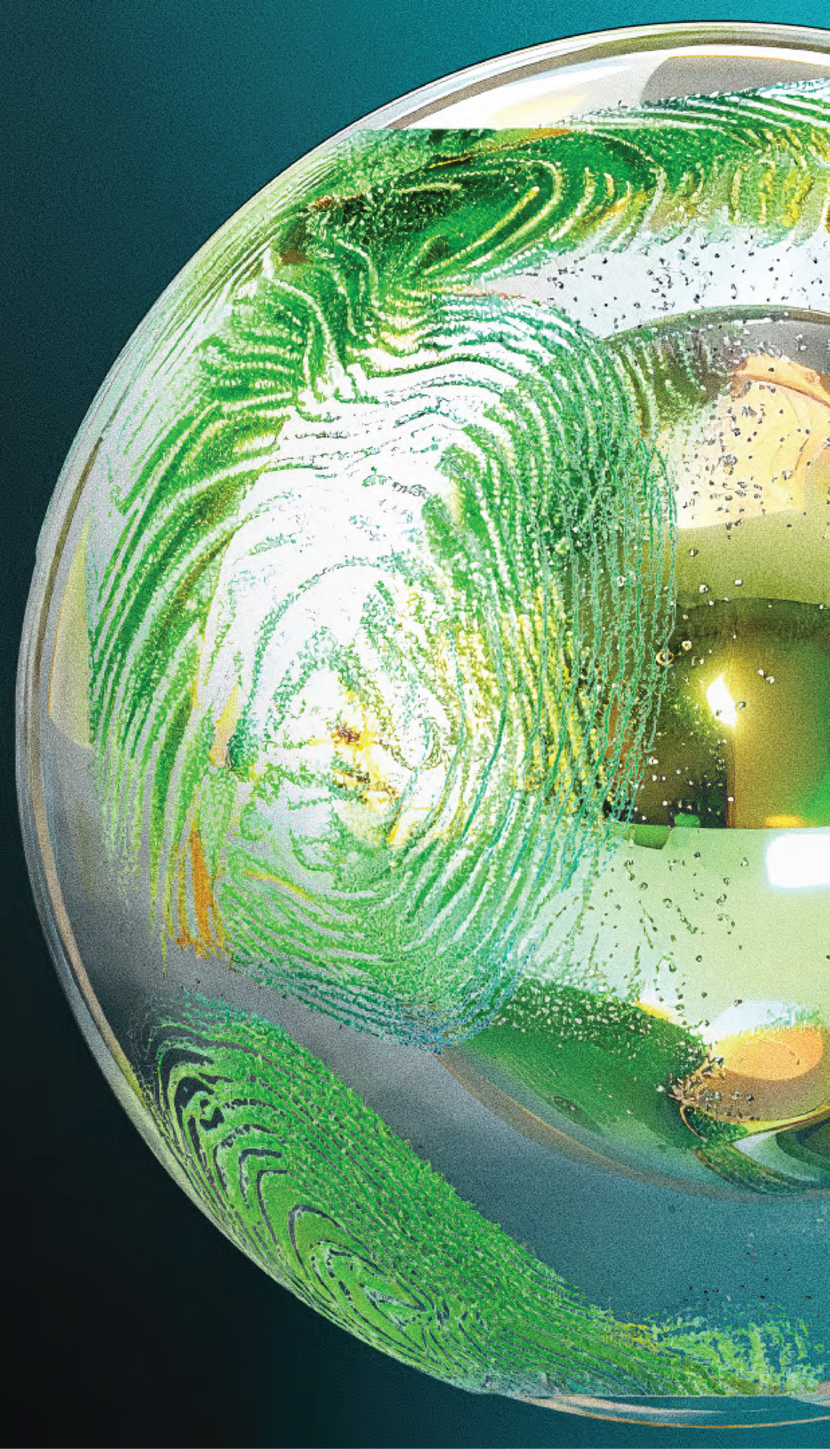
Deloitte.

Together makes progress

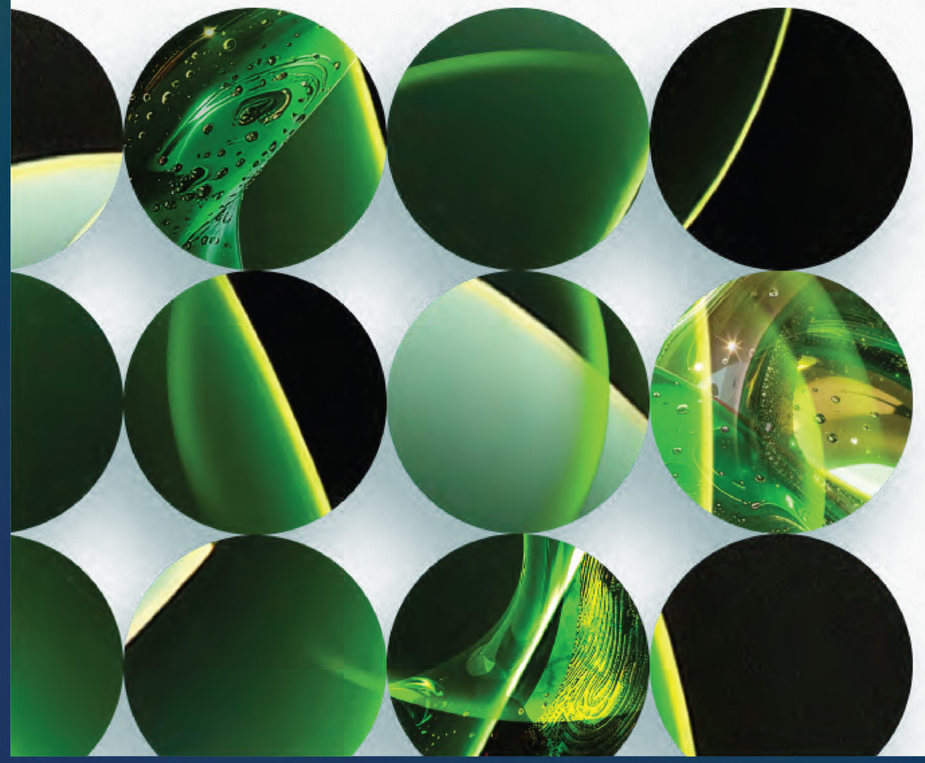
5.ª EDICIÓN DE LA ENCUESTA GLOBAL SOBRE EL FUTURO DE LA CIBERSEGURIDAD

CINCO PARADOJAS QUE DAN FORMA AL FUTURO DE LA CIBERSEGURIDAD

Contradicciones en el núcleo de las estrategias de ciberseguridad actuales y cómo los líderes navegan en la ciberseguridad.



Paradojas y Progreso



A lo largo de los años en que se realiza esta encuesta, hemos documentado el progreso constante de las capacidades de ciberseguridad en condiciones cada vez más desafiantes. El panorama de amenazas ha evolucionado considerablemente durante este tiempo. Sin embargo, los encuestados han respondido con firmeza, respaldado por el apoyo ejecutivo y la asignación de recursos, para defenderse con éxito frente al creciente volumen de riesgos cibernéticos.

Nos entusiasma analizar en profundidad los datos de la encuesta de este año para conocer lo que más de 1,000 líderes globales de ciberseguridad y de negocio tienen que decir sobre el entorno actual y sobre lo que viene. ¿Qué descubrimos? Una serie de paradojas fundamentales: datos que, a primera vista, parecen contradecirse entre sí, pero que, tras un examen más detallado, pueden ofrecer perspectivas más amplias y valiosas sobre los desafíos a los que se enfrentan los responsables de las decisiones en materia de ciberseguridad y cómo están respondiendo a un mercado complejo y en constante cambio.

Quizá no debería sorprendernos encontrar paradojas y contradicciones en el núcleo de una encuesta centrada en ciberseguridad realizada a finales de 2025. Los últimos años han estado marcados por un nivel significativo de cambio “no solo en el panorama de amenazas, sino también en las herramientas y tecnologías utilizadas por ambos lados del espectro cibernético”, por lo que las desconexiones entre estrategia y ejecución quizá hayan sido inevitables.

Independientemente de las razones que explican su aparición, estas paradojas merecen la atención cuidadosa de cualquiera que tenga cierta responsabilidad en la estrategia de ciberseguridad de su organización, ya que podrían revelar debilidades o brechas que deban resolverse con rapidez.

En las siguientes páginas encontrará una combinación de perspectivas basadas en datos proporcionados directamente por los encuestados, junto con observaciones prospectivas de Deloitte basadas en entrevistas de mercado y en nuestra amplia experiencia global en ciberseguridad.

Esperamos que estas perspectivas le ayuden a navegar su propio camino en materia de ciberseguridad. Que disfrute la lectura.

Emily Mossburg
Líder Global de Ciberseguridad en Deloitte.

Qué distingue a los *Frontrunners* en Ciberseguridad

Al analizar cómo evoluciona el mercado de ciberseguridad y cómo las organizaciones se preparan para el futuro, siempre nos ha interesado particularmente identificar las características que distinguen a los líderes. El índice de madurez en ciberseguridad de Deloitte, de propiedad exclusiva, es un elemento distintivo en ediciones anteriores de este informe, utiliza datos de la encuesta para destacar a las organizaciones que han ejecutado con éxito un conjunto definido de acciones centradas en la ciberseguridad. Sus perspectivas, comportamientos y prácticas pueden resultar instructivos para aquellas organizaciones que buscan avanzar en sus capacidades de ciberseguridad de manera rápida y eficaz, así evitan las dificultades y callejones sin salida que otros ya han tenido que enfrentar.

Anteriormente, definíamos a los líderes como aquellos que habían integrado el mayor número de elementos clave de programas de ciberseguridad para reducir el riesgo en sus organizaciones y que mantenían un enfoque constante en la inteligencia artificial (IA). Hoy, son requisitos básicos para cualquier organización que se tome en serio la ciberseguridad. Por ello, al reflexionar sobre lo que se necesita para ser un líder en un mercado donde el estándar mínimo se ha elevado, recurrimos a los datos para establecer un nuevo marco basado en lo que hemos descubierto.

La encuesta más reciente revela una brecha entre la confianza de los encuestados en sus capacidades de ciberseguridad y su nivel de preparación para los desafíos cibernéticos futuros “la primera paradoja analizada en este informe”. En respuesta, hemos evolucionado el Índice de Madurez en Ciberseguridad de Deloitte, nuestra clasificación y segmentación del nivel de madurez de los encuestados según su adopción de prácticas líderes. El índice actualizado nos permite examinar y comprender las acciones que toman los encuestados para cerrar con éxito esa brecha, centrándonos en aquellos con los niveles más altos de confianza y preparación en materia de ciberseguridad.

Este informe identifica tres grupos según sus niveles de confianza y preparación. El grupo de *Frontrunners* obtuvo las puntuaciones más altas en preguntas relacionadas tanto con la confianza como con la preparación en ciberseguridad. Aquellos con puntuaciones inferiores se ubican de forma incremental en los grupos de *Followers y Foundation Builders.*[1]

FRONTRUNNERS	FOLLOWERS	FOUNDATION BUILDERS
17%	60%	24%

Para obtener detalles adicionales sobre la metodología utilizada para categorizar a los encuestados de la encuesta, consulte la sección de Metodología al final de este informe.

Cinco paradojas

Los *Frontrunners* lograron avances significativos en el fortalecimiento de relaciones clave y en la integración de estrategias de ciberseguridad en los niveles más altos de sus organizaciones. Sin embargo, las cinco paradojas identificadas aquí revelan fuerzas opuestas que podrían obstaculizar la preparación cibernética, la ejecución, las estrategias de plataformas, el impacto y la estabilidad, tanto ahora como en el futuro.

Nota [1]: los porcentajes pueden no sumar exactamente 100% debido a ajustes por redondeo, dicha discrepancia es esperada y no representa un error.

PARADOJA #1

La confianza en ciberseguridad es alta. ¿Están las organizaciones preparadas?

PARADOJA #1

Avances clave de los líderes en ciberseguridad para fortalecer la confianza

Nuestro informe anterior reveló una madurez creciente en las capacidades y los enfoques de ciberseguridad. En su mayoría, los encuestados informaron que el cargo de *Chief Information Security Officer* (CISO) estaba plenamente incorporado y en proceso de maduración, las estrategias de ciberseguridad se integran en diversas áreas de la organización, en el C-*suite* existía una comprensión cada vez mayor del papel que puede desempeñar la estrategia de ciberseguridad en la generación de valor real para el negocio y que los encuestados incrementan su enfoque en impulsar resultados positivos para la empresa.

