¿Cómo reducir las brechas para lograr la Ciberresiliencia? El manual de estrategias para los altos ejecutivos

Conclusiones del informe Global Digital Trust Insights 2025

pwc

2%

de los encuestados a nivel global ha implementado acciones de ciberresiliencia en toda su organización.

25%

de los CISO colombianos participan, en gran medida, en actividades comerciales clave**. A nivel Global, esta cifra asciende al 37 %.**

13%

de los encuestados refiere **una brecha de confianza entre los CISO/CSO y los CEO** con respecto al **cumplimiento de las regulaciones de IA y a la resiliencia.**

Dado que la superficie de ataque continúa expandiéndose debido a los avances en la inteligencia artificial, **los dispositivos conectados y las tecnologías en la nube, así como a un sistema regulatorio en constante cambio; lograr ciberresiliencia a nivel empresarial es fundamental.** No obstante, a pesar de la consciencia generalizada de los desafíos que lo anterior presenta, continúan presentándose brechas significativas.

Para proteger a sus organizaciones, **los ejecutivos deben tratar la ciberseguridad como un tema permanente en la agenda empresarial, incorporándola en cada decisión estratégica y exigiendo la colaboración de los altos ejecutivos.**

La encuesta Global Digital Trust Insights 2025 de PwC, aplicada a 4.042 ejecutivos de empresas y líderes de tecnología de setenta y siete países, reveló brechas importantes que las empresas deben superar antes de lograr la ciberresiliencia.

Brechas en la implementación de la ciberresiliencia: a pesar de las crecientes preocupaciones sobre el riesgo de ciberseguridad, solo el 2 % de los ejecutivos dice que su empresa ha implementado acciones de ciberresiliencia en toda la organización.

Brechas en la preparación: las organizaciones se sienten menos preparadas para abordar las amenazas a la seguridad que más les preocupan, como los riesgos relacionados con la nube y las filtraciones por parte de terceros.

Brechas en la participación de los CISO: menos de la mitad de los ejecutivos encuestados dice que sus CISO están involucrados, en gran medida, en la planificación estratégica, los informes a la Junta y la supervisión de las implementaciones de tecnología.

Brechas en la confianza en el cumplimiento normativo: los CEO y los CISO tienen diferentes niveles de confianza en la capacidad de su empresa para cumplir con las regulaciones, en particular con respecto a la inteligencia artificial, la resiliencia y la infraestructura crítica.

Brechas en la medición del riesgo de ciberseguridad: aunque los ejecutivos reconocen la importancia de medir el riesgo de seguridad, menos de la mitad lo hace de manera efectiva y solo el 15 % valora el impacto financiero de estos riesgos en una medida significativa.

Todo esto advierte de la necesidad de promover una mejor colaboración entre los altos ejecutivos, así como una inversión estratégica para fortalecer la ciberresiliencia. Al abordar estos desafíos, superar las brechas y hacer de la ciberseguridad una prioridad empresarial, los ejecutivos pueden construir un puente hacia un futuro más seguro. Los CISO pueden ayudar a alcanzar este resultado compartiendo conocimientos basados en la tecnología y explicando las prioridades en la seguridad en términos empresariales (costo, oportunidad y riesgos).

Contenidos

4

Cuantificación del riesgo de seguridad
¿Cómo liberar el potencial de la cuantificación del riesgo de ciberseguridad? ¿Qué frena a las organizaciones?

5

Inversión y prioridades en materia de ciberseguridad
Invertir en resiliencia, generar confianza

6

Estrategia y liderazgo digital
¿Tu estrategia y liderazgo digital impulsan una resiliencia real?

Perspectivas de amenazas y riesgos emergentes

Navegando por las amenazas digitales: establecer una visión compartida para la preparación

Más de la mitad

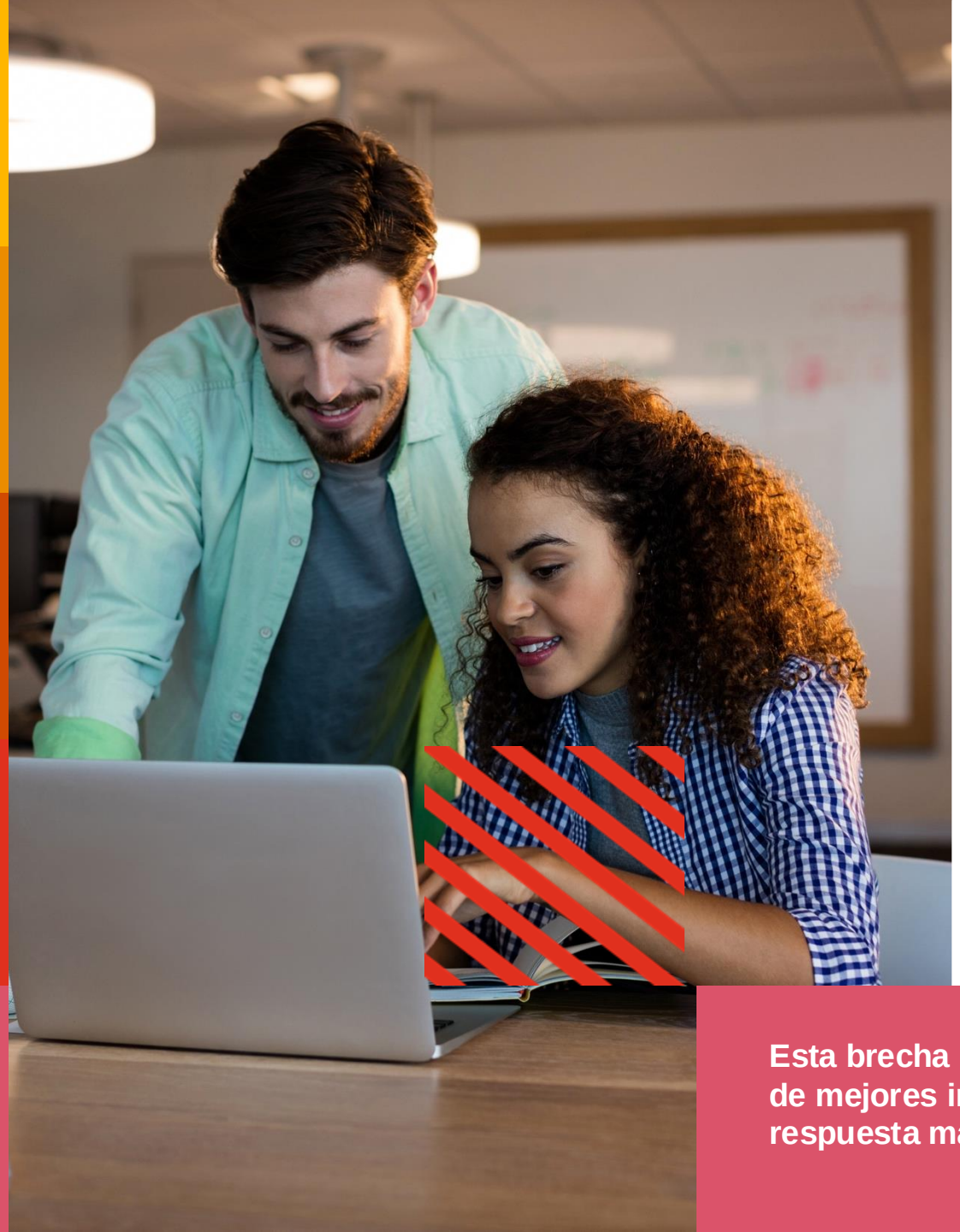
de los líderes en Colombia y en el mundo **está priorizando los riesgos digitales, tecnológicos y de ciberseguridad** por encima de los riesgos relacionados con la situación económica. .

51%

de los ejecutivos en Latinoamérica (42 % a nivel global) **clasifica las amenazas relacionadas con la nube como su amenaza digital más preocupante.**

Top 2 amenazas

los ataques a la nube y a los productos conectados son las amenazas para los que los ejecutivos en todo el mundo **se sienten menos preparados para abordar.**



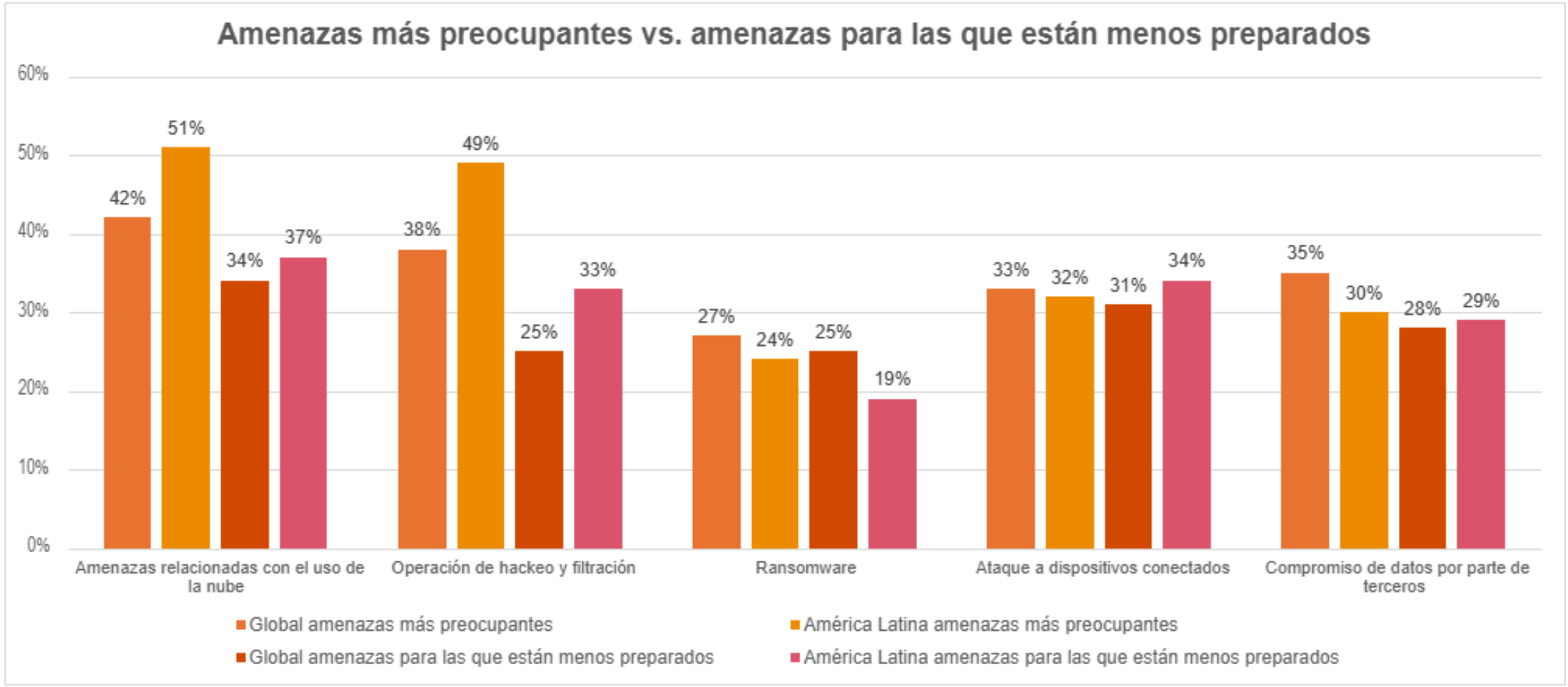
Mientras el panorama de la ciberseguridad continúa evolucionando**, las organizaciones se enfrentan a amenazas cada vez más volátiles e impredecibles.** Una superficie de ataque en expansión, impulsada por una mayor dependencia de la nube, la IA, los dispositivos conectados y terceros, exige un enfoque ágil y de resiliencia en toda la empresa. Alinear las prioridades y la preparación de la organización es esencial para mantener la seguridad y la continuidad del negocio.

