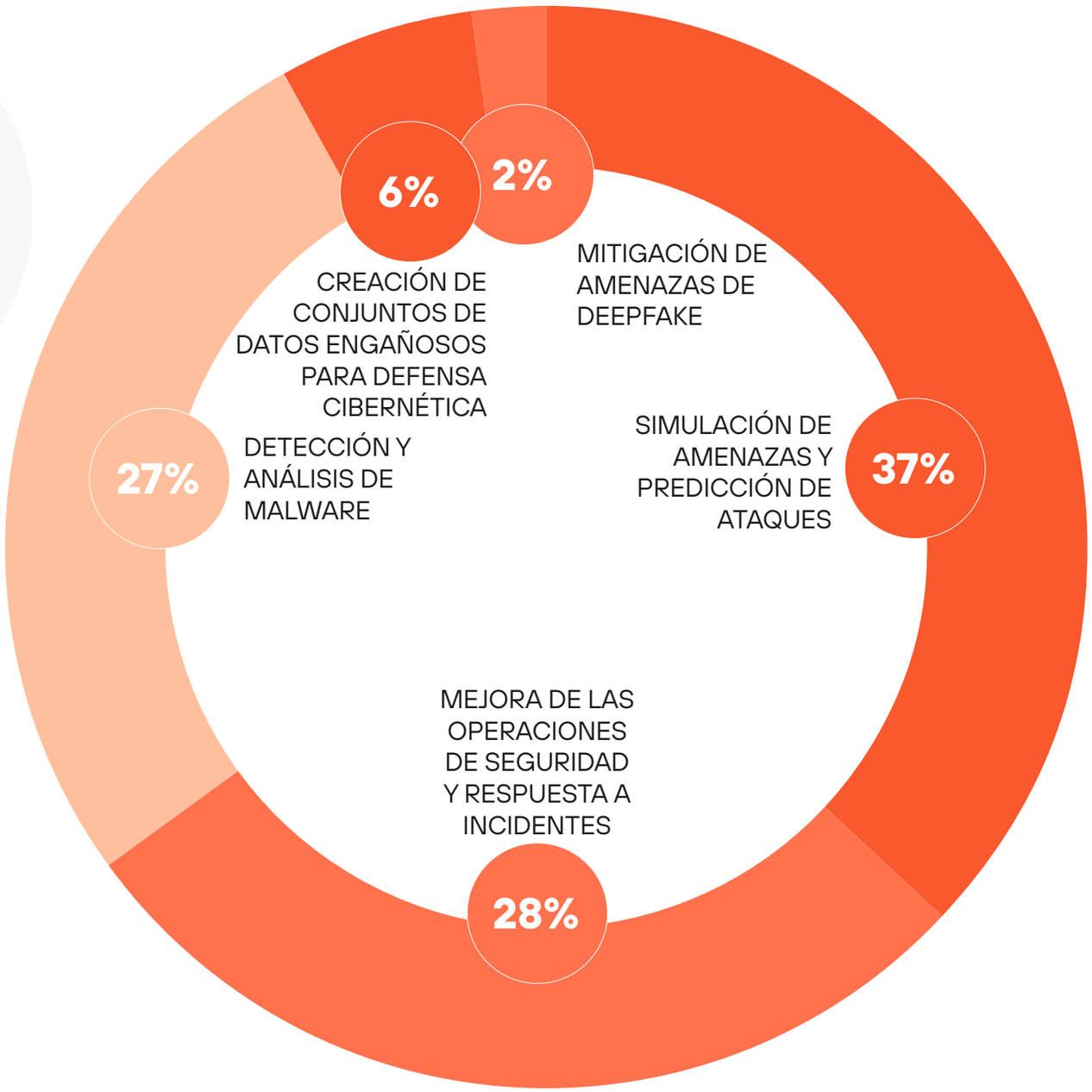


Principales insights:

Además de los desafíos esperados en ciberseguridad, como el escenario de amenazas en rápida evolución (20%), la cuestión de las restricciones de recursos (7%) fue menos mencionada por los encuestados en comparación con los desafíos relacionados con herramientas y soluciones. Esto puede sugerir que las organizaciones están invirtiendo más ampliamente en recursos como IA y automatización para gestionar estos desafíos.