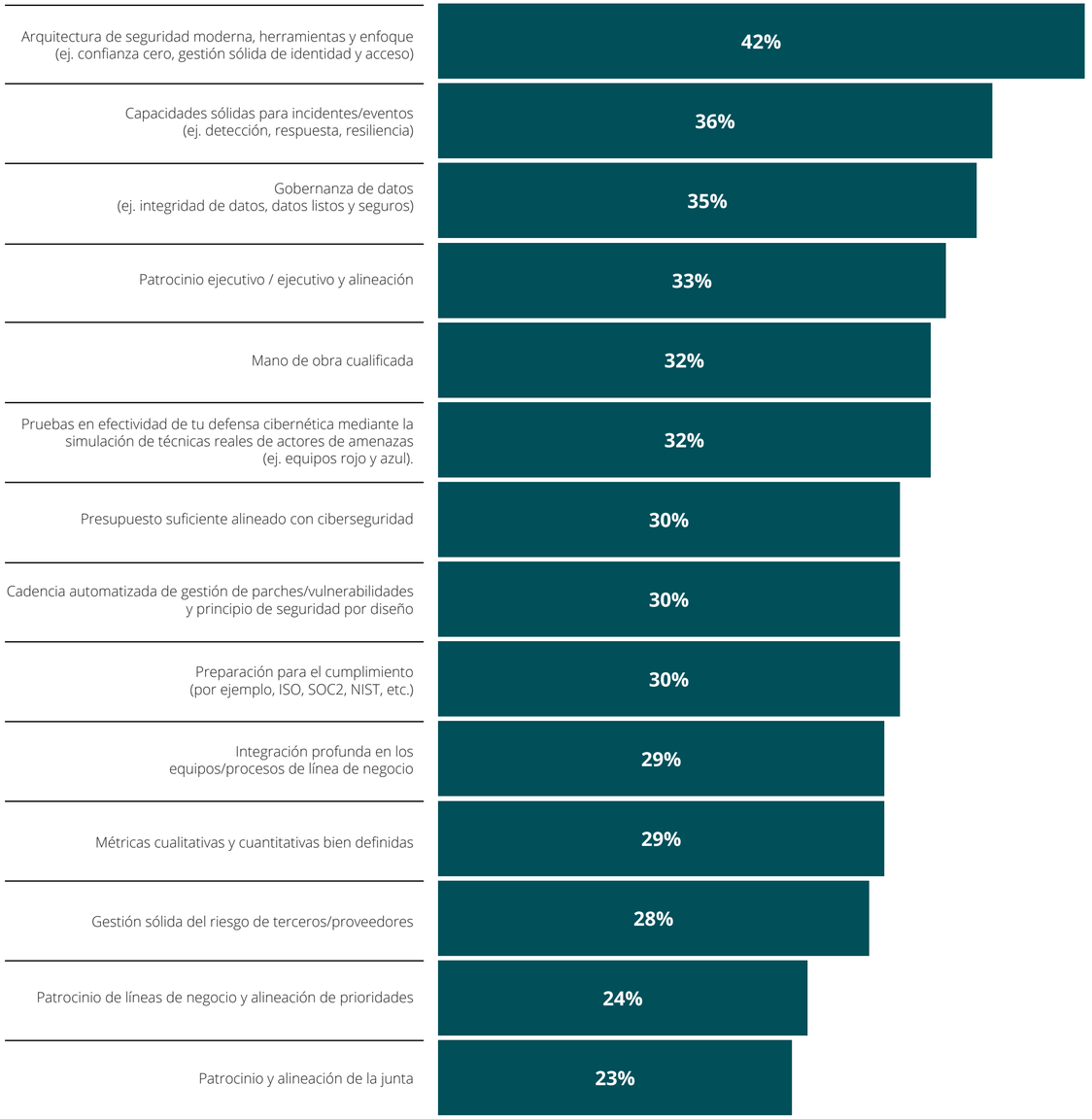
En esta edición de la encuesta, la mayoría de los encuestados (85 %) afirma sentirse algo o muy confiado en la estrategia de ciberseguridad de sus organizaciones, citan arquitecturas de seguridad modernas, sólidas capacidades de respuesta a incidentes, gobierno de datos y otros factores que se muestran en la figura de la derecha.

Asimismo, señalan contar con un sólido respaldo de la alta dirección (C-*suite*) y con acceso oportuno a los presupuestos que necesitan para mantenerse un paso adelante. Este apoyo se evidencia cada vez más en la integración de la ciberseguridad en el ciclo del negocio: un 54 % combinado de los encuestados indica que ya ha integrado plenamente la ciberseguridad en sus planes estratégicos generales de negocio y tecnología, o que incorporan activamente requisitos de ciberseguridad en su estrategia a futuro.

Existen múltiples razones por las que los encuestados se han ganado esa confianza. Pero ¿algunos confían más de lo que deberían?

Factores clave que aportan a la confianza en ciberseguridad de la organización

P: ¿Cuál de los siguientes factores contribuye más a la confianza de su organización en ciberseguridad hoy?



Total (n=1,058)

PARADOJA #1

Preocupación persistente por la preparación ante futuras amenazas

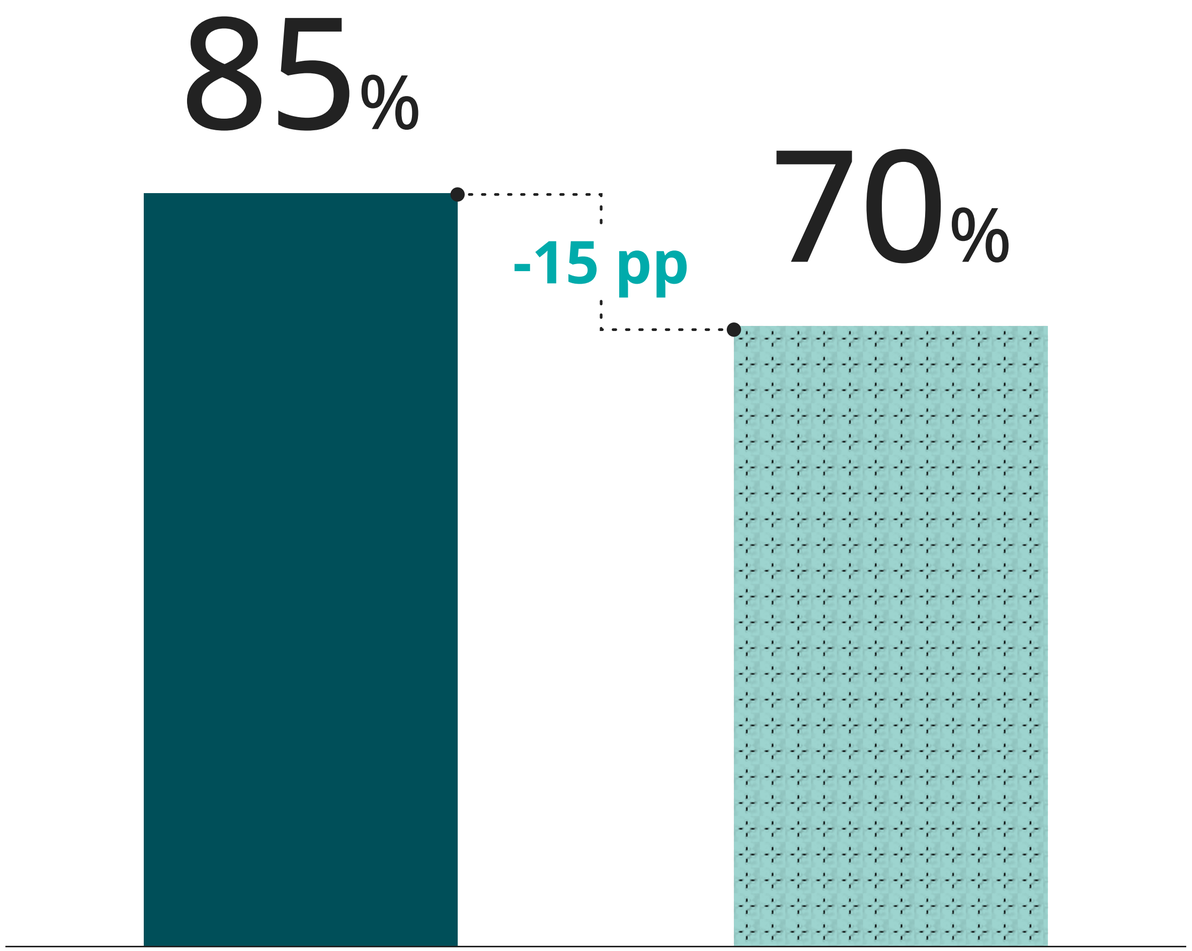
Para determinar el nivel de preparación en ciberseguridad de los encuestados, se les presentó una lista de acciones relacionadas a ciberseguridad y se les preguntó en qué medida dichas acciones se habían implementado en sus organizaciones.

En promedio, el 70 % de los encuestados ha implementado todas aquellas en gran medida o en muy gran medida, lo que indica un alto nivel de preparación. Al comparar este resultado con los datos de la encuesta que miden su confianza en tener estrategias de ciberseguridad en vigor, se revela una brecha notable: en promedio, los encuestados reportan 15 puntos porcentuales más de confianza en ciberseguridad que de preparación efectiva.

"Recibimos el nivel adecuado de inversión, contamos con el involucramiento del liderazgo que necesitamos, tenemos las herramientas y los procesos correctos", afirma un CISO de una empresa del sector salud. "Pero, como en cualquier organización grande, una cosa es tener confianza en nuestra capacidad para comprender el riesgo inherente y el entorno de amenazas; otra muy distinta es poder afirmar de manera categórica que lo tenemos todo cubierto al detalle, sin dejar cabos sueltos, de modo que no haya ninguna posibilidad de sufrir un incidente significativo."

Confianza vs Brecha de implementación

Grado de implementación de acciones relacionadas con la ciberseguridad
P1: ¿En qué medida ha implementado su organización las siguientes acciones relacionadas con la ciberseguridad?
P2: ¿Qué tan de acuerdo o en desacuerdo está con las siguientes afirmaciones respecto de la estrategia de ciberseguridad de su organización?



Total (n=1,058)

Los encuestados cuentan con el patrocinio a nivel de consejo y la financiación que necesitan. Se muestran seguros del trabajo que sus organizaciones han realizado hasta la fecha. Entonces, ¿por qué no reportan niveles más altos de preparación en ciberseguridad de cara a las amenazas y desafíos futuros? Cuatro hallazgos de la encuesta ofrecen pistas en particular:

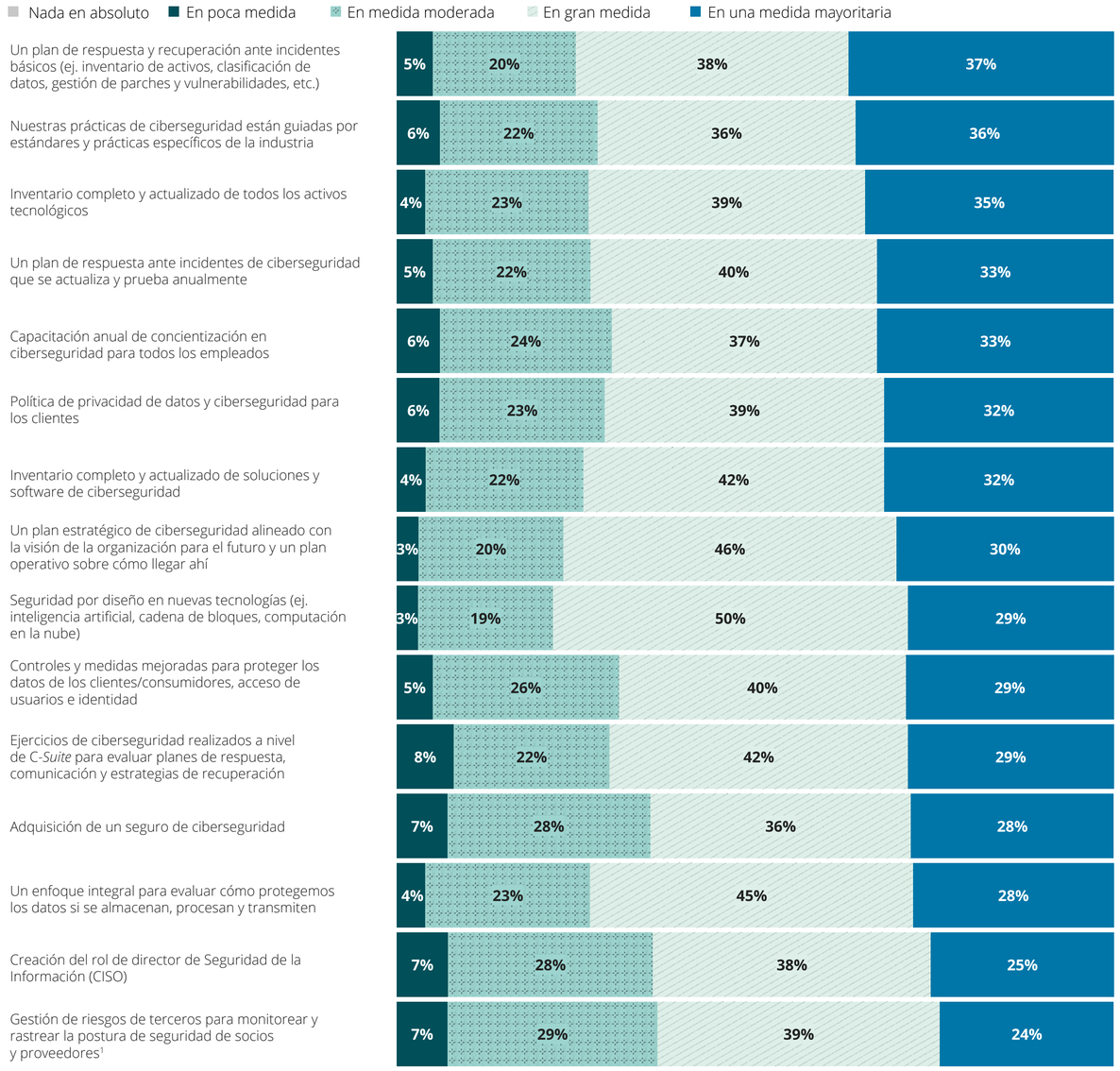
Alineación de negocio insuficiente

Muchos encuestados señalan que sus organizaciones aún no han creado la función de *Business Information Security Office* (BISO), cada vez más reconocida como un elemento central de las estrategias de ciberseguridad maduras. Solo el 63 % de los encuestados ha implementado esta función en gran o muy gran medida, lo que sugiere que muchas organizaciones carecen de los mecanismos necesarios para conectar sus dominios de negocio con las operaciones de ciberseguridad, gestión de riesgos y resiliencia.

Las capacidades de gestión del riesgo cibernético de terceros siguen desaprovechadas

Aunque los encuestados reportan depender de un número grande y creciente de proveedores de tecnología, al preguntarles en qué medida han incorporado capacidades de gestión de riesgos de ciberseguridad de terceros para monitorear y dar seguimiento a la postura de seguridad en su organización, califican este aspecto como el más bajo entre una larga lista de acciones relacionadas con la ciberseguridad. Solo el 65 % afirma haber implementado estas capacidades en gran o muy gran medida, lo que revela un riesgo potencialmente significativo no mitigado.

Grado de Implementación en Acciones Relacionadas con Ciberseguridad
P1. ¿En qué medida se han implementado en su organización las siguientes acciones relacionadas con la ciberseguridad?



Nota [1]: los porcentajes pueden no sumar exactamente 100% debido a ajustes por redondeo, dicha discrepancia es esperada y no representa un error.