Sin preparación para las amenazas más preocupantes

Lo que más preocupa a las organizaciones es aquello para lo que están menos preparadas. **Las cuatro amenazas digitales más preocupantes en Latinoamérica y a nivel global (amenazas relacionadas con la nube, operaciones de piratería informática y fuga de información, infracciones de terceros y ataques a productos conectados) son las mismas que los ejecutivos de seguridad se sienten menos preparados para abordar.**

Esta brecha resalta la necesidad urgente de mejores inversiones y capacidades de respuesta más sólidas.

Existe, además, **una brecha a nivel global de percepción entre los ejecutivos de seguridad y el resto de la organización**, ya que los CISO y CSO tienen mayores probabilidades de clasificar el *ransomware* entre las tres amenazas más preocupantes. Esto puede reflejar su función, dado que el *ransomware* es más central para las tareas de ciberseguridad/de TI y, quienes desempeñan esa función, probablemente comprenden mejor las vulnerabilidades que sus pares comerciales. **Lo anterior refuerza aún más la importancia de un intercambio de información más eficaz entre los equipos de liderazgo para alinear las prioridades.**



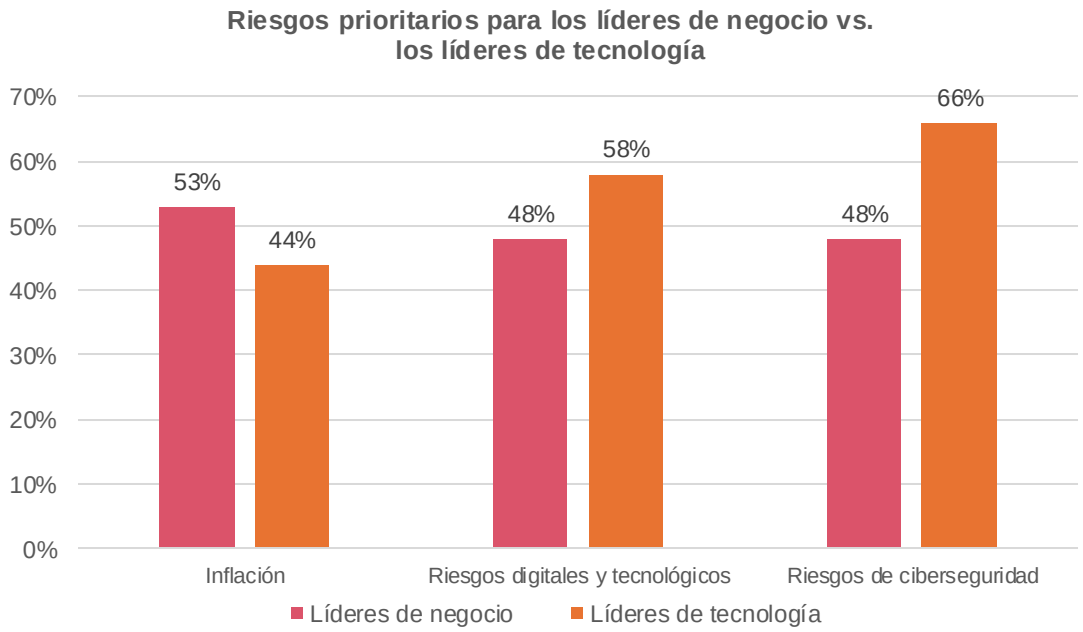
Fuente: Global Digital Trust Insights 2025

Llamada a la acción

Es esencial contar con una estrategia de inversión en ciberseguridad que tenga en cuenta las amenazas, priorice las inversiones en los riesgos de seguridad digital más urgentes y observe más de cerca en dónde se están concentrando los recursos en términos de personas, procesos y capacidades de defensa.

La división estratégica: prioridades empresariales y tecnológicas

Los ejecutivos de empresas y los ejecutivos de tecnología priorizan riesgos diferentes. **Mientras que los primeros están más preocupados por la inflación, los segundos clasifican los riesgos de ciberseguridad como su prioridad debido, probablemente, a su proximidad al panorama de amenazas en este campo.** Aun así, casi la mitad de los ejecutivos de empresas todavía clasifican los riesgos digitales entre sus tres principales preocupaciones, lo que subraya su importancia crítica. **Esta preocupación compartida representa una oportunidad para que los CISO conecten la agenda de ciberseguridad con la agenda empresarial.**



Fuente: Global Digital Trust Insights 2025

Llamada a la acción

Ejecutivos de empresas y tecnología: es hora de ponerse de acuerdo**. Equilibren la priorización de los riesgos de seguridad con las presiones económicas**, para ayudar a proteger los activos y crear resiliencia. Las evaluaciones interdisciplinarias periódicas mantendrán sincronizadas sus estrategias y sus prioridades.

El costo máximo que han experimentado los líderes de empresas en Latinoamérica por las filtraciones de datos se encuentra entre 1 millón y 9,9 millones de dólares.

Más de una cuarta parte de los ejecutivos a nivel global dijeron que la filtración de datos más perjudicial que sufrieron en los últimos tres años le costó a su organización al menos 1 millón de dólares. Esta cifra es ligeramente inferior a la que se indicó en la encuesta del año pasado, que se realizó en organizaciones de todos los tamaños y en la mayoría de las regiones y sectores. **En general, se estima que la filtración de datos promedio en el mundo asciende a 3,32 millones de dólares.**

A nivel global, entre los mejores resultados identificamos que, aquellos líderes, que respondieron que su organización tiene más probabilidades de demostrar prácticas de ciberseguridad de alta calidad de manera habitual, fueron menos propensos a sufrir filtraciones de datos en los últimos tres años. Los mejores resultados suelen pertenecer a organizaciones más grandes y de mayor crecimiento, cuyos presupuestos en ciberseguridad se prevé que aumenten en un 15 % o más el próximo año**, lo que indica que la madurez y la financiación de los programas de ciberseguridad se correlacionan con una mayor resiliencia.**

No te detengas en tu viaje hacia la ciberseguridad y la resiliencia. Los delincuentes y los actores de los estados nacionales se están volviendo expertos en encontrar fisuras: controles de identidad y acceso débiles, dispositivos sin parches y configuraciones de seguridad erróneas.

Rob Joyce
Investigador sénior en materia de ciberseguridad, riesgos y normativas, PwC US, exasistente especial del presidente y asesor interino de Seguridad Nacional.

Llamada a la acción

Es necesario priorizar **estrategias integrales de mitigación de riesgos que abarquen la prevención, la detección, la respuesta y la recuperación**, así como entender los impactos más amplios de una vulneración de seguridad (más allá del daño financiero) **para generar una verdadera resiliencia.**

Llamado a la acción de los ejecutivos

A medida que las organizaciones se enfrentan a un panorama de amenazas más sofisticado**, es importante que los ejecutivos de todos los niveles asuman un papel proactivo en la evaluación de los riesgos actuales y emergentes.** Al alinear las estrategias de ciberseguridad con objetivos empresariales más amplios, los ejecutivos pueden preparar mejor a sus organizaciones para gestionar el riesgo y generar resiliencia.

CISO: deben recalcar al resto de los altos ejecutivos las amenazas que más ponen en peligro su negocio, especialmente si es necesario reorientar los esfuerzos de inversión.

CIO y directores de tecnología (CTO): deben sostener conversaciones con los ejecutivos de riesgo (CRO) y evaluar cómo ciertas amenazas pueden atentar contra la seguridad de la información y la infraestructura en general. Por otro lado, identificar qué amenazas plantean las mayores barreras para la resiliencia.

CFO: deben obtener una visión más profunda del CISO y el CRO sobre las prioridades de inversión y gestión en ciberseguridad más críticas.

CEO: deben reunirse periódicamente con el CRO y el CISO para comprender los vectores de amenazas que más les preocupan. Deben asegurarse de recibir informes periódicos sobre las medidas de mitigación de amenazas actuales.

Junta directiva: debe comprender los principales riesgos a la seguridad para la organización y plantear las preguntas difíciles a la Gerencia. ¿Cómo se están mitigando los riesgos? ¿Contamos con los planes y la financiación adecuados para abordar los riesgos de manera proactiva y responder en caso de que ocurra un evento?

Tecnologías emergentes y GenAI

GenAI y tecnología emergente:
equilibrio entre oportunidades y riesgos

58%

de los **ejecutivos de seguridad en Latinoamérica** (68 % a nivel global) dicen **que GenAI ha aumentado su superficie de ataque** durante el último año.

72%

de los **líderes en Latinoamérica** (78 % a nivel global) **han aumentado su inversión en GenAI** en los últimos doce meses.

72%

de los **líderes mundiales** ha aumentado su inversión en gestión de riesgos en la gobernanza de la IA.