14

¿Está utilizando IA y automatización en alguna de las siguientes aplicaciones para enfrentar la brecha de habilidades en ciberseguridad?



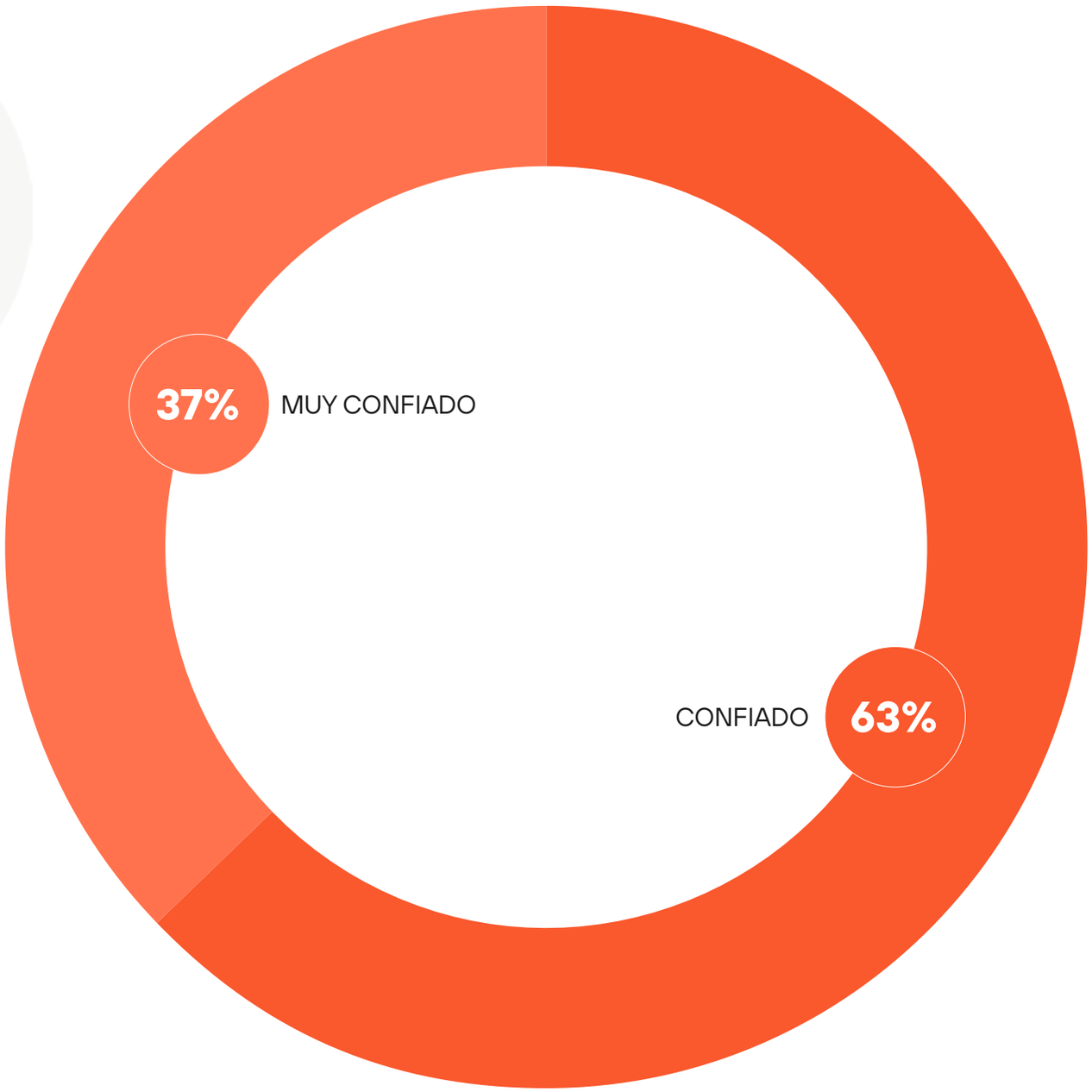
Principales insights:

La IA y la automatización están dominando el panorama tecnológico, y las organizaciones están ansiosas por identificar cómo usar estas herramientas para mejorar y simplificar procesos. Aunque los agentes malintencionados también están utilizando IA para organizar ataques rápidos, hay muchos casos en los que la automatización está fortaleciendo las defensas, especialmente en un sector conocido por la escasez de habilidades.

De hecho, más de un tercio (37%) de los encuestados están usando IA para simulación de amenazas y predicción de ataques, mientras que 27% la utilizan para detección y análisis de malware. Estos resultados muestran cómo muchas organizaciones están utilizando IA y automatización en todo el panorama de la ciberseguridad, destacando el impacto positivo de esta tecnología.

15

En caso de un ataque cibernético, ¿qué tan confiado está en la capacidad de su organización para responder y mantener las operaciones comerciales mientras protege los datos críticos?



Principales insights:

Los datos a menudo se llaman “el corazón palpitante” de una organización, lo que demuestra su importancia y la necesidad de protegerlos. Los encuestados se mostraron “confiados” (63%) o “muy confiados” (37%) en sus habilidades para responder a ataques cibernéticos y mantener las operaciones comerciales mientras protegen datos críticos, reforzando la convicción de que las organizaciones están priorizando la protección de estos datos como parte de su estrategia. Estos resultados reflejan las capacidades empresariales en el escenario actual y ayudan a generar confianza en los clientes.

Conclusión

A medida que los CIOs se preparan para asumir un papel más estratégico en los próximos cinco años, su enfoque se centra cada vez más en impulsar la transformación de los negocios mediante la adopción de tecnologías avanzadas. La ciberseguridad sigue siendo una preocupación central, con la IA desempeñando un papel crucial en la simulación de amenazas, la detección de malware y la automatización de las operaciones de seguridad. El cumplimiento de regulaciones como DORA, CRA y NIS2 exige ajustes continuos en las políticas, especialmente en la cadena de suministro.

El aumento del trabajo remoto y la expansión de los dispositivos IoT (Internet of Things, en inglés) han hecho de la ciberseguridad una prioridad para el próximo año. Casi la mitad de los entrevistados está fortaleciendo sus operaciones de seguridad con IA y automatización para enfrentar la escasez de habilidades, lo que ayuda a inspirar confianza entre los empleados y proteger funciones críticas.

El informe enfatiza la importancia de una cultura de concienciación y capacitación en ciberseguridad, destacando que la adopción de IA para automatización y resiliencia cibernética se está volviendo cada vez más común. Tendencias como el enfoque “Cloud First”, la prioridad en ciberseguridad y la expansión de la automatización están moldeando el futuro.

Los CIOs deben garantizar que las inversiones en tecnología generen un ROI medible, aprovechando herramientas digitales para aumentar la rentabilidad y simplificar procesos. La colaboración entre los ejecutivos de la alta dirección y entre diferentes funciones es fundamental para fortalecer las defensas cibernéticas y alinear los objetivos estratégicos. En resumen, el informe destaca la necesidad de estrategias adaptativas para enfrentar los desafíos futuros.

CxO Priorities, a Lynchpin Media brand
63/66 Hatton Garden
London, EC1N 8LE

www.cxopriorities.com

Patrocinado por:

3000 Tannery Way
Santa Clara, CA 95054
info@paloaltonetworks.com

www.paloaltonetworks.com