Brechas de habilidades que impulsan la preocupación por la fuerza laboral

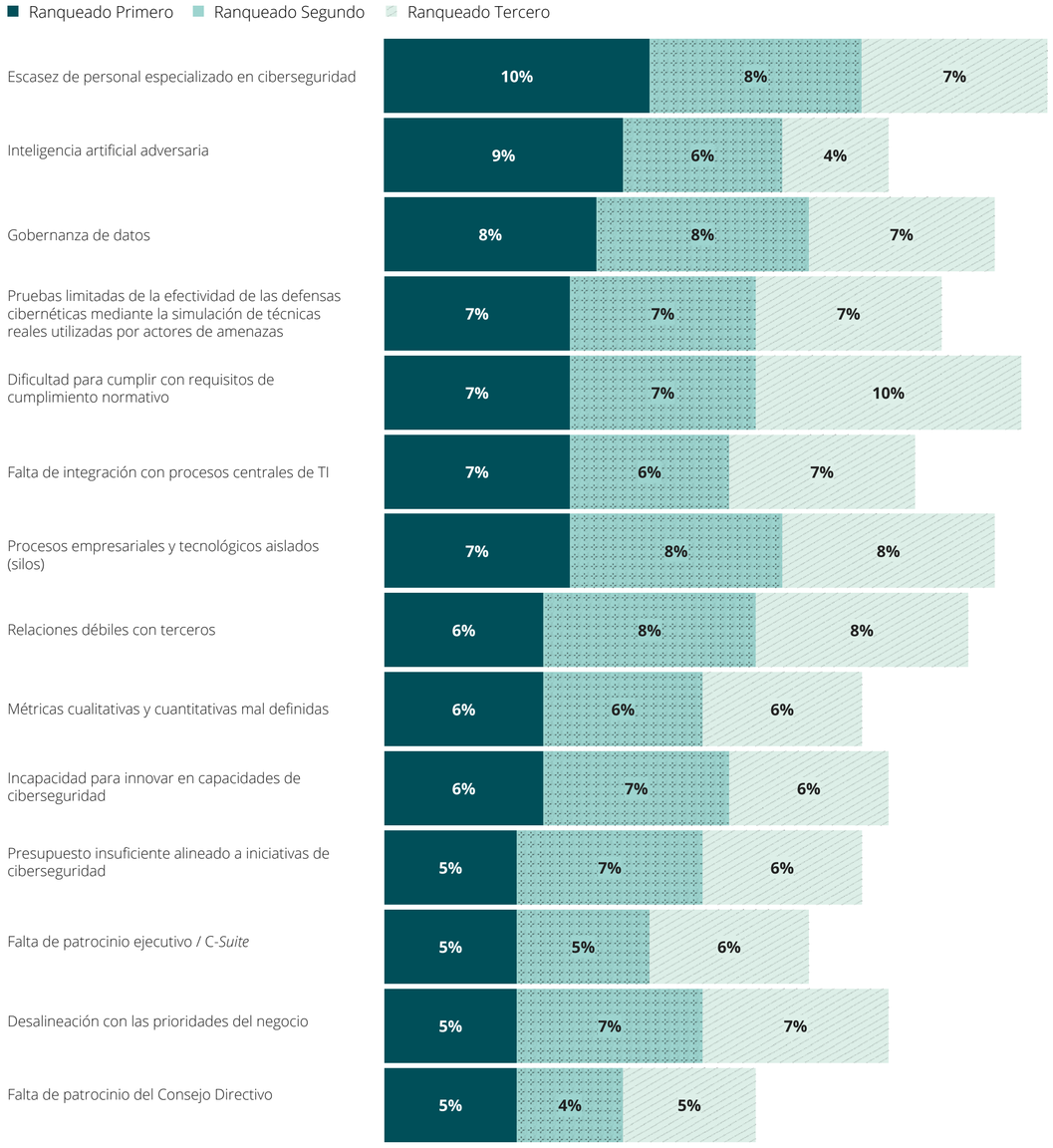
Se pidió a los encuestados que clasificaran los principales factores que limitan su capacidad para ser ágiles y atender asuntos de ciberseguridad, la falta de personal calificado apareció en los primeros lugares de la lista. Entre los participantes, la mayor parte lo ubicó como su principal factor limitante. De quince desafíos potenciales, el 10 % de los encuestados lo clasificó en primer lugar, lo que subraya la importancia de las competencias de la fuerza laboral para garantizar la preparación en ciberseguridad.

Un entorno de amenazas en evolución

La Inteligencia Artificial adversaria se produce si un actor de amenazas explota vulnerabilidades en sistemas de IA y utiliza técnicas avanzadas para perpetrar su ataque. Ingeniería social, *deepfakes*, identidad sintética, desinformación y envenenamiento de datos son ejemplos de IA adversaria, que los encuestados identifican como el segundo factor que más limita su capacidad para ser ágiles al atender asuntos de ciberseguridad. Esto sugiere que existe preocupación sobre la capacidad para adaptarse a un entorno tecnológico que cambia rápidamente y a las amenazas desconocidas que probablemente introduzca la IA, que afecta su nivel de preparación.

"Existen sistemas de IA capaces de mutar después de ser detectados y de que empecemos a combatirlos como si fueran un programa maligno", afirma el VP de Seguridad Global de una empresa de tecnología médica. "Luego mutan a otro tipo de programa maligno. Hablamos de ataques a escala. Necesitamos responder de manera automatizada para defendernos: si nuestros adversarios despliegan un enjambre de ataque de IA agentiva, debemos contar con un enjambre defensivo habilitado por IA igualmente sofisticado, capaz de aprender sus patrones de ataque."

Principales Factores que Limitan la Capacidad para Abordar Problemas de Ciberseguridad (Clasificado desde el más importante)
P. ¿Cuál de los siguientes factores limita más la capacidad de su organización para ser ágil y responder a los problemas de ciberseguridad? Clasifique los 3 factores principales.



Total (n=1,058)

Desentrañando la paradoja

La brecha entre confianza y preparación en ciberseguridad quizá se comprenda mejor en el contexto del recorrido que va de la estrategia y la visión a la ejecución. Tras dedicar años a consolidar con éxito el apoyo de la alta dirección y la financiación para iniciativas de ciberseguridad, así como a diseñar y ejecutar la planificación estratégica junto con sus pares del negocio, los encuestados aún no han logrado impulsar los principios, procesos y tecnologías de ciberseguridad a mayor profundidad en toda la organización. Confían en su capacidad para ayudar a la organización a avanzar en materia de ciberseguridad, pero todavía no han puesto en marcha los mecanismos que saben que se requieren para garantizar la preparación.

¿Cuáles son los siguientes pasos para los líderes que buscan traducir los éxitos a nivel estratégico en ejecución operativa en primera línea? Tanto los hallazgos de nuestra encuesta como las entrevistas en profundidad con los encuestados "en especial con quienes destacan tanto en confianza como en preparación" señalan varios hitos críticos.

Considerar incluir el rol BISO en la agenda

Los BISO *(Business Information Security Officer)* pueden servir como enlace entre las funciones de ciberseguridad y el negocio. Para las organizaciones que buscan convertir estrategias de ciberseguridad bien diseñadas en ejecución a nivel de negocio, quizá no haya un rol más importante. De hecho, muchas organizaciones reportan integrar arquitectos de seguridad y funciones BISO para mantenerse estrechamente alineadas con los equipos de producto, DevOps (Desarrollo y Operaciones) y arquitectura. Dado el foco previo en la estrategia, no debería sorprender que, hasta ahora, se haya prestado menos atención a los BISO.

El rol BISO puede no ser adecuado para todas las organizaciones, aunque lograr una integración estrecha entre los procesos y funciones de negocio y de tecnología es relevante para todas. Las organizaciones más pequeñas (o aquellas con alta centralización) podrían estar mejor posicionadas para utilizar equipos ágiles que incluyan profesionales de seguridad, en lugar de crear un nuevo puesto.

Aprovecha las capacidades estratégicas de los proveedores

Los terceros suelen contratarse para asumir o automatizar trabajos tediosos y de gran consumo de tiempo que las organizaciones no tienen recursos para gestionar por sí mismas. A medida que las organizaciones fortalecen sus capacidades y estas relaciones maduran, pueden evolucionar hacia colaboraciones aún más valiosas, basadas en la estrategia. Los terceros son una parte fundamental de una postura de ciberseguridad sólida

Ante las amenazas emergentes, encuentra el equilibrio entre la preocupación y el riesgo real

Si bien en la encuesta las preocupaciones de los encuestados sobre la Inteligencia Artificial adversaria parecen elevadas, la experiencia de clientes de Deloitte sugiere que estas inquietudes podrían estar sobredimensionadas respecto al riesgo real que se plantea hoy. En nuestras entrevistas con ciertos encuestados, señalaron aprensión por la naturaleza relativamente desconocida de la IA adversaria. Si bien afrontan "incógnitas conocidas" *(known unknowns),* es comprensible que se sientan menos cómodos ante "incógnitas desconocidas" *(unknown unknowns).*

La IA adversaria amerita atención y cuidado por parte de los líderes con responsabilidades en ciberseguridad, sin embargo, enfocarse en desafíos conocidos y abordables, como la exposición involuntaria de datos y el uso indebido de información sensible en entornos de IA generativa (GenAI), puede tener un mayor impacto hoy. No permita que el miedo supere a la razón de abordar la IA adversaria en su lugar, investíguela para comprender qué nivel de inversión se justifica, mientras mantiene el enfoque constante en otros retos más inmediatos.

> **"Contamos con el nivel adecuado de inversión, tenemos el involucramiento del liderazgo que necesitamos y disponemos de las herramientas y procesos correctos.** Pero, como en cualquier organización grande, una cosa es tener confianza en nuestra capacidad para comprender el riesgo inherente y el entorno de amenazas, otra muy distinta es poder afirmar, de manera general, que lo tenemos todo cubierto al detalle, sin que exista posibilidad de sufrir un incidente significativo."
>
> **-CISO, Sector Salud**

PARADOJA #2

El equipo ejecutivo cree y prioriza la estrategia cibernética. En el resto de la organización, la ciberseguridad no tiene el mismo nivel de influencia.

La alta dirección está alineada y comprometida.

La ciberseguridad es una prioridad clara para las empresas en los niveles más altos. Este fue un hallazgo clave en nuestra encuesta anterior y nuestros datos más recientes muestran un patrocinio a nivel ejecutivo que continúa fortaleciéndose en torno a las prioridades de ciberseguridad.

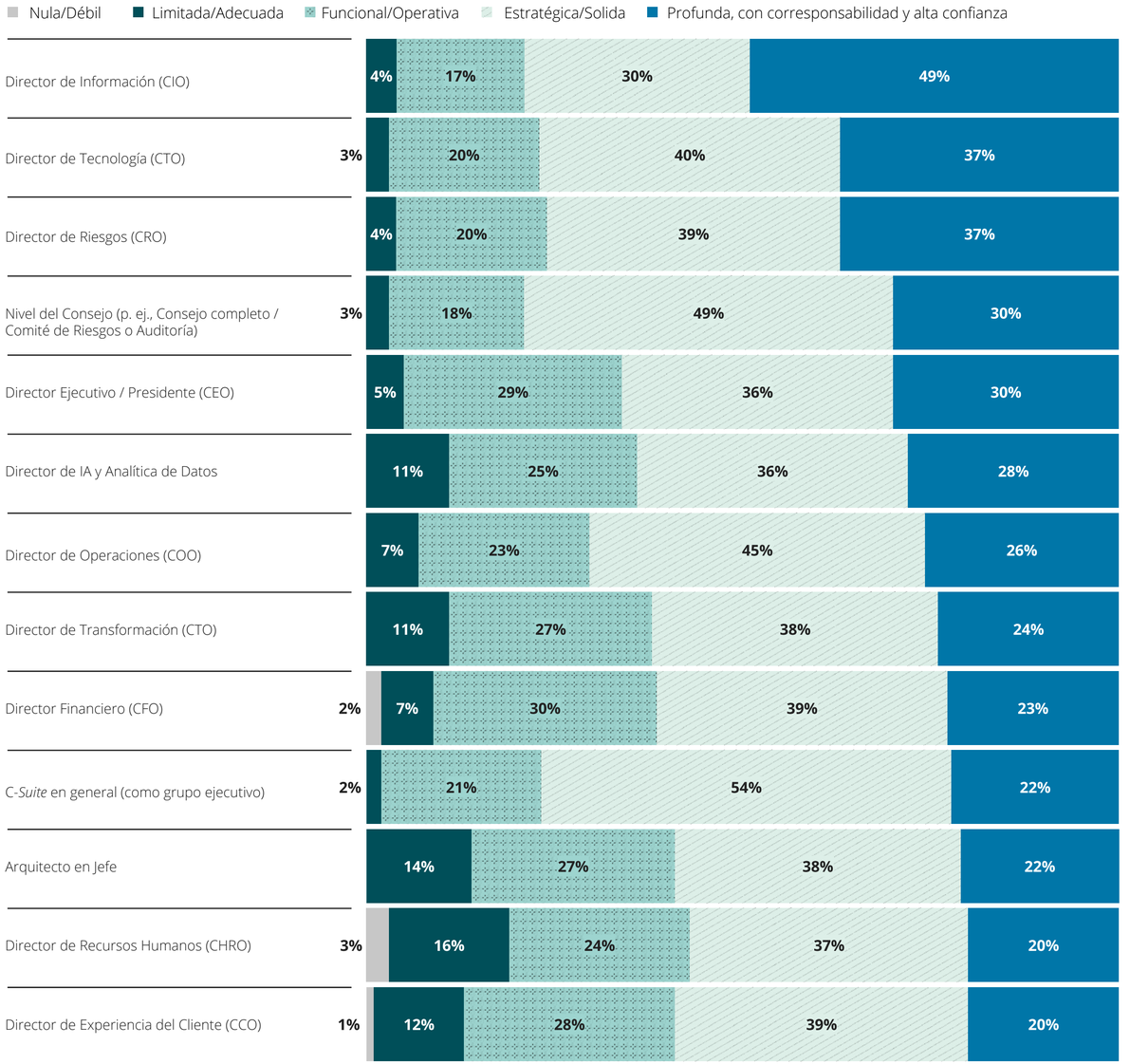
Los *Frontrunners* se distinguen por tener CISOs con relaciones sólidas en lo más alto: con la C-suite en general, el CEO y el consejo de administración (más del 90 %). En comparación, en las organizaciones *Followers* donde se reporta que los CISOs mantienen relaciones sólidas con el consejo y con el CIO (80 % en cada caso). Entre los *Foundation Builders,* los CISOs tienen sus relaciones más sólidas con los CIO (72 %).

Este año, la ciberseguridad sigue siendo una prioridad empresarial para la C-*suite*. La mayoría de los encuestados afirma que el CISO de su organización mantiene una relación sólida con el CEO (66 %) y un porcentaje aún mayor (76 %) indica lo mismo respecto de la C-*suite* en general son elementos clave para asegurar que la organización esté preparada para enfrentar futuros desafíos cibernéticos.