Si bien el rápido avance de la IA generativa (GenAI) está gestando nuevas oportunidades en todas las industrias, también representa riesgos para ciberseguridad. A medida que las organizaciones adoptan GenAI y otras tecnologías emergentes, los directivos deben abordar vectores de ataque más complejos e impredecibles, obstáculos de integración y la naturaleza de doble filo de GenAI, tanto en la ciberdefensa como en la ofensiva. **Detrás de estos desafíos hay importantes problemas legales y de datos que pueden complicar la implementación y la gobernanza de GenAI.**

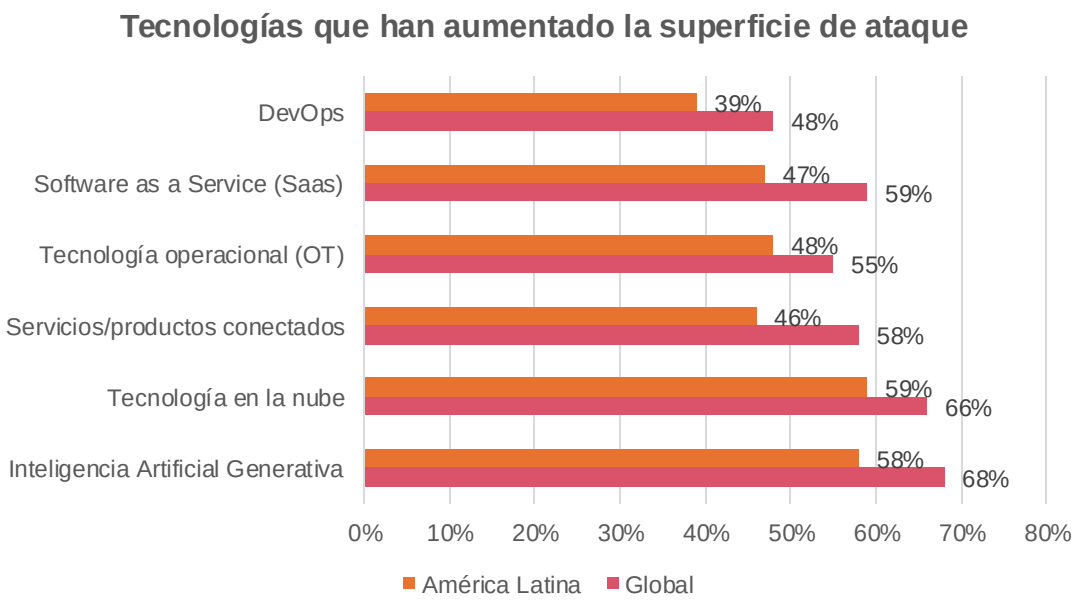
La ciberseguridad es, en su mayoría, un problema de ciencia de datos. Es cada vez más necesario que los defensores de la seguridad aprovechen el poder de la inteligencia artificial generativa y el aprendizaje automático para acercarse a los datos y generar información oportuna y práctica que sea de suma importancia.

Michael Elmore
director de seguridad de la información
global de GSK

Una superficie de ataque en evolución

Los ejecutivos de seguridad informan que GenAI (57 % en Latinoamérica y 68 % a nivel global) y las tecnologías en la nube (64 % en Latinoamérica y 66 % a nivel global) **ampliaron la superficie de ataque durante el año pasado, lo que hace que las empresas sean más vulnerables a amenazas sofisticadas.** GenAI también puede reducir las barreras de entrada para actores de amenazas menos sofisticados, lo que les permite diseñar ataques de *phishing* y *deepfakes* efectivos a gran escala. Esto coincide con los hallazgos de nuestra 27.ª Encuesta Anual Global de CEO, en la que el 64 % de los CEO a nivel mundial estuvo de acuerdo en que es probable que GenAI aumente el riesgo de ciberseguridad en su organización. **El uso de GenAI también genera inquietudes sobre la integridad de los datos, la privacidad y el cumplimiento normativo,** ya que las empresas se enfrentan a obligaciones regulatorias que aún están evolucionando.

Asimismo, están ampliando la superficie de ataque de otras tecnologías, como los dispositivos conectados y la Tecnología Operativa (OT), que afectarán, a nivel global, a sectores como el industrial, salud y energía. **A medida que más dispositivos se interconectan, la seguridad de estos sistemas se vuelve más difícil.** Además, aunque la computación cuántica todavía está en el horizonte, el 42 % de los ejecutivos de seguridad informan que ya les ha hecho abordar vulnerabilidades.



Fuente: Global Digital Trust Insights 2025

Llamada a la acción

La evaluación continua de nuevas vulnerabilidades; **la inversión en medidas de seguridad avanzadas; y el fomento de una colaboración más estrecha entre los equipos de tecnología, seguridad, riesgos y asuntos legales, son fundamentales.** Al estar preparadas para estas amenazas, las empresas pueden proteger mejor sus activos críticos y mantener la confianza de las partes interesadas.

Aprovechar GenAI para la ciberdefensa: oportunidades y desafíos

Si bien GenAI está aumentando la superficie de ataque de riesgo en ciberseguridad para la mayoría de las organizaciones, los ejecutivos también están utilizando esa misma tecnología para la ciberdefensa. Las tres formas principales en que están aprovechando GenAI incluyen la detección y respuesta ante amenazas, la inteligencia sobre amenazas y la detección de *malware/phishing*. No obstante, a pesar de estas oportunidades, las organizaciones enfrentan varios obstáculos al incorporar GenAI en sus estrategias de ciberdefensa, como los que se referencian a continuación:

- **Dificultad para integrarse con sistemas/procesos existentes** (39 % tanto para Latinoamérica como para global);
- **Falta de confianza en GenAI** en relación a las partes interesadas internas (36 % para Latinoamérica y 39 % para global);
- **Controles internos y gestión de riesgos inadecuados** (37 % para Latinoamérica y 38 % para global);
- **Falta de políticas internas estandarizadas** que regulen su uso (40 % para Latinoamérica y 37 % para global)
- **La implementación de una gobernanza de datos** (37 % para Latinoamérica y 35 % para global).

Llamada a la acción

GenAI puede transformar las defensas, pero solo si supera los desafíos de integrarla, confiar en ella y gobernarla de manera eficaz, aplicando prácticas de IA responsables. De lo contrario, corre el riesgo de quedarse atrás en la carrera contra los actores de amenazas.

GenAI lidera las prioridades de inversión en ciberseguridad

Al reconocer el aumento de los riesgos en la seguridad digital**, el 72 % de los líderes en Latinoamérica y el 78 % a nivel global, ha incrementado su inversión en GenAI para la ciberseguridad, centrándose especialmente en la mejora de la infraestructura para la región (la gobernanza para global).** Esta inversión en GenAI subraya la importancia de gestionar tanto sus capacidades como sus riesgos.

Las empresas también están empezando a invertir en el aprendizaje automático —*o machine learning* — y en robots. Si bien la computación cuántica es un campo en donde los líderes están poniendo su atención, todavía faltan años para que esta se adopte; **existe actualmente una necesidad imperiosa de desarrollar tecnologías resistentes a la tecnología cuántica para combatir las amenazas futuras que plantee esta tecnología en manos equivocadas.**

Llamada a la acción

Invertir en GenAI es solo el comienzo. **Haz que la situación cambie para ayudar a que tus defensas superen las amenazas en evolución.** Explora aún más el potencial sin explotar otras tecnologías, así como las soluciones resistentes a la tecnología cuántica.

Llamado a la acción de los ejecutivos

A medida que las tecnologías emergentes están rediseñando el panorama de la ciberseguridad, **es fundamental que todos los altos ejecutivos asuman un papel activo a la hora de guiar a sus organizaciones** a través de las oportunidades y los riesgos que presentan estas innovaciones.

CISO: deben ayudar a impulsar la estandarización en todo el sector tecnológico para integrar la IA En la ciberdefensa. Asimismo, hacer cumplir los derechos de acceso de cada usuario para identificar posibles vectores de ataque.

CIO y CTO: deben desarrollar una evaluación del impacto de la IA, para informar a los ejecutivos de negocios acerca de dónde tiene más sentido implementarla e invertir. Deben preparar la infraestructura para la escalabilidad a medida que crece el uso de GenAI.

CFO: deben trabajar con el CISO para priorizar la seguridad y confidencialidad de la protección de datos financieros.

Directores de datos (CDO): deben mejorar sus protocolos de gobernanza, evaluar los riesgos asociados a las leyes y reglamentos que protegen la privacidad de los datos.

Directores jurídicos (CLO) y asesores jurídicos generales (GC): deben colaborar con otros equipos de riesgo y cumplimiento para proteger a la organización de usos secundarios indebidos de los datos y una posible exposición legal.

Evolución normativa

Un mundo digital altamente regulado: ¿están realmente preparadas las empresas?

94%

de los líderes latinoamericanos (96 % a nivel global) informan **que las regulaciones de ciberseguridad los han impulsado a aumentar su inversión en los últimos doce meses.**

80%

de los encuestados en Latinoamérica (78 % a nivel global) cree que **las regulaciones han ayudado a desafiar,** mejorar o aumentar su postura en materia de ciberseguridad.

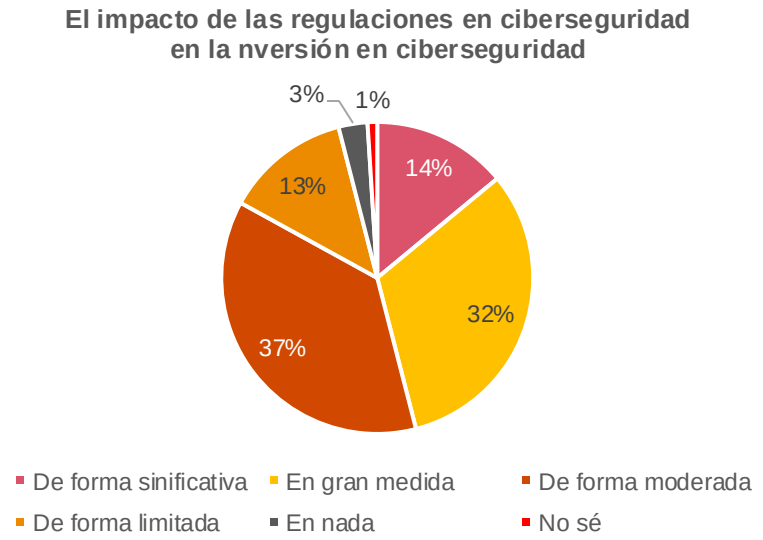
Hay un 13%

de brecha de confianza entre los CISO/CSO y los CEO, a nivel global, con respecto al cumplimiento de las regulaciones de IA y la resiliencia.

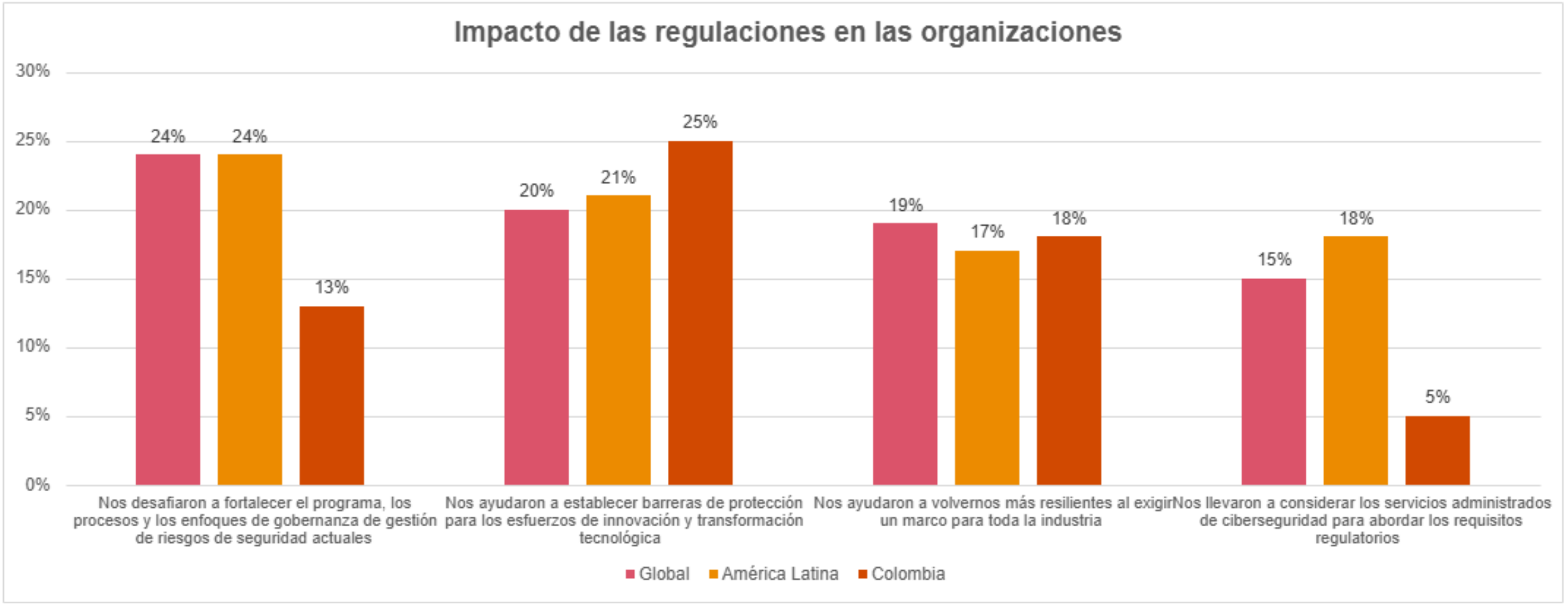
Los marcos regulatorios exigen a las empresas que cumplan rápidamente con una gama cada vez mayor de requisitos. Una oleada de nuevas regulaciones (DORA, Ley de ciberresiliencia, Ley de Inteligencia Artificial, CIRCIA, Ley de Ciberseguridad de Singapur, etc.) subraya la urgencia de que las organizaciones adapten sus prácticas a estas mayores expectativas. A medida que las empresas de todo el mundo abordan estas demandas, se enfrentan a una brecha crítica en la confianza entre los CISO/CSO y los CEO, con respecto a su capacidad para lograr el cumplimiento total. Abordar estos desafíos es esencial para construir una postura de ciberseguridad resiliente y compatible que pueda soportar tanto el escrutinio regulatorio como las amenazas emergentes.

Las regulaciones en ciberseguridad están impulsando un cambio positivo

Las regulaciones están demostrando ser un importante impulsor de la inversión en ciberseguridad: **el 94 % de los ejecutivos latinoamericanos (96 % a nivel global) reconoce que los requisitos regulatorios los ha impulsado a mejorar sus medidas de seguridad.** Además, el 80 % (78 % a nivel global) cree que las regulaciones han ayudado a cuestionar, mejorar o incrementar su postura en materia de ciberseguridad. Esto indica que, a pesar de las dificultades de cumplimiento, las regulaciones están ayudando a desarrollar aún más las capacidades de ciberseguridad en todas las industrias.



Fuente: Global Digital Trust Insights 2025



Fuente: Global Digital Trust Insights 2025

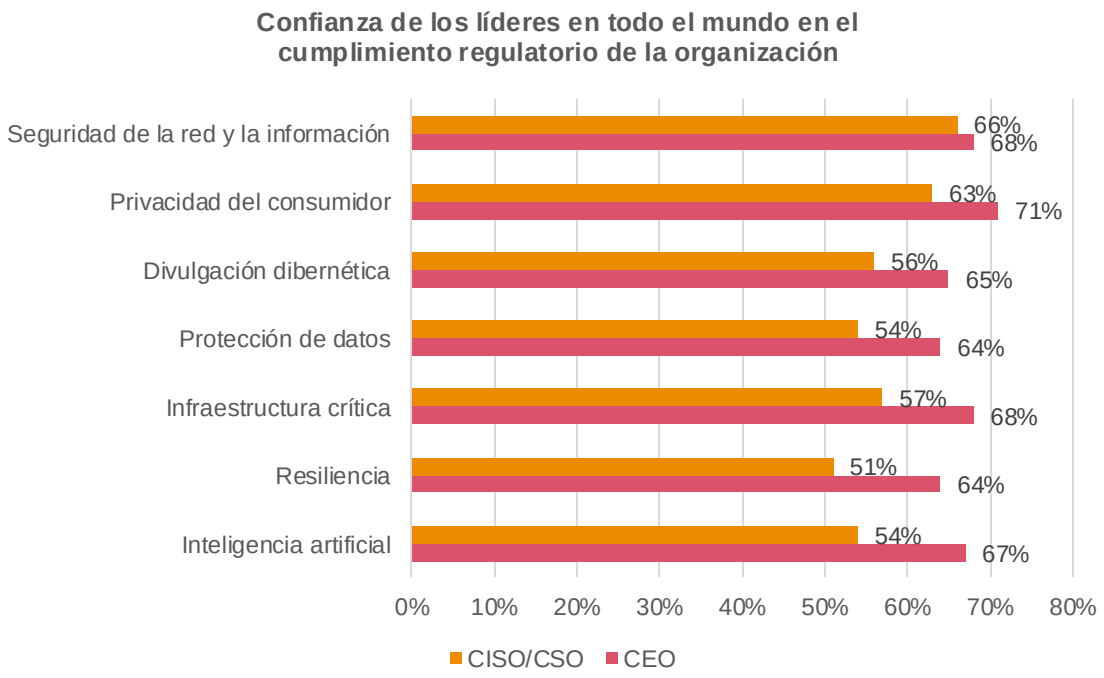
Llamada a la acción

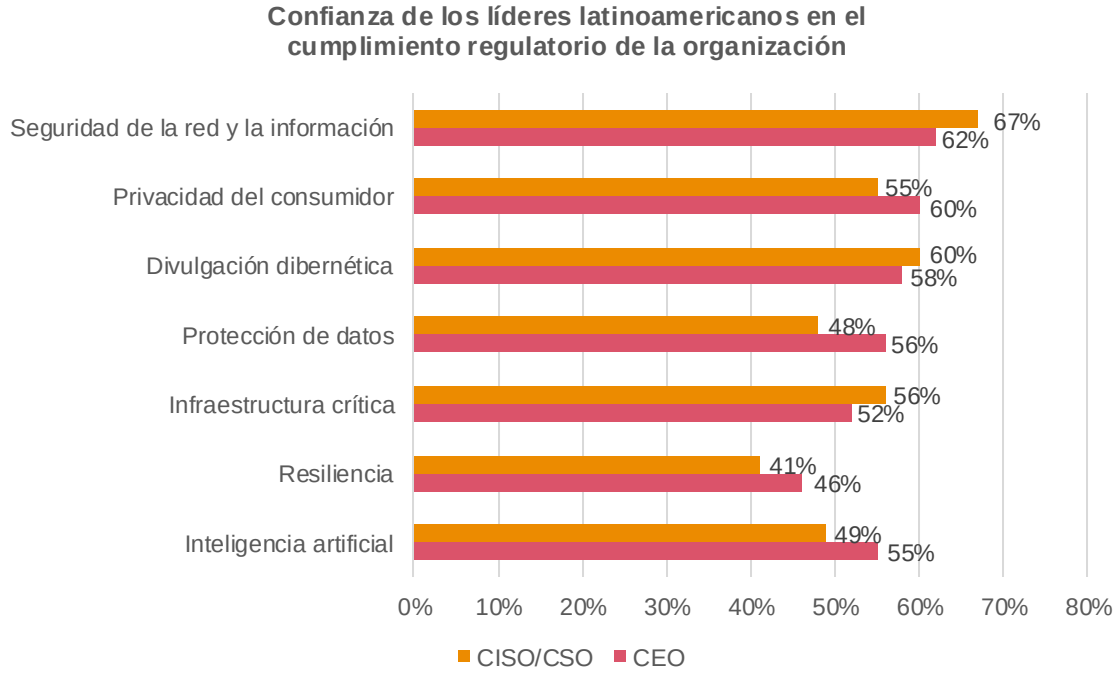
Las organizaciones que adoptan los requisitos normativos **suelen beneficiarse de marcos de seguridad más sólidos y de una postura más resistente frente a las amenazas emergentes.** El cumplimiento normativo no debería verse como un ejercicio para acatar requisitos, sino como una oportunidad para generar resiliencia y confianza a largo plazo con las partes interesadas.

Brecha de confianza a nivel mundial: los CISO se sienten menos seguros que los CEO sobre el cumplimiento de las regulaciones en materia de Ciberseguridad

A pesar de la creencia de que las regulaciones están ayudando a la organización, existe una diferencia significativa entre la confianza de los CEO y los CISO/CSO en su capacidad para cumplir con estas. **Las brechas más grandes involucran el cumplimiento de los requisitos de IA, resiliencia e infraestructura crítica.** Los CISO, que están en la primera línea de la ciberseguridad, son menos optimistas que los CEO sobre la capacidad de su organización para cumplir con los requisitos regulatorios.