La mayoría de los Cisos reporta al CEO (28 %) o al CIO (33 %), lo que les da una línea directa con el equipo de liderazgo ejecutivo. La mayor proporción de los encuestados señala que integran plenamente la ciberseguridad en sus planes estratégicos más amplios de negocio y tecnología o que incorporan activamente requisitos de ciberseguridad en su estrategia a futuro (54 %). Los *Frontrunners* tienen una probabilidad significativamente mayor de que la ciberseguridad sea corresponsable o sea impulsor de la estrategia y del presupuesto tanto del stack central de TI (61 %) como de la estrategia central del negocio (57 %), en comparación con los *Followers* (43 % y 29 %, respectivamente) y los *Foundation Builders* (31 % y 15 %, respectivamente).

Aunque las iniciativas de ciberseguridad cuentan con un amplio apoyo en los niveles superiores de sus organizaciones, los encuestados enfrentan dificultades para ampliar su alcance hacia los procesos cotidianos de ejecución y la toma de decisiones operativas.

Fortaleza de la Relación entre el CISO y Otros Líderes del Negocio
P. Piensa en el CISO de su organización (o el líder equivalente de seguridad), ¿qué tan sólida es su relación de trabajo con cada uno de los siguientes líderes?



***Excluye respuestas de "no sabe".**

Total (n=1,039)*

PARADOJA #2

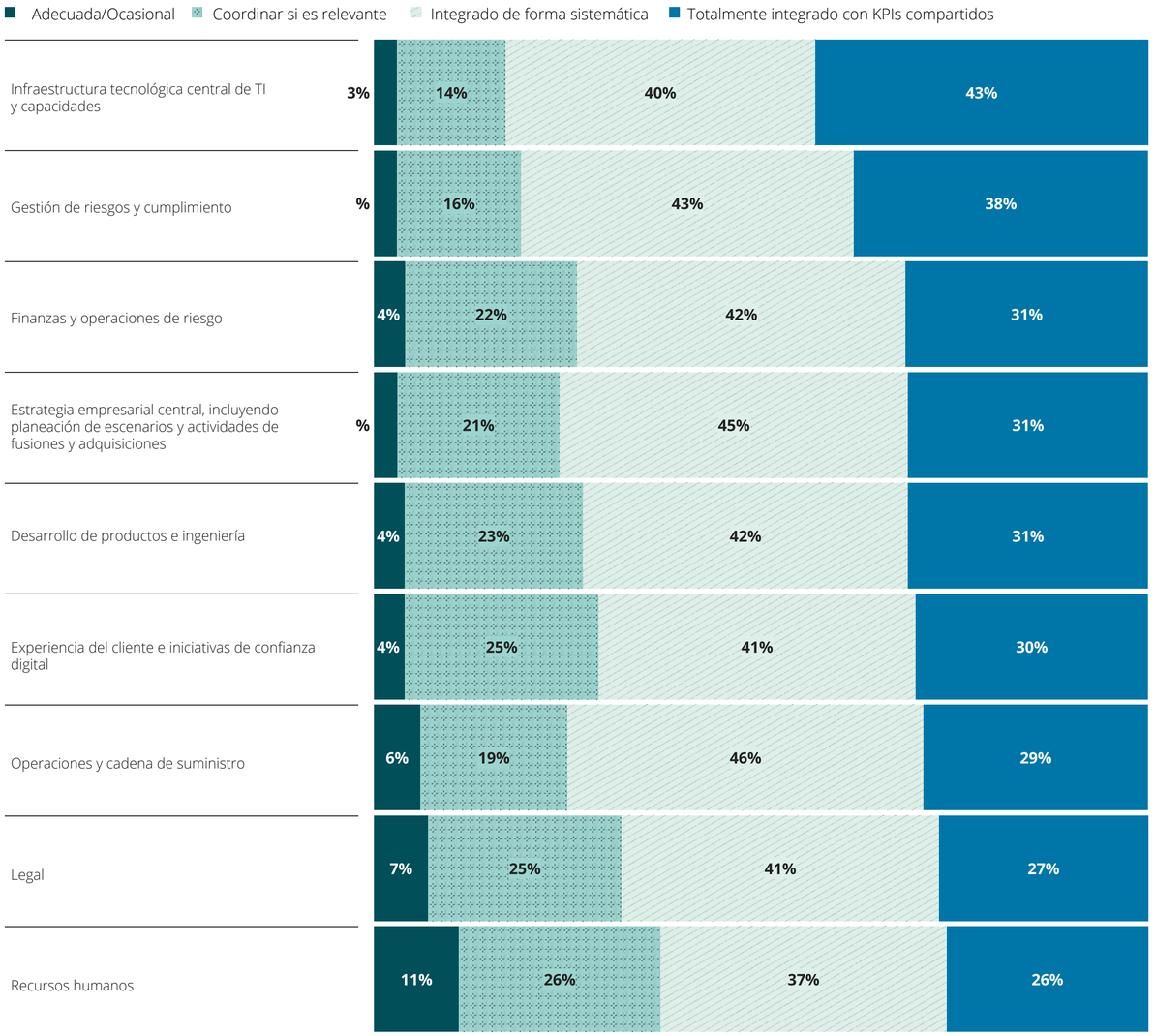
La influencia de la ciberseguridad aún no pasa de la visión a la ejecución

Si bien en general existe una sólida alineación en materia de ciberseguridad dentro de la C-*suite*, el siguiente paso para muchas organizaciones es la integración sistémica de la ciberseguridad en las funciones críticas de las unidades de negocio y de tecnología.

La ejecución por la línea de negocio es un factor clave para el despliegue exitoso de las estrategias de ciberseguridad. Los encuestados señalaron que, entre nueve dominios, la ciberseguridad tuvo la mayor influencia en la estrategia y en los procesos relacionados con la TI central y la gestión de riesgos. En ambas áreas, más del 80 % de los encuestados afirma que los indicadores clave están en marcha de una fuerte alineación entre las prácticas de negocio y de ciberseguridad. Fuera de este ámbito de influencia, la ciberseguridad tiene menor impacto en la estrategia central del negocio y en otras funciones. Mientras tanto, la mayoría de los *Frontrunners* indica que sus organizaciones integran plenamente la ciberseguridad en su estrategia más amplia. Asimismo, es significativamente más probable que cuenten con todos los mecanismos necesarios para conectar la ciberseguridad con la estrategia del negocio, especialmente en la estrategia de gestión de riesgos empresariales (96 %).

"El objetivo del CISO es lograr la transición de ser muy táctico y técnico a estar más alineado con el negocio mediante una nueva metodología", afirma el CISO del Grupo en una empresa de servicios financieros. "Esa nueva metodología debería permitirles realizar modelado de amenazas y evaluación de riesgos sobre las cadenas de valor de generación de ingresos del negocio, que es lo que realmente importa a los líderes empresariales."

Grado en que la Organización Conecta Ciberseguridad con Otros Dominios
P. ¿En qué medida su organización conecta la ciberseguridad con los siguientes dominios en la planificación y en la toma de decisiones del día a día?



Total (n=1,058)

Adicional, la ciberseguridad aún no influye de manera significativa en el desarrollo tecnológico de productos. Aunque DevSecOps ha alcanzado una madurez máxima y el 78 % de los encuestados afirma que los líderes de ciber de sus organizaciones están integrados formalmente en las prácticas de DevSecOps, solo el 40 % considera que existe corresponsabilidad real con indicadores clave compartidos. Los *Frontrunners* superan ampliamente a los *Followers* en contar con una corresponsabilidad más estrecha en DevSecOps por 22 puntos porcentuales (61 % frente a 39 %), así como en diseño de soluciones y modelado de amenazas (52 % frente a 26 % de los Seguidores) y en directrices del *stack* tecnológico *(guardrails)* (51 % frente a 28 % de los Seguidores).

Esto podría deberse a la falta de influencia actual de ciberseguridad, sobre los líderes que "poseen" los mecanismos de control organizacional, como el CTO y el *Chief Architect*. Se trata de relaciones estratégicas importantes que tienen la llave para impulsar una integración más profunda en ingeniería de producto, diseño de aplicaciones y funciones de seguridad.

Actualmente, los CISO no cuentan con las estructuras de reporte ni con las relaciones necesarias para abordar esta falta de influencia. Por ejemplo, al analizar las líneas de reporte, podemos hacernos una idea de la fortaleza de las relaciones. Solo el 37 % de los CISO mantiene una relación profunda y de confianza con el CTO, a pesar de que el CTO es un socio fundamental para el desarrollo y la ejecución tecnológicos. De forma similar, apenas el 22 % declara tener una relación profunda y de confianza con el *Chief Architect,* el cargo responsable de definir la futura base técnica de la organización. Estos hallazgos reflejan y refuerzan la brecha entre la visión y la implementación identificada en la paradoja previa sobre confianza y preparación.

> "El objetivo del CISO es poder pasar de ser **muy táctico y técnico a estar más alineado con el negocio mediante una nueva metodología.** Esa nueva metodología debería permitirles realizar modelado de amenazas y evaluación de riesgos sobre las cadenas de valor de generación de ingresos del negocio, que es lo que realmente importa a los líderes empresariales."
>
> **-Grupo CISO, Servicios Financieros**

Desentrañando la paradoja

Las iniciativas de ciberseguridad gozan de un amplio respaldo en los niveles superiores. Al mismo tiempo, la ciberseguridad está menos integrada con las funciones centrales del negocio que amplían su alcance hacia los procesos cotidianos a nivel de ejecución y la toma de decisiones. A continuación, algunos de los pasos más importantes para cambiar esta dinámica:

Incorpora la ciberseguridad en todas las mesas de decisión

La mayoría de las organizaciones cuenta con una base de ciberseguridad. Por ejemplo, los principios y procesos de DevSecOps están ampliamente adoptados. Pero para que la ciberseguridad esté verdaderamente incorporada en las arquitecturas tecnológicas, los sistemas deben diseñarse con corresponsabilidad real e indicadores claves compartidos entre los líderes de ingeniería y seguridad. Ese es el objetivo de los enfoques de seguridad desde el diseño *(secure by design),* que incorporan principios de seguridad en los sistemas desde el inicio.

La implementación, sin embargo, requiere más que una postura sólida de ciberseguridad o una mentalidad de "marcar la casilla". Una arquitectura empresarial con principios de seguridad integrados exige que la organización pase de una mentalidad de "seguir el proceso" a trabajar por resultados compartidos, como la ingeniería orientada a la agilidad y la resiliencia. Para lograr todo esto, la ciberseguridad debe incluirse como parte del proceso lo antes posible, en toda la organización.

Toma en serio la relación entre el CISO y el *Chief Architect*

Actualmente, los CISO no cuentan con relaciones sólidas, a nivel estratégico, con los *Chief Architects* que se requieren para impulsar la integración de los principios y prácticas de ciberseguridad en la ingeniería de producto, el diseño de aplicaciones y la funcionalidad tecnológica. Como en cualquier relación, estos vínculos no se fortalecerán por sí solos, los CISO deben elaborar un plan para establecer lazos más firmes con estas partes interesadas críticas, a fin de asegurar que las medidas de ciberseguridad se incorporen directamente en las soluciones que se desarrollen en el futuro.

"Antes teníamos un equipo centralizado de arquitectura empresarial que reportaba al responsable de tecnología y que, con el último CTO, se unió... Así que ahí perdimos algo de impulso... mi equipo creó un consejo de revisión de seguridad de arquitectura, lo iniciaron diciendo: 'este es un lugar al que pueden venir a recibir asesoría'", comenta el CISO de una empresa del sector salud.

Una relación más sólida entre el CISO y el *Chief Architect* podrá desbloquear beneficios importantes para la organización. Por ejemplo, casi la mitad de los encuestados considera que una integración entre la arquitectura empresarial y la ciberseguridad beneficiaría de manera significativa los tiempos de recuperación de TI/operaciones tanto en el corto como en el largo plazo. También identifican como beneficios principales, el fortalecimiento de la inteligencia de amenazas y de la seguridad de aplicaciones. Todas estas son áreas que requieren la adhesión y el apoyo activo del *Chief Architect.*

Alinea las prioridades de la organización con sus responsables

¿Dónde se encuentran hoy las prioridades críticas para la misión de su organización y qué líderes tienen la responsabilidad principal de gestionarlas? Las respuestas pueden servir como un mapa práctico hacia las relaciones más importantes para los CISO y otros con responsabilidades de ciberseguridad. Si la organización activa una nueva estrategia orientada al cliente, la ciberseguridad debe estar en la conversación, sobre todo: desde temas de datos de clientes, experiencia del cliente, privacidad y más. Estas son las relaciones clave del negocio que pueden ser determinantes para extender el alcance de ciber más allá de la estrategia e introducirlo en las operaciones centrales del negocio.

El impacto puede ser significativo. El 61 % de los CISO en organizaciones *Frontrunner* comparten la corresponsabilidad en el desarrollo de estándares operativos de TI. También van a la cabeza en la prestación de apoyo consultivo sobre diseño de soluciones y modelado de amenazas, el 52 % de los CISO *Frontrunner* participan en estas iniciativas.

Refuerza las habilidades blandas

Los CISO y otros líderes de ciberseguridad suelen llegar a sus cargos por sus sólidas capacidades técnicas y estratégicas. Pero su capacidad para abrirse camino con éxito en otras partes de la organización—una característica clave de estos roles—depende en buena medida de las llamadas "habilidades blandas" que quizá fueran menos relevantes en sus posiciones anteriores. ¿Son buenos escuchas y comunicadores? ¿Pueden establecer terreno común con colegas y con otros líderes? Estas habilidades inciden directamente en su capacidad para convencer a los demás de que la ciberseguridad es un habilitador del negocio y no un obstáculo incómodo.

> "Antes teníamos un equipo centralizado de arquitectura empresarial que reportaba al responsable de tecnología y que, con el último CTO, se unió... Así que ahí perdimos algo de impulso... mi equipo creó un consejo de revisión de seguridad de arquitectura... lo iniciaron diciendo: 'oye, este es un lugar al que puedes venir a pedir consejo".
>
> **-CISO, Sector Salud**

PARADOJA #3

“Queremos menos proveedores.”

“Necesitamos más proveedores.”