Dado que los CISO son más conscientes de las dificultades operativas cotidianas, las limitaciones de recursos y las posibles vulnerabilidades que pueden obstaculizar el cumplimiento de las normas, es fundamental que comuniquen estos riesgos de manera eficaz al equipo de liderazgo. ¿Qué lo impide? **Los obstáculos potenciales incluyen barreras que limitan la participación de los CISO en las decisiones estratégicas, así como la dificultad para justificar la inversión necesaria en la gestión de los riesgos de seguridad.**





Fuente: Global Digital Trust Insights 2025

Llamada a la acción

Para superar la brecha de confianza es necesario mejorar la coordinación y la comunicación entre los líderes de seguridad y los altos ejecutivos. **Los CEO deben asegurarse de que los CISO no solo sean escuchados, sino que también cuenten con los recursos y el apoyo necesarios para cumplir con las exigencias regulatorias**. Los CISO deben brindar información respaldada por datos y presentar argumentos comerciales para elevar el cumplimiento normativo a un imperativo estratégico.

Llamado a la acción de los ejecutivos

A medida que los requisitos regulatorios continúan dando forma al panorama de la ciberseguridad, **es esencial que los altos ejecutivos se mantengan a la vanguardia en temas de problemas de cumplimiento normativo mientras se apalancan en las regulaciones como catalizador de la innovación.** Establecer una alineación entre los equipos de seguridad, las funciones de riesgo y el liderazgo ejecutivo es crucial para garantizar la preparación en pro del cumplimiento normativo y, así, impulsar mejoras estratégicas.

CISO y CRO: deben brindar informes frecuentes a otros líderes ejecutivos sobre el estado de las regulaciones que impactan directamente en las respectivas necesidades de la industria o territorio, y trabajar para implementar procesos de gestión de cambios tecnológicos y regulatorios.

CFO: deben verificar la precisión, integridad y capacidad de defensa de toda la información reglamentaria sobre la gestión de riesgos digitales y la postura del programa. Desarrollar una comprensión clara de la materialidad y el impacto específico de un incidente, incorporando la cuantificación del riesgo digital, para evaluar y comunicar con precisión los riesgos potenciales.

CEO: deben comprender las responsabilidades de supervisión para orientar los esfuerzos de cumplimiento, incluida la coordinación necesaria entre las diferentes unidades de negocio. Deben identificar las preguntas clave que deben formular los CISO para cerrar cualquier brecha de conocimiento sobre la postura de cumplimiento.

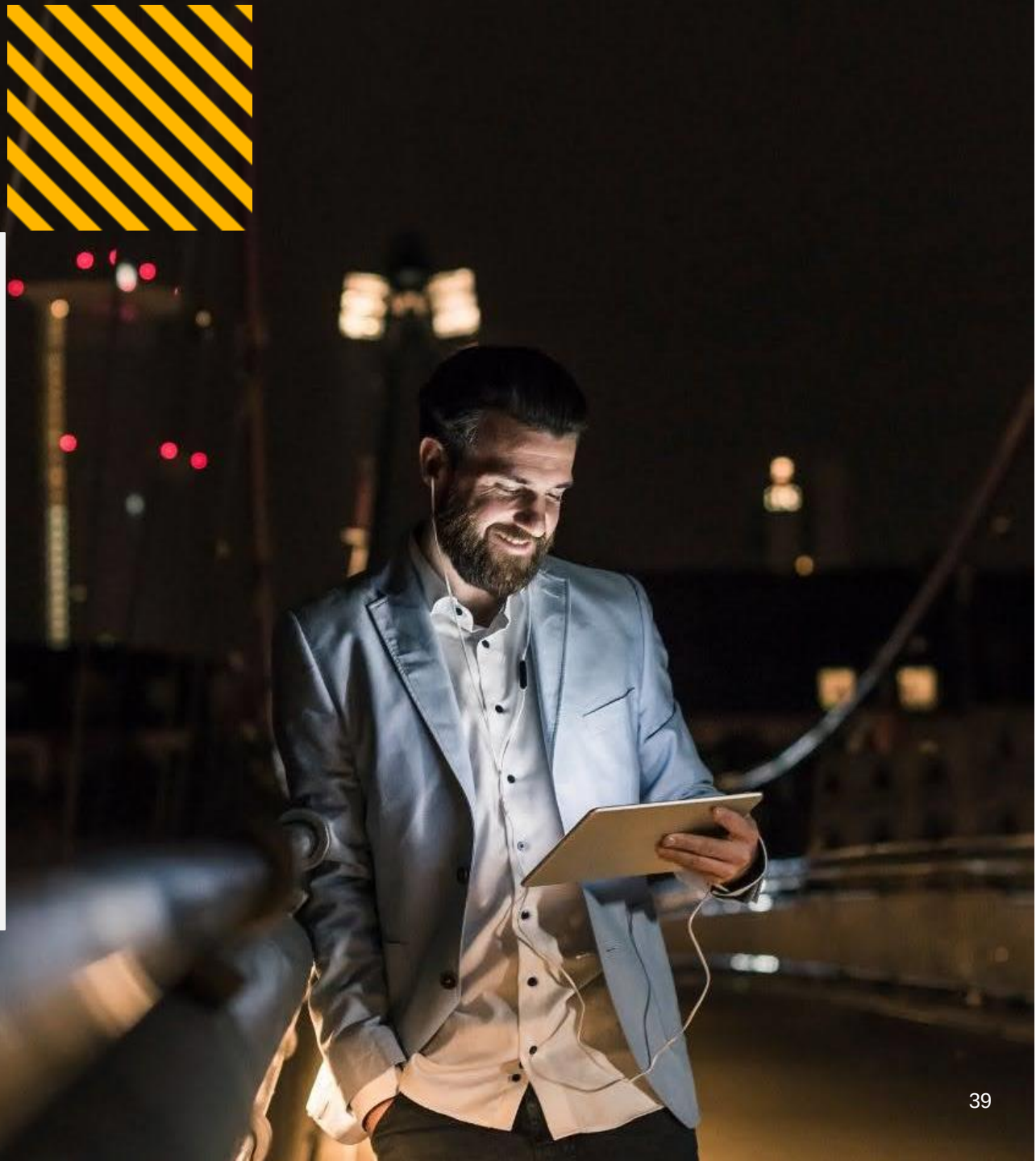
Directores de cumplimiento: deben mantenerse al tanto de los requisitos de cumplimiento normativo y colaborar con el CISO y el CRO para incorporar medidas proactivas y monitoreo para confirmar periódicamente el cumplimiento.

CLO y GC: deben determinar la cantidad correcta de detalles de divulgación necesarios para cumplir con las obligaciones de informes del programa de ciberseguridad, logrando un equilibrio entre transparencia y confidencialidad.

Junta directiva: debe mantenerse informado acerca de los requisitos normativos vigentes y solicitar la opinión de la dirección sobre las medidas proactivas que se están adoptando como preparación para los nuevos requisitos. Comprender el enfoque de la dirección para evaluar y divulgar los incidentes cibernéticos.

Cuantificación del riesgo Digital

¿Cómo liberar el potencial de la cuantificación del riesgo digital?
¿Qué frena a las organizaciones?



19%

de los líderes en Latinoamérica (15 % a nivel global) están **valorando en gran medida el impacto financiero de los riesgos digitales.**

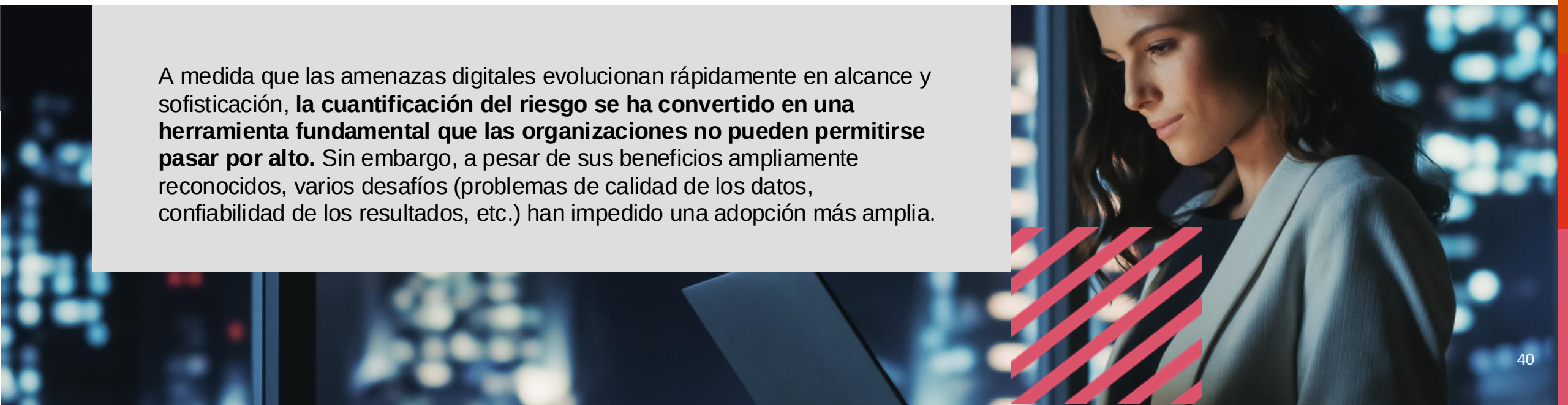
92%

de los líderes en Latinoamérica (87 % a nivel global) dicen que **es de suma importancia asignar recursos a las zonas de mayor riesgo.**

41%

de los líderes en Latinoamérica (44 % a nivel global) dicen que los problemas de datos son uno de los principales desafíos a los que se enfrenta cuando se cuantifica el impacto financiero del riesgo de seguridad.

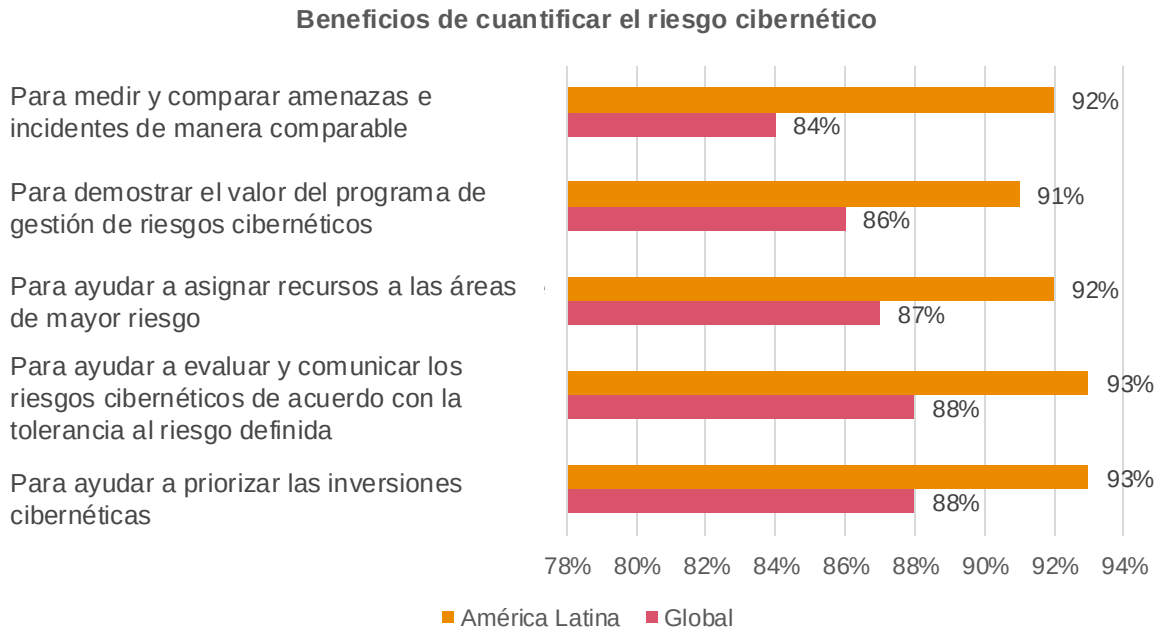
A medida que las amenazas digitales evolucionan rápidamente en alcance y sofisticación, **la cuantificación del riesgo se ha convertido en una herramienta fundamental que las organizaciones no pueden permitirse pasar por alto.** Sin embargo, a pesar de sus beneficios ampliamente reconocidos, varios desafíos (problemas de calidad de los datos, confiabilidad de los resultados, etc.) han impedido una adopción más amplia.



La medición del riesgo es fundamental pero limitada

Si bien los ejecutivos coinciden en gran medida en que valorar el riesgo es crucial para priorizar la inversión en gestionarlo (92 % en Latinoamérica y 87 % a nivel global) y asignar recursos a las áreas de mayor riesgo (92 % en Latinoamérica y 87 % a nivel global), solo el 19 % (15 % a nivel global) de las organizaciones realmente lo está haciendo en una medida significativa (por ejemplo, cuantificación extensa del riesgo con automatización e informes exhaustivos).

En el caso de las organizaciones a nivel global que sí miden el riesgo, **siete de cada diez ejecutivos indican que utilizan evaluaciones de la postura de seguridad para cuantificar el riesgo residual teniendo en cuenta la eficacia de los controles clave,** como el cumplimiento de la corrección de vulnerabilidades, las revisiones de acceso de los usuarios y la finalización de la formación. **No obstante, la adopción de prácticas de cuantificación de riesgos de seguridad más holísticos sigue siendo limitada.**



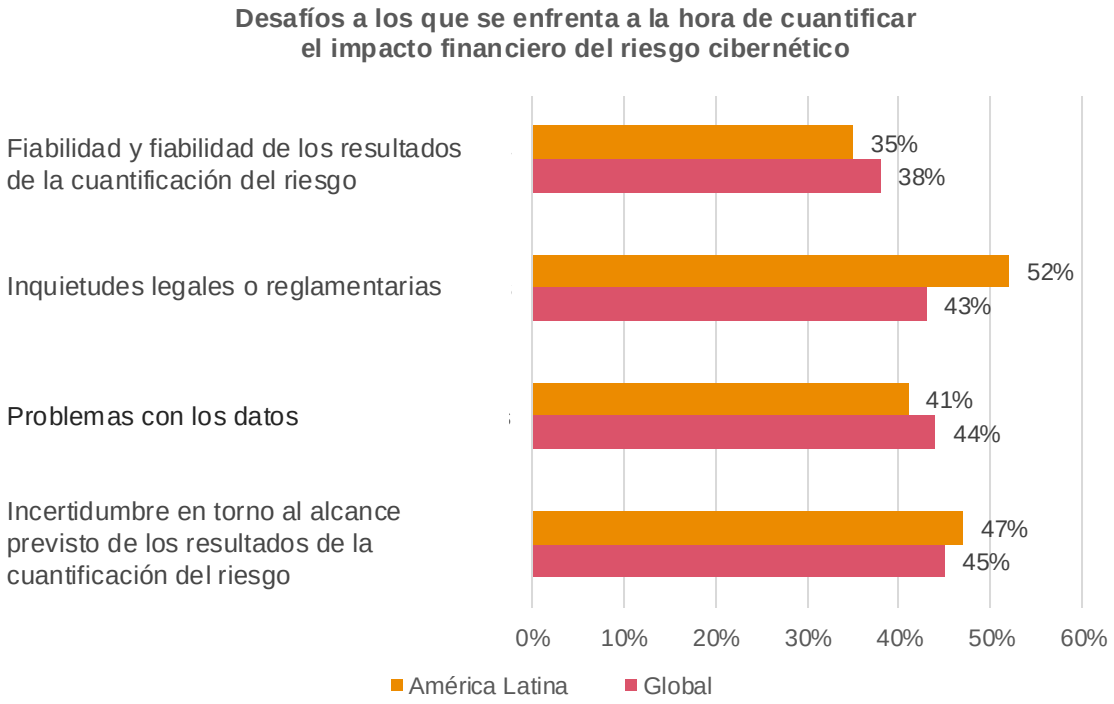
Fuente: Global Digital Trust Insights 2025

Llamada a la acción

Es hora de aprovechar todo el potencial de la cuantificación del riesgo de seguridad. **La brecha entre el reconocimiento y la implementación es una oportunidad perdida que ya no se puede ignorar.** Las organizaciones que no miden el riesgo o que no han desarrollado plenamente esta capacidad, están desaprovechando información fundamental, en particular cuando se trata de fundamentar las decisiones de la Junta directiva y la asignación de capital.

¿Cuáles son los obstáculos para una implementación más amplia?

Los problemas de datos, la incertidumbre sobre el alcance y las preocupaciones legales ocupan los primeros lugares de la lista de obstáculos para implementar la cuantificación del riesgo de ciberseguridad, tanto en Latinoamérica como a nivel global. **La falta de confianza en la fiabilidad de los resultados de la cuantificación es otro de los obstáculos.** Otro factor que complica aún más la adopción es la brecha entre lo que esperan los altos ejecutivos y lo que ofrecen los CISO, dado que la medición del riesgo digital requiere una alineación entre los ejecutivos de seguridad y el apetito de riesgo de la empresa.



Fuente: Global Digital Trust Insights 2025

Llamada a la acción

Las barreras para la adopción de la cuantificación del riesgo de seguridad pueden estar obstaculizando el progreso. **Las organizaciones no pueden permitir que los desafíos obstaculicen la toma de decisiones críticas;** Es necesario abordar estos obstáculos de frente, generar confianza en la cuantificación del riesgo digital e integrarla por completo en el proceso estratégico.

Llamado a la acción de los ejecutivos

Establecer un sistema confiable de cuantificación de riesgos **es fundamental para tomar decisiones informadas y priorizar inversiones estratégicas.** Al medir con precisión el riesgo, los ejecutivos pueden alinear las iniciativas de ciberseguridad con los objetivos empresariales más amplios.

CISO: deben comenzar gradualmente, con un resultado específico en mente. Aprovechar la información que tiene dentro de su organización (por ejemplo, eficacia de los controles, madurez, datos de incidentes o pérdidas). Las nuevas herramientas pueden ayudar con la cuantificación de riesgos, pero no son un requisito. Definir el programa y buscar tecnologías habilitadoras para respaldar lo que se ha diseñado.

CISO y CRO: deben mostrar a los ejecutivos de alto nivel los resultados de medición de riesgo financiero más impactantes obtenidos a partir de herramientas y prácticas de cuantificación. Estos ejemplos pueden ayudar a persuadir a los líderes para que prioricen y asignen los recursos adecuados a las áreas de mayor riesgo.

CEO: deben trabajar con su CISO y CRO para obtener una comprensión más profunda del valor comercial de la cuantificación del riesgo de seguridad, así como los costos potenciales y las oportunidades perdidas al no medir los riesgos.

Junta directiva: debe comprender los métodos que utiliza actualmente la organización para evaluar el riesgo. Presionar a la gerencia respecto a sus planes de implementar de manera más amplia la cuantificación del riesgo, con el fin de evaluar e informar mejor sobre la postura de riesgo digital de la empresa.

Inversión y prioridades en materia de ciberseguridad

Invertir en resiliencia, generar confianza

65%

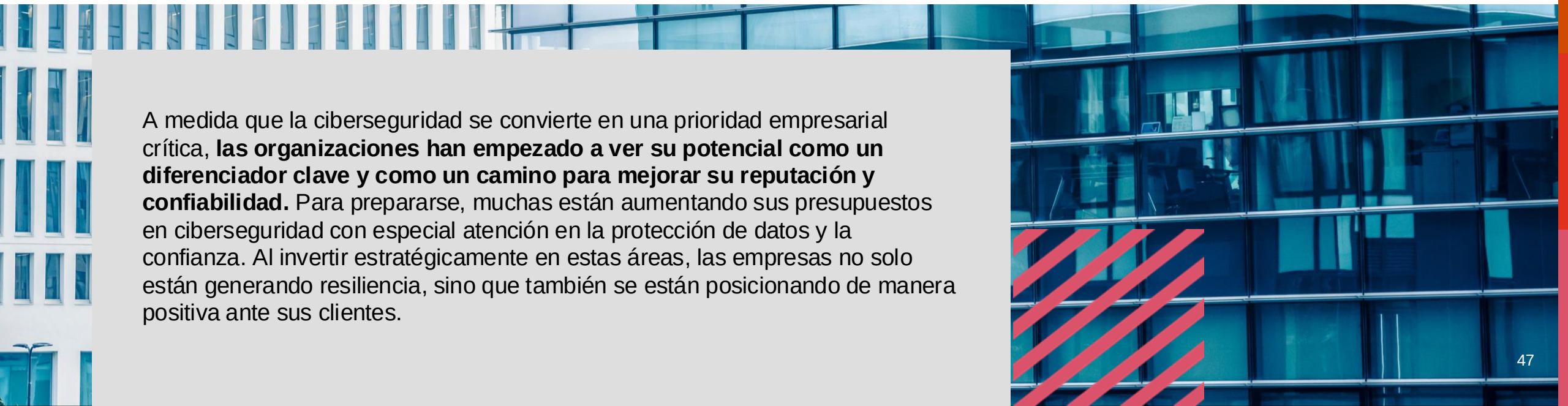
de líderes colombianos (77% a nivel global) esperan que **su presupuesto de ciberseguridad aumente el próximo año.**

67%

de los ejecutivos de empresas colombianas **priorizan la modernización de la tecnología y su infraestructura** como la principal inversión en seguridad durante el próximo año.