Sobrecarga de proveedores

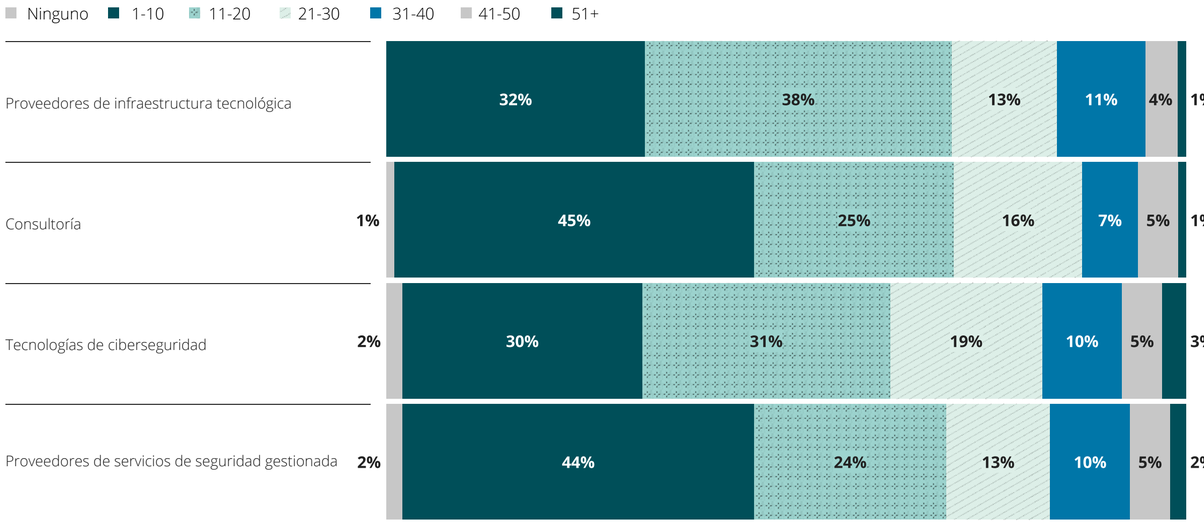
Los cambios continuos en el panorama de amenazas, combinados con un conjunto de soluciones y capacidades tecnológicas en constante evolución, han llevado a los profesionales de ciberseguridad a establecer relaciones con un número grande y creciente de proveedores y sin un final a la vista.

Los encuestados trabajan con lo que parece ser una cantidad abrumadora de proveedores para gestionar y se espera que esos números aumenten en los próximos tres y cinco años. En cuanto a la infraestructura tecnológica, la mayor proporción (38%) de los encuestados tiene entre 11 y 20 proveedores, aunque 29% tiene 21 o más.

Y aunque nuestras entrevistas sugieren que muchos no desean necesariamente aumentar el número de proveedores, dado el creciente interés en migrar hacia plataformas, es posible que no haya alternativa si las tecnologías actuales no satisfacen las necesidades presentes o futuras. Para algunas organizaciones, mantener un gran número de proveedores (a menudo más de 20) es una estrategia intencional para evitar el riesgo de concentración en un solo proveedor.

Incluso entre los líderes que preferirían asociarse con menos proveedores para simplificar la integración y reducir la complejidad operativa, muchos ven la consolidación como un camino hacia un riesgo concentrado: un menor número de actores puede crear puntos únicos de falla. No existe una solución única que funcione para todos frente a este dilema.

Número de socios cibernéticos por categoría
Pregunta: ¿Con cuántos socios cibernéticos trabaja su organización en cada una de las siguientes categorías?



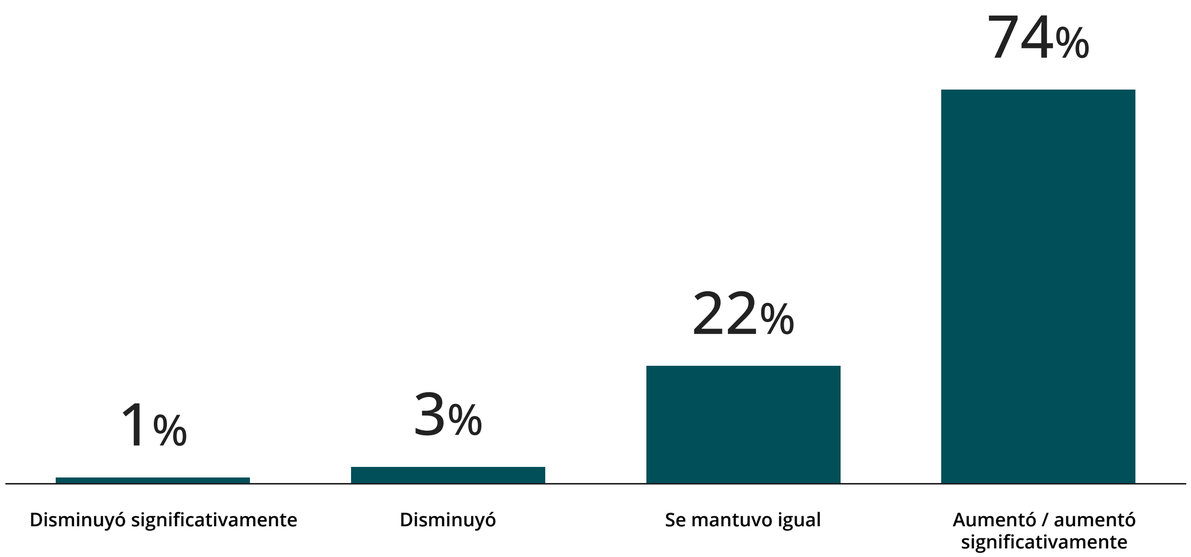
Total (n=1,058)

El portafolio de proveedores: grande y en crecimiento
A pesar de contar ya con un número elevado de proveedores, los encuestados afirman que el total de proveedores ha aumentado o incrementado significativamente en el último año, y que esperan depender de un número aún mayor de proveedores en los próximos uno, tres y cinco años. El 74% de los encuestados afirma que la cantidad de socios de ciberseguridad con los que trabaja su organización ha aumentado o incrementado significativamente en el último año.

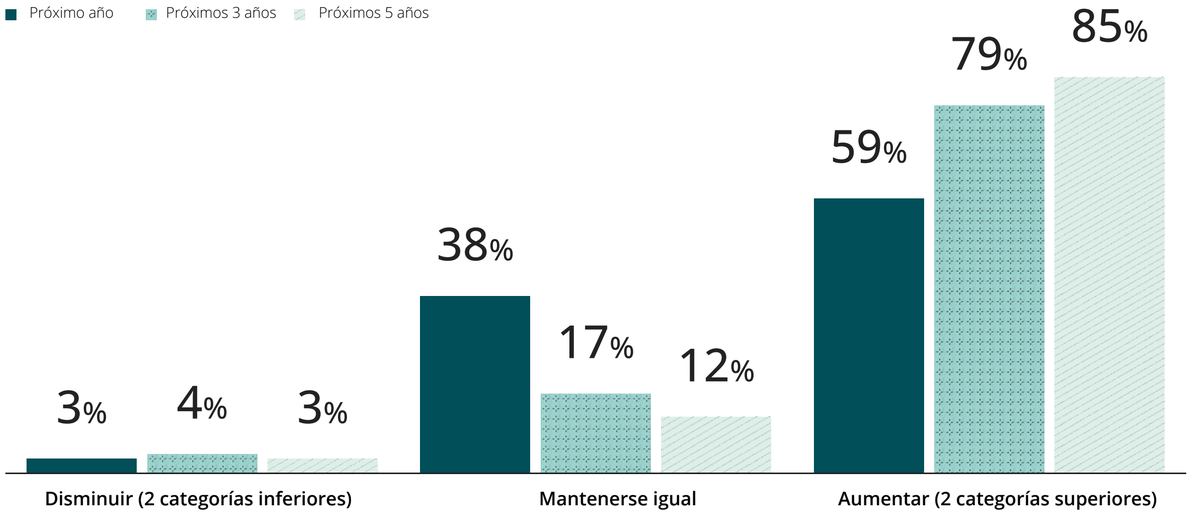
"Hemos incorporado a nuevos terceros que proveen soluciones de ciberseguridad para la empresa, y TI también ha sumado más socios para gestionar algunos de sus servicios de infraestructura", comenta el CISO de una empresa de servicios financieros. "Lo mismo ocurre con los CIO: ellos también han añadido más soluciones y a terceros para sus equipos de aplicaciones".

Solo el 38% espera que el número de socios de ciberseguridad se mantenga estable durante el próximo año. La mayoría anticipa un crecimiento: el 79% de los encuestados prevé que la cifra aumentará o incrementará significativamente en los próximos tres años. Y se les preguntó por los próximos cinco años, este porcentaje ascendió a 85%.

Cambio en el número de socios de ciberseguridad en el último año
Pregunta: ¿Cómo ha cambiado el número de socios de ciberseguridad con los que trabaja su organización durante el último año?



Cambio futuro esperado en el número de socios de ciberseguridad
Pregunta: ¿Y cómo anticipa que esto cambie en los próximos 1, 3 y 5 años?



Total (n=1,058)

¿Qué impulsa este crecimiento?

Los nuevos proveedores se buscan debido a la IA
Aunque las organizaciones ya cuentan con numerosos proveedores, una razón por la cual podrían establecer nuevas relaciones estratégicas es para incorporar nuevas capacidades técnicas o abordar riesgos emergentes. La IA ha sido un fuerte impulsor de las mejoras en las capacidades de ciberseguridad durante el último año; una amplia mayoría de los encuestados (casi 75%) ha actualizado los programas de ciberseguridad existentes para incorporar capacidades de razonamiento avanzado para el análisis de amenazas en tiempo real y la monitorización de la infraestructura digital. El 76% de los encuestados indicó que contratan proveedores de ciberseguridad que integran IA en sus servicios.

La ciberseguridad no está bien integrada en el *stack* tecnológico
Actualmente, solo aproximadamente 30% de los encuestados considera que la ciberseguridad está altamente integrada en el *stack* tecnológico. Estos datos sugieren que pueden existir patrones de arquitectura redundantes, lo que crea una oportunidad para la racionalización y consolidación de proveedores mediante una arquitectura empresarial más optimizada.

Los encuestados indican que las organizaciones podrían avanzar en esa dirección en los próximos 12 a 24 meses, con un aumento esperado de 8 puntos porcentuales en los niveles de integración. Observamos el mismo patrón en el movimiento hacia plataformas de ciberseguridad más integradas como un mecanismo para optimizar (y potencialmente reducir) el ecosistema de proveedores.

> **"Hemos incorporado a nuevos terceros que proporcionan soluciones de ciberseguridad a la firma,** y el área de TI también ha añadido más socios para gestionar algunos de sus servicios de infraestructura. Ocurre lo mismo con los CIO: ellos también han sumado más soluciones y a terceros para sus equipos de aplicaciones".
>
> **— Director Global de Seguridad de la Información (CISO), Servicios Financieros**

PARADOJA #3

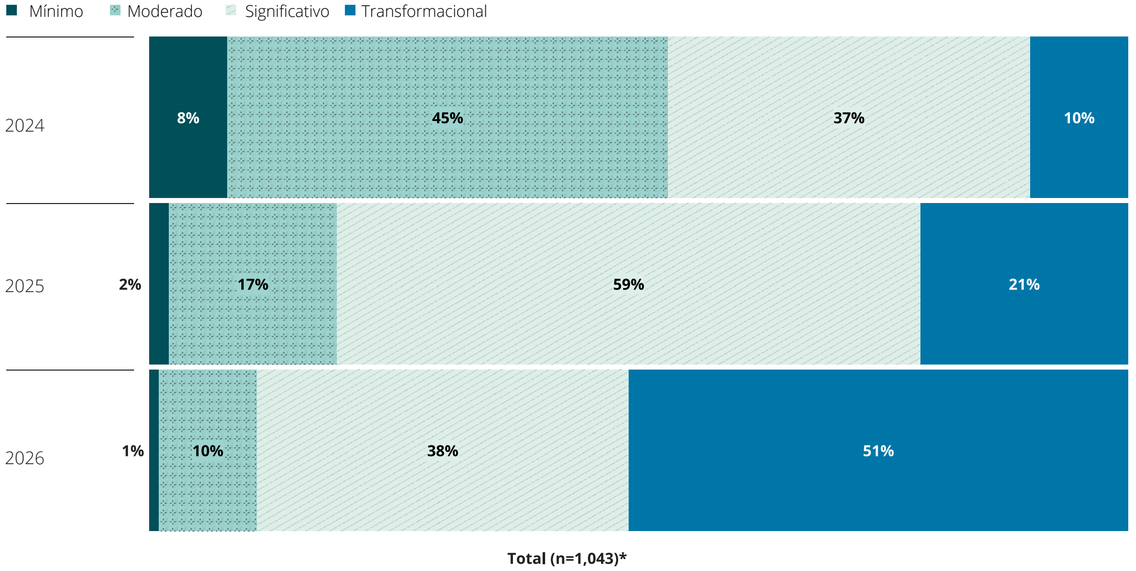
Los encuestados reportan un crecimiento de 5 veces en el avance hacia plataformas de ciberseguridad integradas, de 2024 a 2026.

En nuestra encuesta anterior (2024), solo 10% de los encuestados indicó que sus organizaciones avanzan hacia plataformas de ciberseguridad integradas de manera transformacional. En 2025, ese porcentaje más que se duplicó, alcanzó el 21%. Y 51% de los encuestados espera que estas plataformas integradas sean transformacionales en 2026, lo que refleja un cambio de impulso significativo hacia la integración. Entre los *Frontrunners,* este cambio es aún más marcado: 64% reportó un movimiento significativo o transformacional en 2024, y 94% espera lo mismo para 2026.

¿Qué explica este cambio de impulso hacia plataformas de ciberseguridad consolidadas? Los impulsores tradicionales —como la reducción de la complejidad y un menor costo total de propiedad— probablemente están detrás de estas decisiones. Algunas empresas prefieren migrar a una sola plataforma "suficientemente buena" en lugar de gestionar una colección de proveedores especializados con soluciones de nicho.

También pueden estar influyendo otros factores, empecemos por la IA. Los líderes de ciberseguridad y tecnología saben que la IA requiere datos consistentes y normalizados para funcionar de manera efectiva, y las plataformas están bien posicionadas para proporcionarlos. Para quienes se implementan estrategias de IA agentica, estas plataformas suelen ofrecer los modelos de datos estandarizados necesarios para construir flujos de trabajo basados en agentes.

Grado en que la organización avanza hacia plataformas integradas para actividades de ciberseguridad
Pregunta: ¿En qué medida su organización avanza hacia una plataforma integrada para sus actividades de ciberseguridad en el año pasado, este año y el próximo año?



Total (n=1,043)*

***Excluye respuestas de "no sabe".**

Desentrañando la paradoja

¿Es inevitable la proliferación de proveedores? Podría parecer que sí hoy en día, ya que el entorno de amenazas sigue siendo cambiante y se requieren nuevas herramientas y capacidades para abordarlas rápidamente. Con presupuestos suficientes y apoyo ejecutivo, los encuestados simplemente suman proveedores a su arsenal.