41%

de los ejecutivos de tecnología latinoamericanos (34 % a nivel global) p**riorizan la seguridad en la nube** como la principal inversión durante el próximo año.

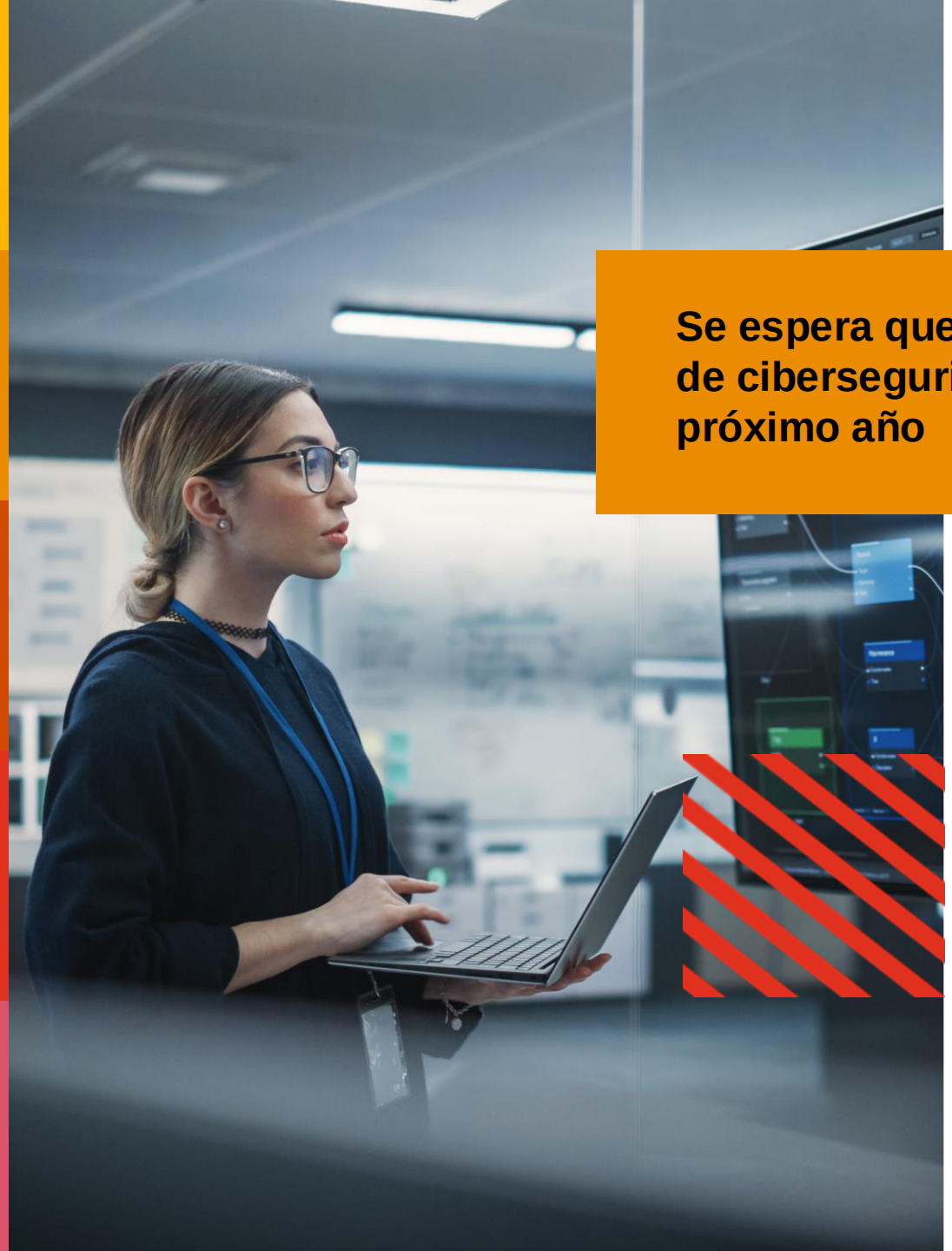


A medida que la ciberseguridad se convierte en una prioridad empresarial crítica, **las organizaciones han empezado a ver su potencial como un diferenciador clave y como un camino para mejorar su reputación y confiabilidad.** Para prepararse, muchas están aumentando sus presupuestos en ciberseguridad con especial atención en la protección de datos y la confianza. Al invertir estratégicamente en estas áreas, las empresas no solo están generando resiliencia, sino que también se están posicionando de manera positiva ante sus clientes.

El panorama de amenazas es cada vez más impredecible ya que estamos viendo amenazas multi-vector a entornos físicos y digitales. Estamos invirtiendo recursos en capacidades integradas de respuesta y recuperación para mejorar la seguridad física y la ciberseguridad.

Los actores de amenazas no hacen distinción. Necesitamos estar preparados en todos los niveles con nuestros programas de resiliencia y continuidad empresarial.

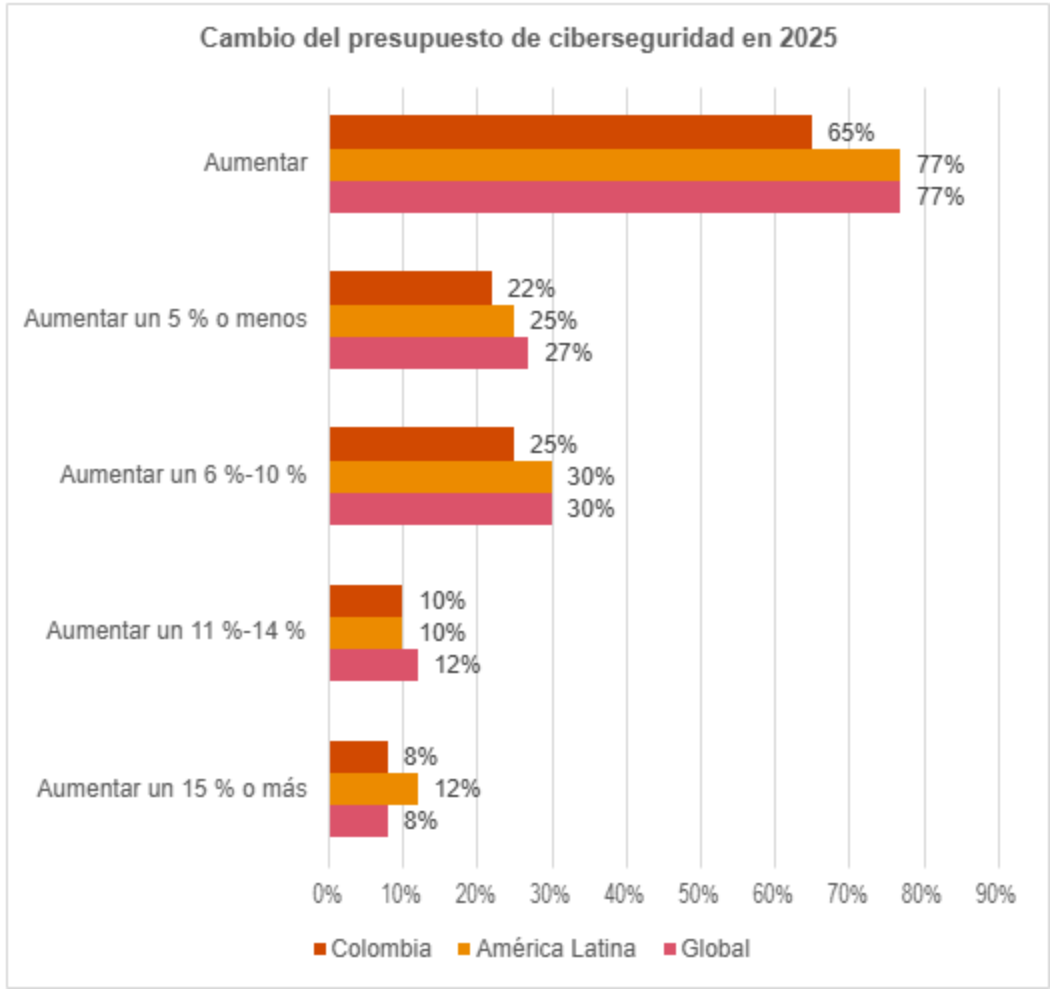
Dr. Georg Stamatelopoulos
director general de En BW AG



Se espera que los presupuestos de ciberseguridad aumenten el próximo año

En términos globales, los presupuestos en materia de ciberseguridad **se mantienen en línea con los del año pasado**, y las organizaciones más pequeñas invierten un porcentaje mayor de sus recursos en comparación con las organizaciones más grandes. **Esto probablemente refleja que las organizaciones más pequeñas están tratando de ponerse al día en áreas en las que las empresas más grandes ya han invertido mucho.** Las organizaciones más grandes, aunque expresan inquietudes sobre las amenazas emergentes y la resiliencia, están adoptando un enfoque más mesurado en sus inversiones, probablemente debido a que cuentan con marcos de seguridad más establecidos.

Más de la mitad (más de tres cuartas partes para global) de los ejecutivos colombianos **esperan que el presupuesto de ciberseguridad de su organización aumente el próximo año.** Esa cifra es mayor (82 %) en el caso de las organizaciones de Norteamérica y del sector de tecnología, medios y telecomunicaciones (TMT).