En este contexto, es fácil comprender el creciente atractivo de las plataformas, especialmente aquellas que requieren menos esfuerzo para administrarse, incorporan muchas de las mismas herramientas y capacidades que los proveedores especializados y pueden integrar diferentes tecnologías con un costo total de propiedad más bajo.

A medida que las organizaciones buscan controlar la proliferación de proveedores impulsada por la IA y por arquitecturas poco integradas, hay algunas acciones que deberían considerar hoy en día:

Evaluar a los proveedores para identificar su valor real y su potencial no explotado

Los proveedores son un componente crítico de la estrategia de ciberseguridad de cualquier organización. ¿Tiene su organización un entendimiento claro y actualizado de cómo están sirviendo realmente a la organización hoy, dónde pueden existir capacidades redundantes entre distintos proveedores, o dónde podrían aportar un valor adicional? Es prácticamente imposible saberlo sin un enfoque estructurado de evaluación de proveedores que sea estratégico, intencional, basado en riesgos y disciplinado.

Aplicar principios de arquitectura empresarial para evaluar proveedores esenciales frente a redundancias

Si bien las organizaciones pueden haber añadido nuevos proveedores con el tiempo para abordar riesgos inmediatos en distintas líneas de negocio y geografías, esto también puede generar redundancias. La IA es solo un ejemplo reciente de una expansión bien intencionada del ecosistema de proveedores. Las organizaciones pueden identificar cuáles proveedores son esenciales para su misión y dónde podrían consolidar, trabajar estrechamente con los equipos de arquitectura empresarial, identificar capacidades duplicadas y buscar oportunidades para racionalizar, integrar y consolidar.

Mirar más allá de los beneficios de costo y eficiencia de las plataformas

El crecimiento de las plataformas está siendo impulsado por diversos factores: reducción de costos y mayor eficiencia, habilitación de IA, transformación de datos y reinvención de flujos de trabajo basados en agentes. En un momento en el que el interés en la IA agéntica aumenta, las plataformas pueden proporcionar estándares, controles y capacidades de integración, además de apoyar estrategias de consolidación y optimización de proveedores.

PARADOJA #4

Las brechas de ciberseguridad se mantienen estables y persistentes. Su impacto en el negocio está contenido.

Las brechas de ciberseguridad llegaron para quedarse

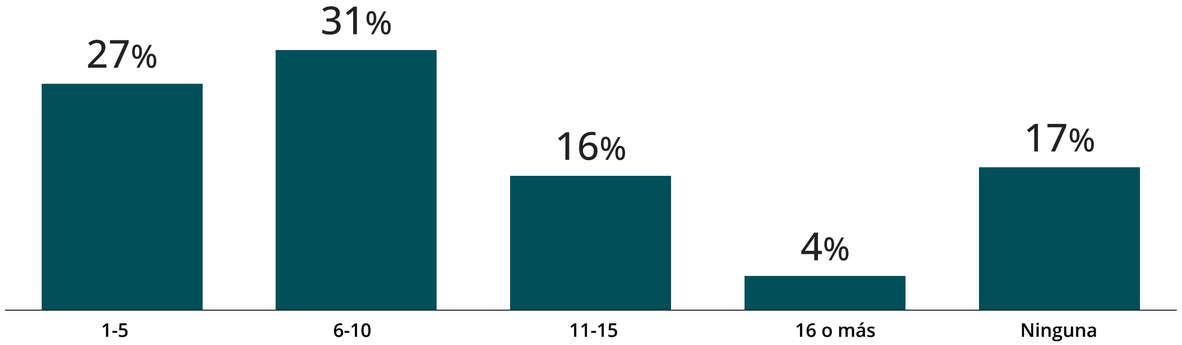
Los encuestados reportan un número elevado de incidentes. El 78% reportó públicamente al menos una brecha en 2025, en comparación con el 91% en 2024. Casi un tercio reportó entre 6 y 10 brechas en 2025, frente al 40% en 2024. Aunque el número de brechas reportadas disminuyó de un año a otro, continúa siendo alto.

También podemos suponer que algunas brechas de ciberseguridad no se reportan, especialmente entre organizaciones que pueden no contar con las capacidades necesarias para identificar y notificar estos incidentes.

Los encuestados están preocupados por un grupo familiar de actores de amenaza, comienza por ciberdelincuentes (30%), ciberterroristas (15%) y hacktivistas (10%). Las herramientas y tecnologías que estos actores utilizan también son conocidas: *ransomware* (20%), *malware* (15%) y exfiltración de datos (14%) siguen siendo las principales preocupaciones. Sin embargo, los hallazgos de este año revelan la aparición de un nuevo factor notable: el uso indebido de la IA, que ahora ocupa el cuarto lugar como un área emergente de preocupación.

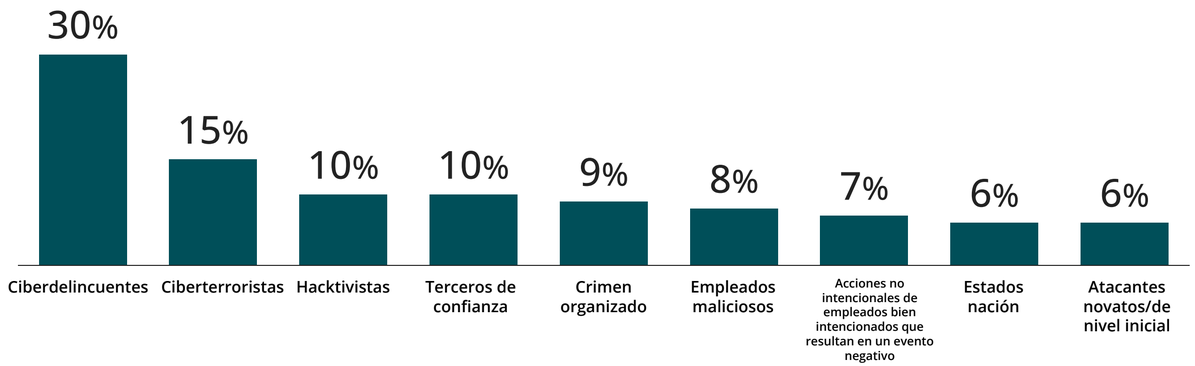
> **"Los compromisos de sistemas, aplicaciones y entornos van a ocurrir.** Si intentas prevenir cada compromiso, será muy difícil que la empresa pueda operar. El objetivo es construir su programa de manera que, si un sistema está comprometido, pueda detectarlo lo más rápido posible, contenerlo de inmediato y erradicarlo antes de que tenga un impacto mayor".
>
> **— CIO Global, Sector Salud**

Brechas de seguridad reportadas públicamente*
Pregunta: En el último año, ¿cuántas brechas de ciberseguridad ha reportado públicamente su organización?

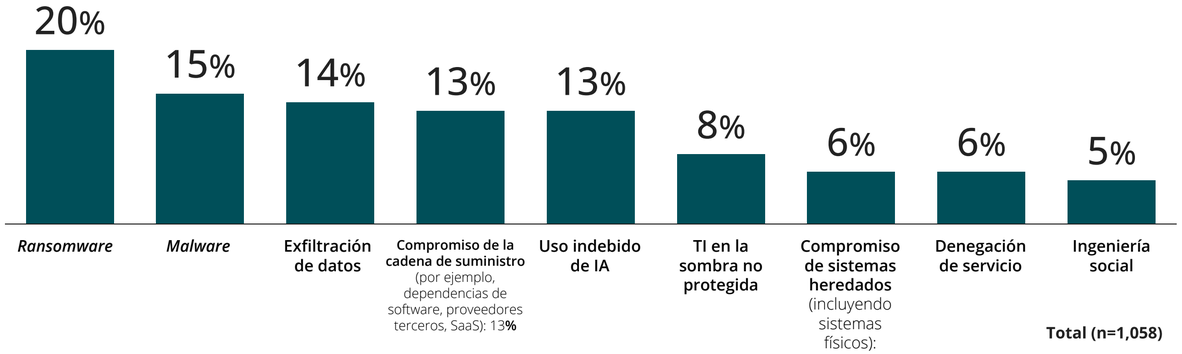


*Nota: No suma 100% porque el 5% de los encuestados son empresas privadas que no tienen obligación de reportar públicamente.

Fuente de amenazas de ciberseguridad más preocupante – Actores / Fuentes
Pregunta: ¿Cuál es la única fuente de amenaza de ciberseguridad que más preocupa a su organización?



Fuente de amenazas de ciberseguridad más preocupante – Herramientas / Técnicas
Pregunta: ¿Cuál es la única herramienta o técnica de ciberataque que más preocupa a su organización?



Total (n=1,058)

PARADOJA #4

Hasta ahora, las empresas han logrado minimizar con éxito el impacto de las brechas

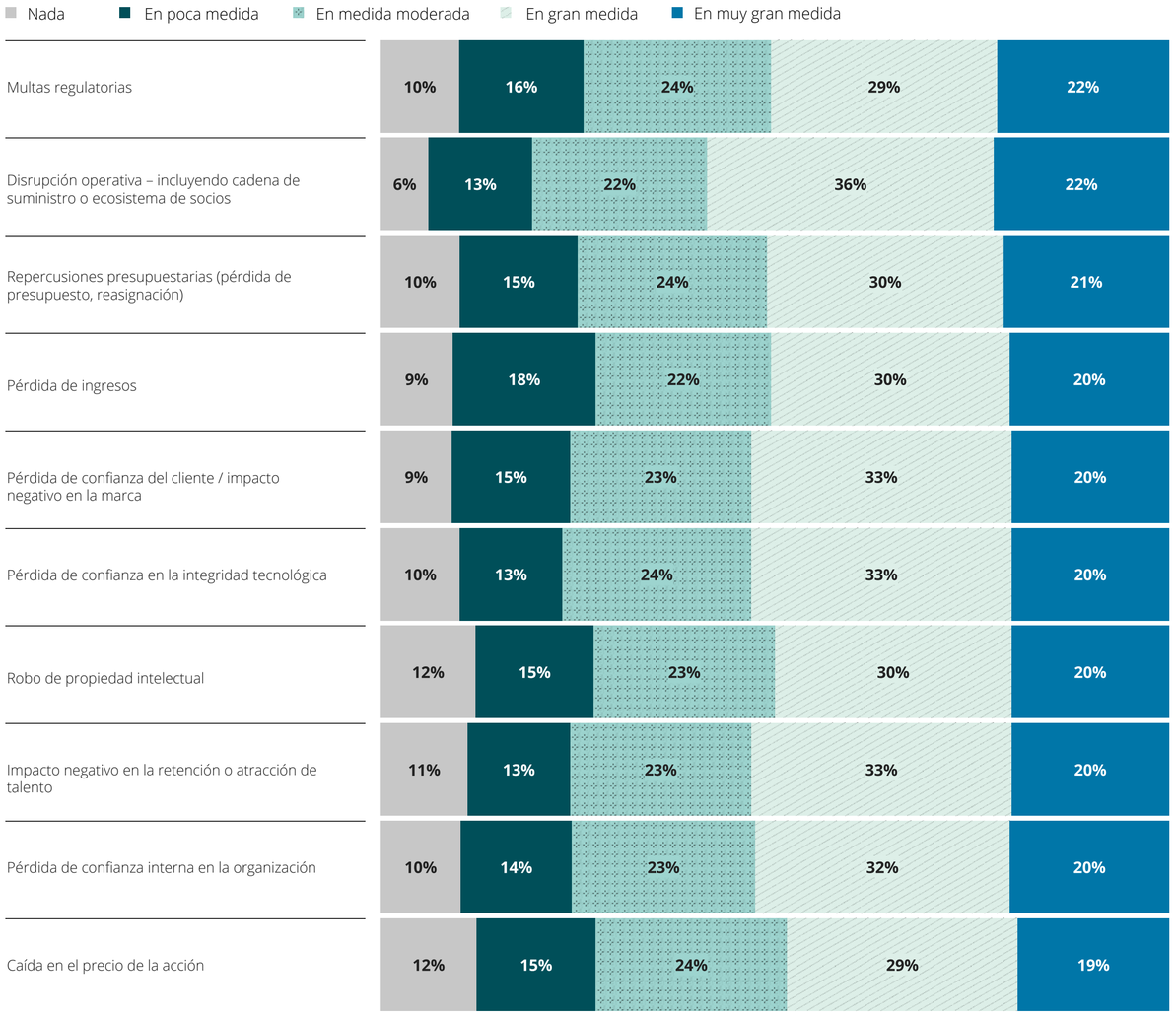
A pesar del número significativo de brechas de ciberseguridad, en promedio el 52% de los encuestados afirma que las consecuencias negativas han afectado a sus organizaciones en gran medida o en muy gran medida debido a incidentes de ciberseguridad en una variedad de posibles impactos. El año pasado, esta cifra era del 64%.

Esto no significa restar importancia al impacto. La disrupción operativa es la principal consecuencia de los incidentes de ciberseguridad, y el 58% afirma que sus organizaciones sufrieron interrupciones grandes o muy grandes en las operaciones, las cuales afectan sus cadenas de suministro y ecosistemas de socios. Sin embargo, hace un año, este mismo impacto fue experimentado por el 66% de los encuestados, lo que sugiere que las organizaciones han mejorado en la gestión de las consecuencias negativas.

"Los compromisos de sistemas, aplicaciones y entornos van a ocurrir", señala el CIO global de una empresa del sector salud. "Si intentas prevenir cada compromiso, será muy difícil que la empresa pueda operar. El objetivo es construir su programa de manera que, si un sistema es comprometido, pueda detectarlo lo más rápido posible—contenerlo de inmediato y erradicarlo antes de que tenga un impacto mayor".

Los *Frontrunners* reflejan especialmente este patrón. Una inteligencia de amenazas más madura puede permitirles reportar un mayor número de brechas que sus pares. El 26% de los *Frontrunners* reportó 11 o más brechas de ciberseguridad en el último año, frente al 19% de los *Followers* y el 20% de los *Foundation Builders*. A pesar de reportar más incidentes, los *Frontrunners* tienen la misma probabilidad que los *Followers* de reportar consecuencias negativas derivadas de incidentes de ciberseguridad.

Grado en que la organización ha sufrido consecuencias por incidentes o brechas de ciberseguridad
Pregunta: ¿En qué medida su organización ha sufrido consecuencias negativas en cada una de las siguientes áreas debido a incidentes o brechas de ciberseguridad?



Total (n=823)*

***Excluye "no sabe".**

Desentrañando la paradoja

Algo funciona. Esa es la conclusión más evidente que se puede extraer de esta paradoja positiva. Frente a una creciente ola de amenazas, los encuestados han logrado contener con éxito las consecuencias negativas asociadas con un incidente de ciberseguridad.

Pero no pueden permitirse caer en la complacencia debido a este éxito. A continuación, algunas formas prácticas de ayudar a extender esta tendencia alentadora:

¿Aumentan los reportes de brechas? No sobrerreacciones
Un aumento en el número de brechas reportadas puede, de hecho, reflejar prácticas sólidas de ciberseguridad, se demuestra que existen capacidades saludables de detección y respuesta de amenazas que se están siguiendo. En cualquier caso, se justifica un análisis más profundo. El volumen de brechas por sí solo no es un indicador útil sin información sobre qué se detecta, qué tan rápido se detecta y cuál es el posible impacto de las brechas en el negocio.

Considere enfocarse menos en el conteo de brechas y más en patrones y resultados.
¿Un aumento en brechas se debe a una detección más rápida de muchos incidentes de bajo impacto? Eso puede ser un signo positivo que apunta a una mayor madurez.
¿El aumento está vinculado a rutas de ataque recurrentes, tiempos prolongados de permanencia del atacante o disrupciones operativas? Sin este tipo de contexto, los líderes corren el riesgo de reaccionar en exceso mediante controles innecesarios, o subestimar su exposición a riesgos importantes.

¿Reportes bajos de brechas? Mira más de cerca
De manera similar, si su organización no reporta brechas, esto podría ser una buena señal, o podría ser el síntoma de una capacidad insuficiente para detectarlas. Como resultado, su organización podría no contar con capacidades adecuadas de monitoreo y analítica para identificar actividades maliciosas y brechas, lo que la dejaría susceptible a ataques latentes o “durmientes”.

Persigue la resiliencia sin descanso
El 67% de los encuestados realiza, de manera proactiva, ejercicios de planificación de escenarios para vincular la ciberseguridad con la estrategia empresarial, un elemento clave (entre muchos) para construir resiliencia. Estos ejercicios también ayudan a aclarar el valor de la ciberseguridad para la organización. ¿Es principalmente un generador de ingresos, un protector de ingresos o está enfocada en evitar disrupciones y los costos que estas generan? La planificación de escenarios debe avanzar a un ritmo que coincida con la rápida evolución de las amenazas que enfrenta la organización.

PARADOJA #5

Los presupuestos de ciberseguridad se mantienen estables año con año.

El entorno de ciberseguridad es profundamente inestable.

Gasto constante, estable y respaldado

Los encuestados que pueden presentar el caso de negocio para realizar una inversión probablemente asegurarán el financiamiento que necesitan.

"Cuando hay una justificación buena, bien pensada y un caso de negocio sólido, generalmente se aprueba el financiamiento", dijo el CIO Global de una empresa del sector salud. Se espera que los presupuestos de ciberseguridad aumenten exponencialmente durante el próximo año, con pocos cambios significativos en su distribución entre las prioridades del negocio, quizá debido a inversiones planificadas a varios años y a la propiedad compartida entre las funciones de negocio, TI y gestión de riesgos. Los líderes que invierten en iniciativas de ciberseguridad tienen mucha más probabilidad que sus pares de esperar resultados comerciales tangibles, especialmente en estas áreas:

- Eficiencia, agilidad y estrategia.
- Confianza, seguridad y resiliencia.
- Valor para el cliente.

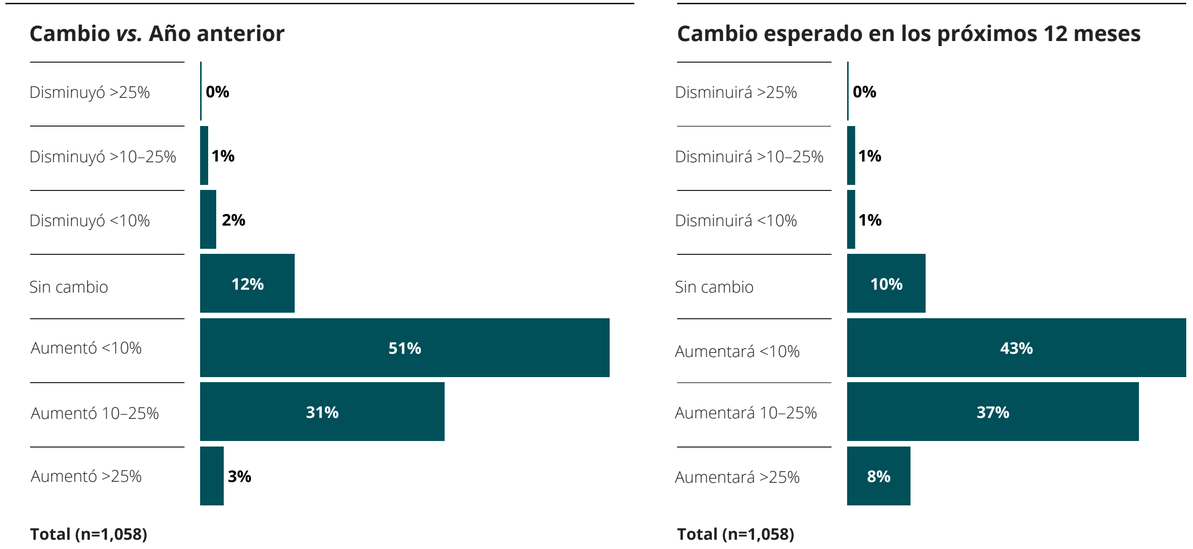
Más del 90% de los líderes destacados anticipan avances en cada área. Una fuerte mayoría de los encuestados (85%) informa que han incrementado sus presupuestos de ciberseguridad año tras año, y aún más (88%) planean aumentarlos en los próximos 12 meses. Para algunos, estos incrementos son significativos: El ocho por ciento de los encuestados espera que los niveles de gasto a 12 meses aumenten más del 25%, y más de un tercio anticipa incrementos de entre 10% y 25% del presupuesto total de ciberseguridad de sus organizaciones en la actualidad, incluyendo TI, negocio, riesgo empresarial y otras fuentes. Es notable que los encuestados anticipan que las fuentes del presupuesto[1] se mantendrán relativamente estables durante los próximos 12 a 24 meses, concentrándose en:

PRESUPUESTO CENTRAL DE TI	NEGOCIOS	RIESGO EMPRESARIAL
43%	30%	26%

Nota [1]: los totales pueden no sumar 100% debido al redondeo. Además, la participación restante corresponde a "Otros".

Presupuesto de ciberseguridad de la organización

Pregunta a: En comparación con el último año fiscal, ¿cuánto cambió el presupuesto total de ciberseguridad de su organización (incluyendo TI y cualquier otra fuente)?
Pregunta b: Piensa en los próximos 12 meses, usted espera que el presupuesto de ciberseguridad de su organización (incluyendo TI y cualquier otra fuente) ...



Casi todos los encuestados han presupuestado inversiones de ciberseguridad a varios años; solo un 7% no lo hace y se enfocan en un ciclo de un solo año. “Nuestros programas suelen ser de 2 a 3 años, pero los presupuestos se aprueban año con año”, comentó el CIO Global de una empresa de salud. “Tengo aspiraciones a largo plazo, y los programas pueden ser de largo plazo, pero los presupuestos siguen estableciéndose cada año”.

Dentro de los planes multianuales, la mayor parte del presupuesto de ciberseguridad (61%) se extiende por 1 a 2 años.

Un año más allá del ciclo actual corresponde al:

35% **del presupuesto de ciberseguridad.**

Dos años más allá del ciclo actual corresponden al:

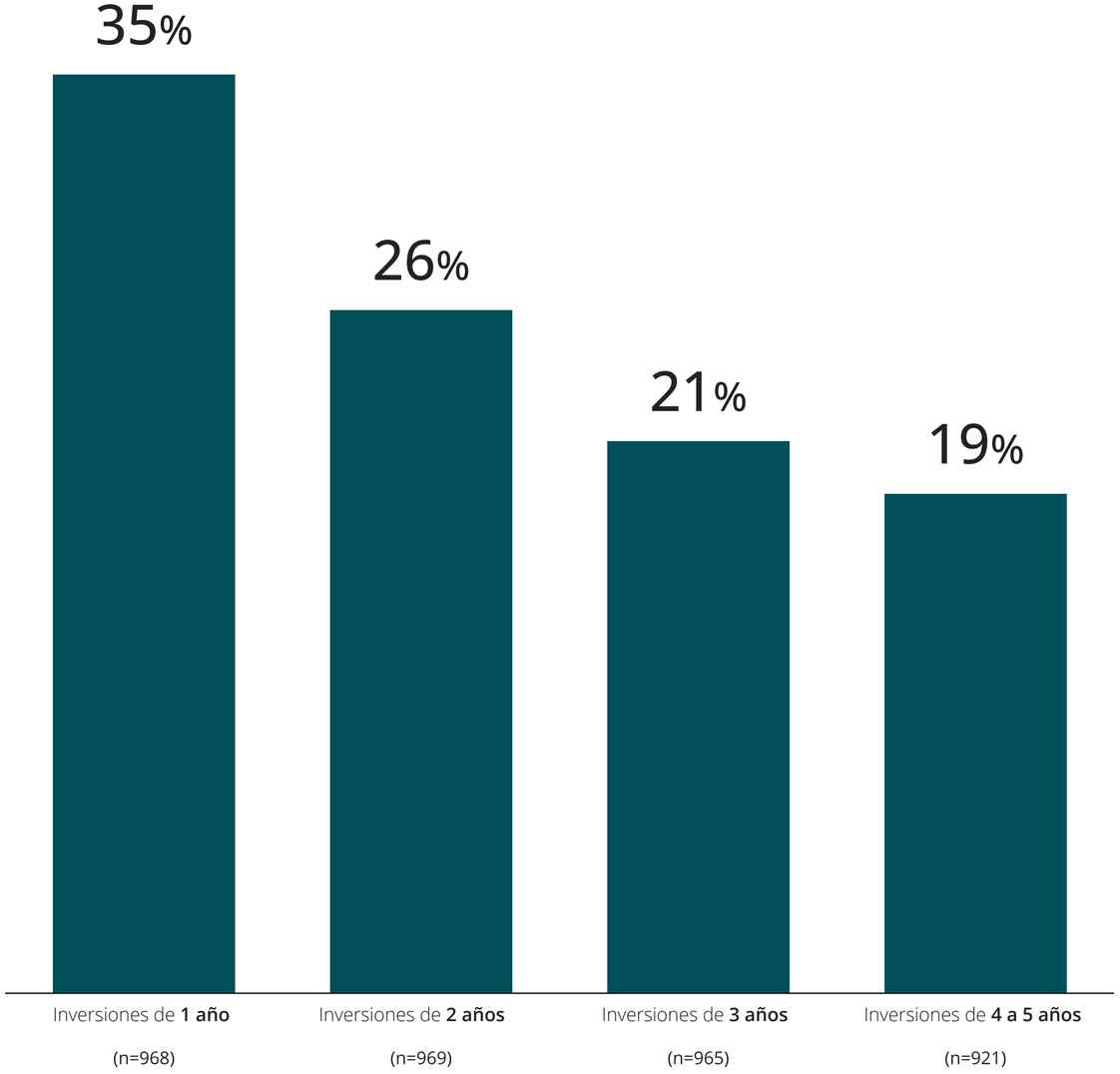
26% **del presupuesto de ciberseguridad.**

El diecinueve por ciento del presupuesto de ciberseguridad está asignado a inversiones multianuales para los próximos 4 a 5 años.

Las prioridades a nivel de programa no cambian de manera significativa, y tampoco las categorías de gasto. De hecho, los encuestados indican que sus asignaciones presupuestarias actuales serán idénticas el próximo año, con la detección y respuesta a amenazas a la cabeza con un 20%. Después de eso, la seguridad de la infraestructura; la seguridad de datos, identidad y aplicaciones; y la estrategia, gobernanza y cumplimiento son las categorías principales de gasto, en ese orden.

> “Cuando existe una justificación buena y bien pensada, y un caso de negocio sólido, **normalmente se consigue el financiamiento.”**
>
> **— CIO Global, Sector Salud**

Asignación del presupuesto de ciberseguridad a inversiones multianuales*
Pregunta: ¿Qué porción del presupuesto de ciberseguridad de este año está explícitamente vinculada a inversiones multianuales?



*Nota: excluye a quienes no tienen inversiones multianuales (n=71).

PARADOJA #5

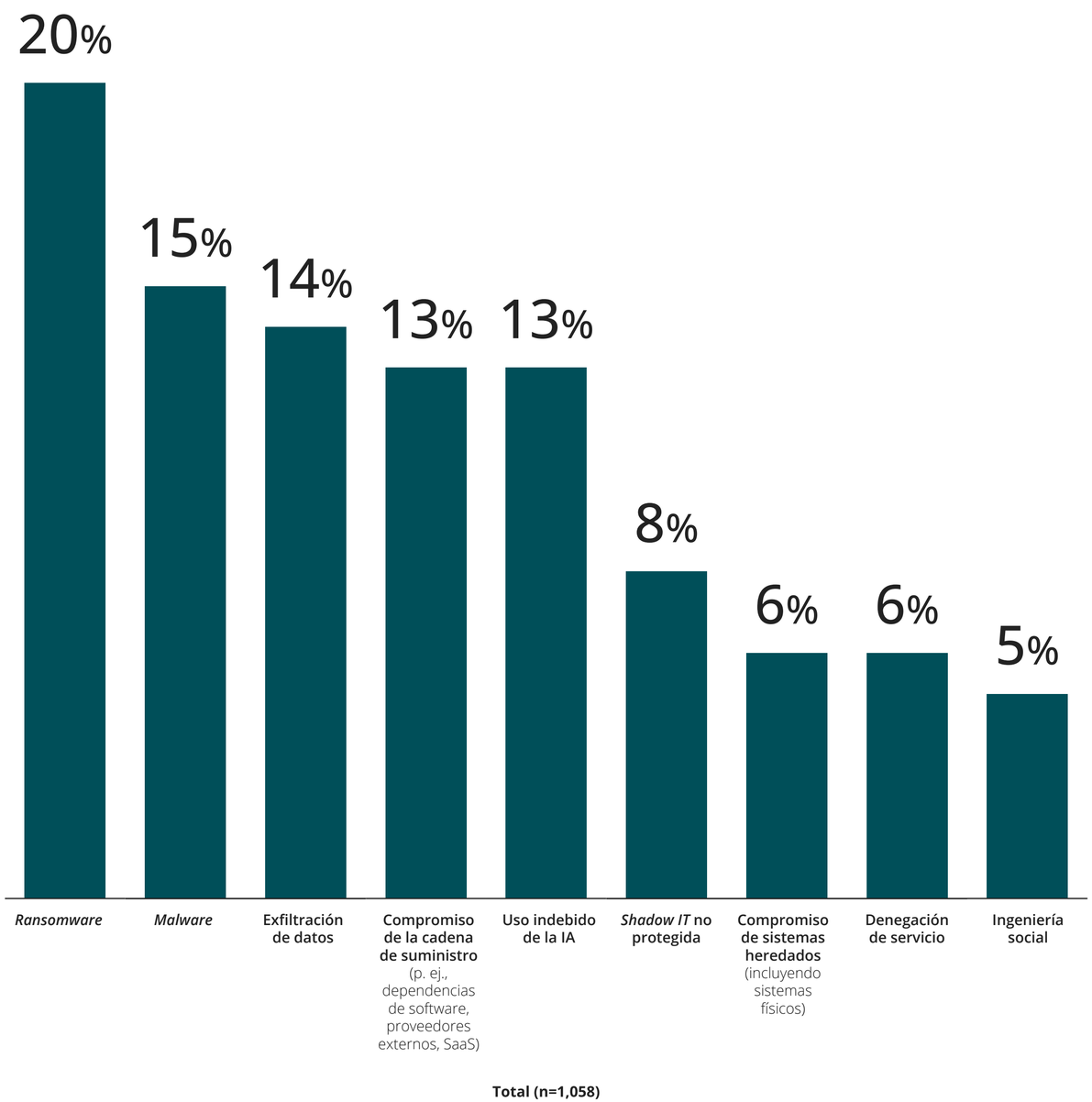
El panorama cibernético es cualquier cosa menos estable y predecible

Considere qué tan rápido ha cambiado ya el panorama cibernético debido únicamente a un factor: el rápido avance de las capacidades de la IA generativa. Hace apenas dos o tres años, pocos hablaban seriamente de la necesidad de realizar inversiones inmediatas en capacidades de IA generativa, y mucho menos de actuar en consecuencia. Hoy, casi tres cuartas partes (72 %) de los encuestados han incorporado nuevos enfoques de razonamiento generativo en sus capacidades de IA existentes en casi una docena de iniciativas de ciberseguridad. Este fue un desarrollo impredecible y en gran medida no planificado que prácticamente ningún presupuesto estático podría haber previsto.

Las amenazas también cambian. Por ejemplo, el "uso indebido de la IA" no aparecía en la lista de amenazas identificadas por los encuestados hace apenas tres años. Ahora es una de las cinco principales preocupaciones, junto con el *ransomware*, el *malware* y la exfiltración de datos. Aplicar controles tradicionales a la IA no es suficiente. Por ejemplo, los sistemas de IA no deterministas requieren salvaguardas altamente específicas para defenderse de amenazas como el *prompt hacking*. Esto representa un nuevo nivel de complejidad que las organizaciones deberían abordar hoy.

> **"Nuestros programas suelen durar de 2 a 3 años, pero los presupuestos se asignan año con año.** Tengo aspiraciones a largo plazo, y los programas pueden ser de largo plazo, pero los presupuestos todavía se establecen cada año."
>
> **— CIO Global, Sector Salud**

Fuente de amenaza de ciberseguridad más preocupante – Herramientas / Técnicas
P. ¿Cuál es la mayor fuente de amenaza de ciberseguridad que más preocupa a su organización?



Total (n=1,058)

Desentrañando la paradoja

Es natural que cualquier organización busque previsibilidad y estabilidad, especialmente si se trata de presupuestos.

Se entiende ampliamente que los presupuestos de tecnología en general deberán cambiar de manera significativa debido a la naturaleza rápidamente cambiante de los avances tecnológicos. Pero incluso en ese contexto, las inversiones en defensas cibernéticas son diferentes, dado el potencial profundamente disruptivo de los riesgos cibernéticos. Por ejemplo, aunque la adopción de IA se considera ampliamente como una fuente de mayor eficiencia y menores costos en la mayoría de las áreas de la organización, en los entornos de ciberseguridad podría tener el efecto contrario, ya que los actores de amenazas aprovechan la IA a su favor de nuevas maneras. Los líderes de ciberseguridad pueden optimizar sus presupuestos de ciberseguridad que usan IA, pero también podrían necesitar aumentar su uso de manera considerable para defenderse de una gama de amenazas en evolución.

¿Cómo pueden lograrlo si están sujetos a niveles de financiación estables y predecibles (por envidiable que este escenario pueda parecer?

Construir flexibilidad en el presupuesto de ciberseguridad

Piense en esto como financiar lo inesperado: reservar, por ejemplo, entre el 10% y el 20% del presupuesto anual de ciberseguridad para realizar inversiones ágiles en nuevas capacidades a medida que surjan, o para responder a amenazas impredecibles a medida que se desarrollen.

Repensar la presupuestación a varios años

¿Qué pasa si los presupuestos plurianuales son simplemente demasiado restrictivos? Considere adoptar pronósticos continuos *(rolling forecasts)* o enfoques de presupuestación continua como alternativas a las estrategias estándar de presupuestos multianuales.

Cambiar la mentalidad de presupuestación

Es posible que los líderes financieros de su organización y los responsables de decisiones presupuestarias no comprendan totalmente los desafíos únicos que la ciberseguridad presenta para la planificación presupuestaria. Si es así, puede ser momento de un cambio de mentalidad organizacional: una oportunidad para informar a estos líderes sobre el panorama cibernético y desarrollar conjuntamente enfoques innovadores para la presupuestación. Los líderes de ciberseguridad son capaces de cuantificar los riesgos cibernéticos que enfrenta la organización en términos financieros, estas conversaciones pueden adquirir mayor urgencia y enfoque. Por ejemplo, si una parte de la organización tiene un perfil de riesgo más alto que otras —con un impacto financiero potencialmente mayor— puede justificarse una inversión más significativa en esa área.

El lado positivo de la paradoja

Las paradojas reveladas en esta encuesta muestran nuevas oportunidades: quienes logren resolverlas se colocarán en posición de cerrar la brecha entre la visión y la ejecución.

Muchas de las condiciones necesarias para detonar este tipo de cambio transformador en la estrategia y la ejecución de ciberseguridad ya están presentes hoy. Quienes son responsables de dirigir la estrategia general entienden la importancia de la ciberseguridad para alcanzar los principales objetivos de la organización, y están listos para respaldar las estrategias de ciberseguridad con una financiación sólida. Mientras tanto, los CISOs y otros líderes con responsabilidades de ciberseguridad han cultivado cuidadosamente las estrategias, los procesos y las estructuras necesarias para defender a sus organizaciones frente a una creciente ola de amenazas cibernéticas.

Ahora es el momento de combinar todos estos elementos clave de una manera que cree un mecanismo de cultura cibernética aún más fuerte, de amplio alcance y verdaderamente integrado, listo para los desafíos futuros. Esto requerirá un agente de cambio y, si está leyendo este informe, es probable que ese rol le corresponda.

Comience por observar su organización a través del lente de las paradojas que hemos identificado aquí, determina cuáles son las más relevantes para la organización y trabaje con sus colegas para resolverlas.

Si desea analizar más a fondo los detalles de esta investigación, discutir cualquiera de los hallazgos del informe o explorar más a fondo su posible impacto en su organización y sus objetivos, estaremos encantados de ayudarle.

Autores

Diana Kearns-Manolatos

Emily Mossburg

Kelly Nelson

Iram Parveen

Agradecimientos

Volker Burgers

Evan Carvouni

Jonathan Chan

Tim Corder

Felix De Andres

Miguel Olias De Lima

Jason Frame

Javier Francisco

John Gelinne

Tanneasha Gordon

Rob Jacoby

Jimmy Joseph

Daphne Lucas

Tara Mahoutchian Mortazie

David Mapgaonkar

Jeffrey Minick

Stephanie Montalvo

Will Nelson

Jose Pela Neto

Sean Peasley

Anand Raghawa Prasad

Frank Santucci

Jennifer A. Sullivan

Contactos

Emily Mossburg

Deloitte Global Cyber Leader
Principal, Deloitte & Touche LLP
emossburg@deloitte.com
+1 571 766 7048

Adnan Amjad

US Cyber Leader
Partner, Deloitte & Touche LLP
aamjad@deloitte.com
+1 713 982 4825

Daphne Lucas

Canada Cyber Leader
Partner, Deloitte Canada
dlucas@deloitte.ca
+1 403 267 1737

Xavier Gracia

Spain Cyber Leader
Partner, Deloitte Spain
xgracia@deloitte.es
+34 931697257

Jose Pela Neto

Brazil Cyber Leader
Partner, Deloitte Brazil
jpela@deloitte.com
+55 11 5186 6396

Yuichiro Kirihara

Japan Cyber Leader
Partner, Deloitte Japan
ykirihara@tohmatsu.co.jp
+81 803 3672805

Paula Alvarez

S-LATAM Cyber Leader
Partner, Deloitte Mexico
palvarez@deloittemx.com
+52 55 5080 6558 ext: 6558

Niels van de Vorle

North and South Europe Cyber Leader
Partner, Deloitte Netherlands
nvandevorle@deloitte.nl
+31 88 2882186

Marius von Spreti

Central Europe Cyber Leader
Partner, Deloitte Germany
mvonspreti@deloitte.de
+49 89 290365999

Metodología

La 5ª edición de la encuesta *Deloitte Global Future of Cyber* se basa en datos de 1,058 líderes de negocios y tecnología en 43 países, que abarcan 5 industrias y 23 sectores.

El análisis también incluye entrevistas ejecutivas con 9 líderes del C-*suite* que tienen conocimiento sobre tendencias de ciberseguridad.

El informe de la encuesta de este año incluye tres categorías para los encuestados, basadas en sus niveles de confianza y preparación:

Frontrunners (Líderes) obtuvieron las puntuaciones más altas en cuanto a sentirse algo/muy confiados en preguntas relacionadas tanto con la confianza en ciberseguridad como con acciones de preparación, que abarcan temas como:

- Uso de herramientas de cuantificación de riesgos para medir el impacto de las inversiones en ciberseguridad.
- Grado en el que se abordan los riesgos de terceros en su cadena de suministro digital.
- Desarrollo de un plan de respuesta a incidentes de ciberseguridad que se actualiza y prueba anualmente.
- Alineación entre las prácticas de ciberseguridad y los estándares y prácticas específicos de la industria.
- ...y muchos más

Followers **(Seguidores)** obtuvieron puntajes en el rango medio para estas mismas preguntas sobre confianza y preparación en ciberseguridad.

Foundation builders **(Constructores de base)** reflejaron los niveles más bajos de confianza y/o preparación.

Este índice de confianza y acción en ciberseguridad determiná cuántas de las 15 acciones de ciberseguridad un encuestado realiza en gran medida, y en cuántas de las 8 estrategias de ciberseguridad se siente muy confiado.

Alineación empresarial insuficiente

Preparación para la implementación — P1

Si la respuesta de un encuestado coincidía en gran medida / completamente en:

10-15 acciones .....se les asignaba un peso de 3.
4-9 acciones .....se les asignaba un peso de 2.
0-3 acciones .....se les asignaba un peso de 1.

Confianza — P2

Si la respuesta de un encuestado coincidía con sentirse muy confiado en:

5-8 estrategias .....se les asignaba un peso de 3.
3-4 estrategias .....se les asignaba un peso de 2.
0-2 estrategias .....se les asignaba un peso de 1.

Cálculo combinado
Ambos pesos se sumaron para obtener un cálculo total de confianza e implementación de estrategias y acciones de ciberseguridad.

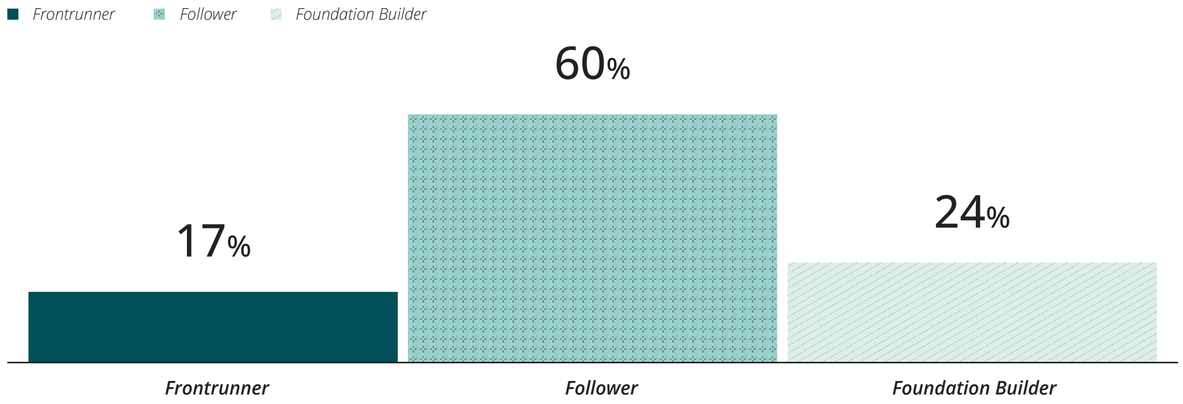
Si un encuestado obtuvo una puntuación total de **5–6**, fue clasificado como ***Frontrunner*** **(Líder).**

Si obtuvo una puntuación total de **3–4**, fue clasificado como ***Follower*** **(Seguidor).**

Si obtuvo una puntuación total de **2**, fue clasificado como ***Foundation Builder*** **(Constructor de base).**

Los *Frontrunners* son quienes han dominado la primera paradoja de este informe. Sus experiencias ofrecen información valiosa sobre las acciones que las organizaciones pueden tomar para abordar con éxito las demás paradojas identificadas.

Índice de confianza e implementación (% del total)*



*Nota: los porcentajes pueden no sumar exactamente 100% debido a ajustes por redondeo, dicha discrepancia es esperada y no representa un error.

Tabla (N = 1,058)

Categoría	*Frontrunner*	*Follower*	*Foundation Builder*
Suma de pesos	5-6	3-4	2
Base	176	631	251
Porcentaje del total de la muestra	17%	60%	24%