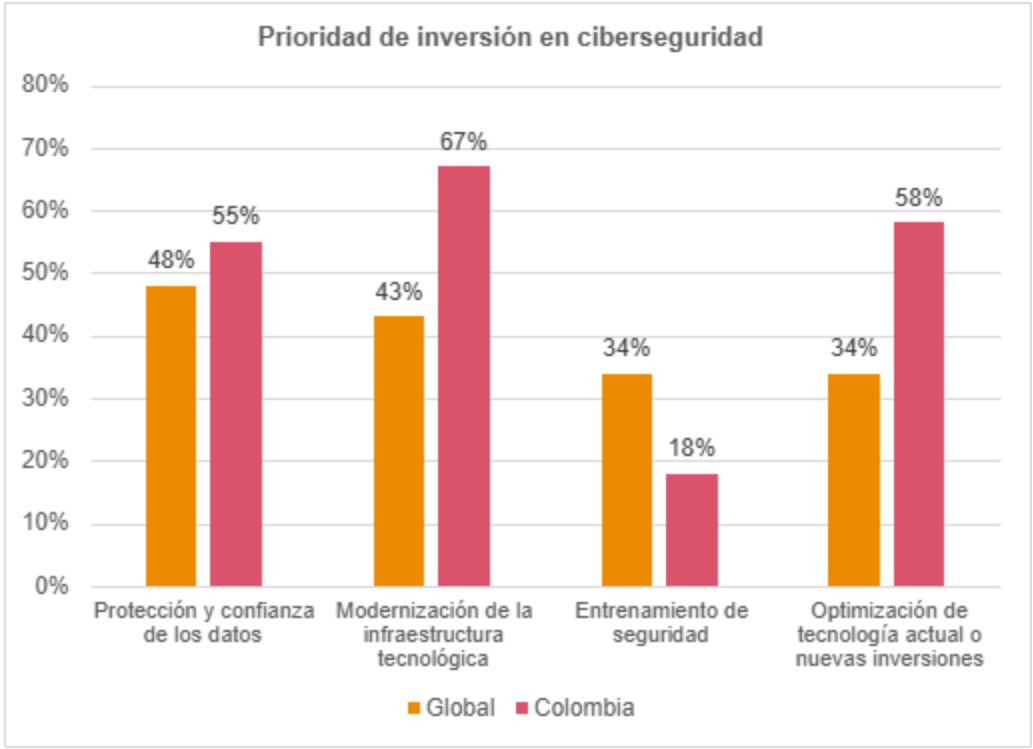
Fuente: Global Digital Trust Insights 2025

Llamada a la acción

Después de un año de mantener los presupuestos **es esencial alinear el aumento planificado del gasto con los riesgos actuales y futuros,** para que cada dólar fortalezca la resiliencia y prepare a la organización para el panorama cambiante de amenazas.

Empresas colombianas: invertir en lo que más importa, la modernización de la tecnología y su infraestructura

Durante los doce meses, las organizaciones colombianas **priorizarán la modernización de la tecnología y su infraestructura por sobre otras inversiones en ciberseguridad.** Para nuestro país es importante crear una red tecnológica fortalecida y optimizada; mientras que para global y Latinoamérica la prioridad es la protección de datos y la confianza de estos, algo que va de la mano. Estos dos últimos entienden que proteger la información confidencial es vital para mantener la confianza de las partes interesadas y la integridad de la marca.

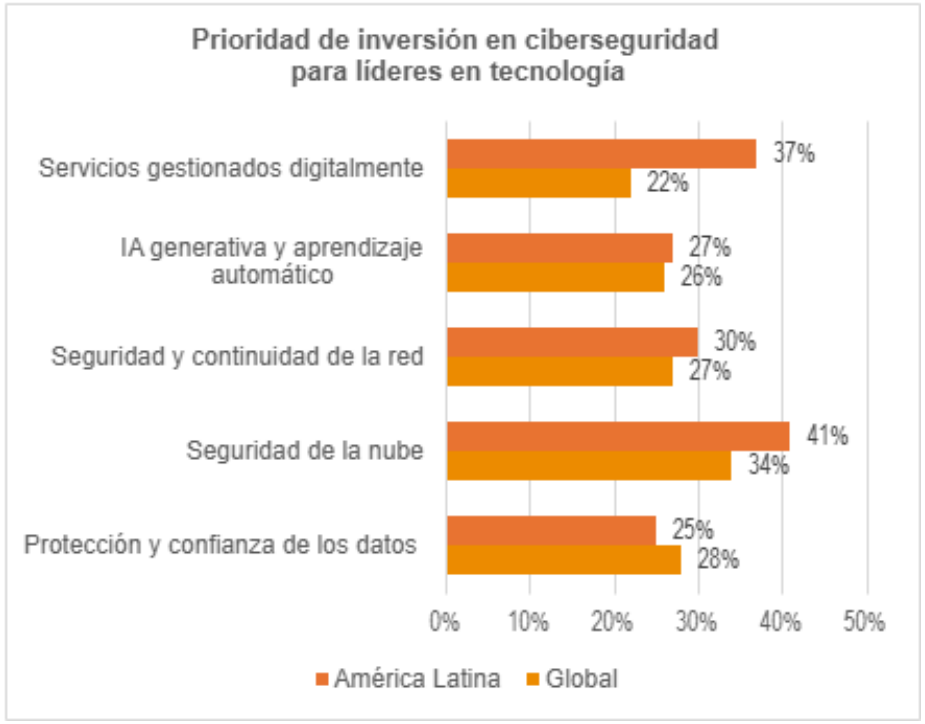


Fuente: Global Digital Trust Insights 2025

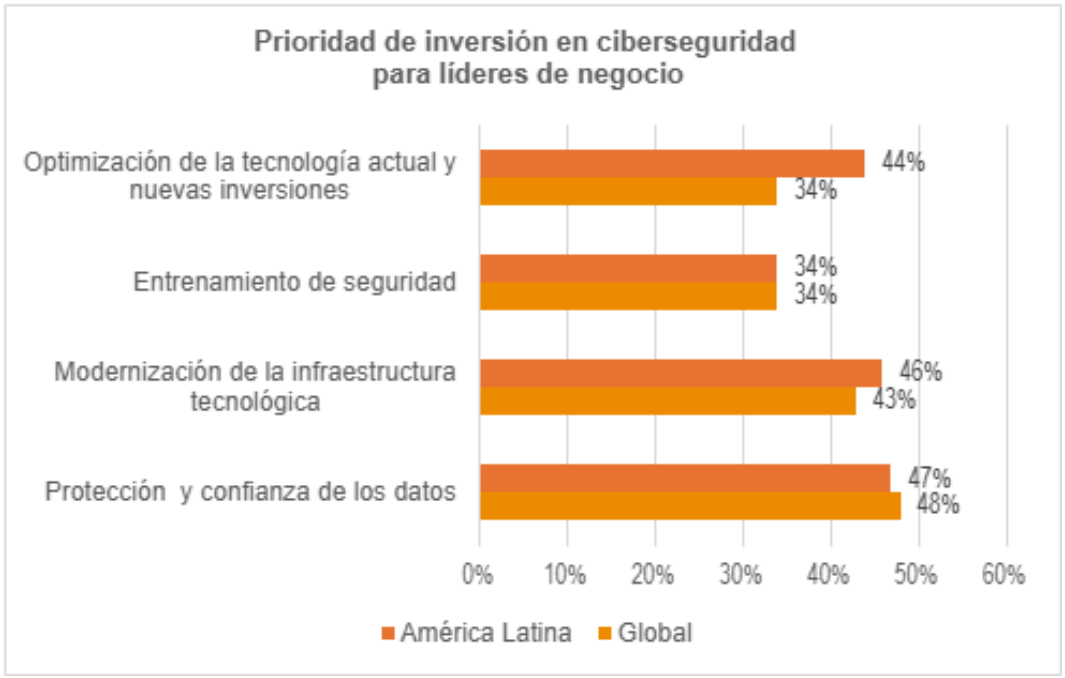
Los ejecutivos de empresas y tecnología clasifican una lista diferente de prioridades según las áreas específicas de sus funciones.

- Los ejecutivos de empresas dicen que la protección de datos y la confianza son su prioridad de inversión en ciberseguridad (47 % para Latinoamérica y 48 % para global), seguida de la modernización y optimización tecnológica (46 % para Latinoamérica y 43 % para global).

- Para los ejecutivos de tecnología, la seguridad en la nube sigue siendo su principal prioridad (41 % para Latinoamérica y 34 % para global), siguiendo la misma tendencia del año pasado. La protección de datos y la confianza son la siguiente prioridad (28 %) para global, mientras que para Latinoamérica serían los servicios gestionados digitalmente (37 %).



Fuente: Global Digital Trust Insights 2025



Fuente: Global Digital Trust Insights 2025

¿Por qué la seguridad en la nube sigue demandando atención?

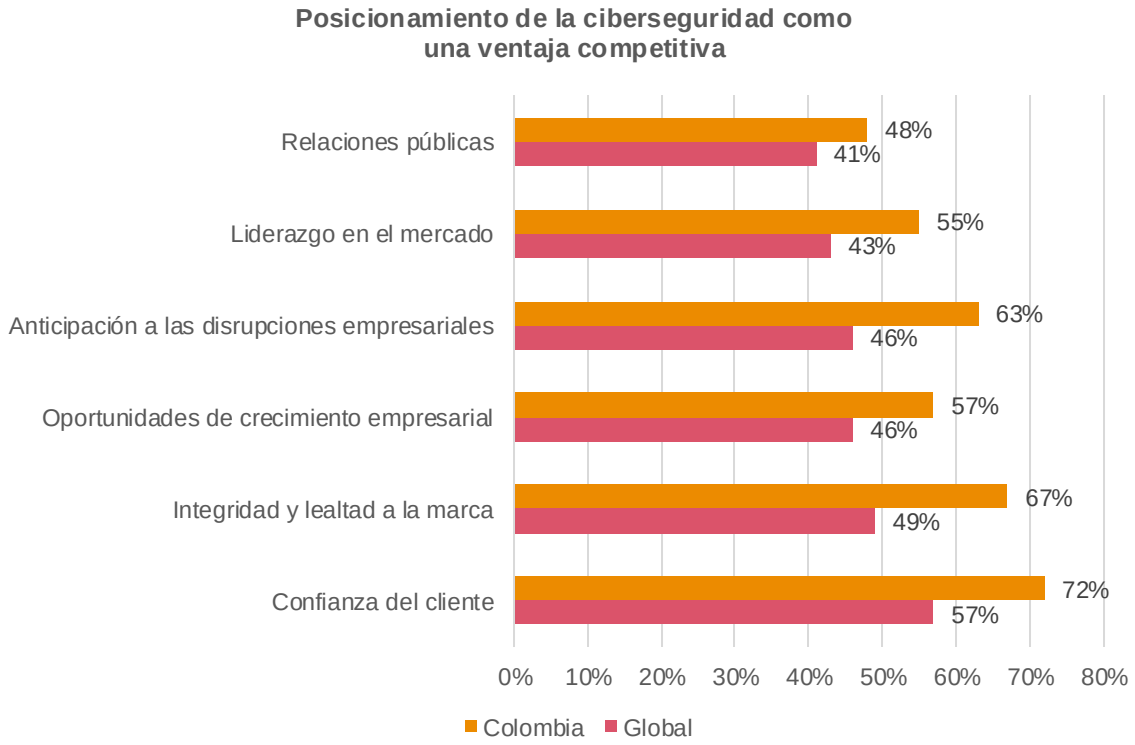
A pesar de años de inversión, la rápida adopción de tecnologías en la nube, la consolidación de *hyperscalers*, el auge de las configuraciones híbridas y el *multicloud* han concentrado el riesgo en este entorno. **Dicha acumulación incrementa el impacto potencial de las configuraciones incorrectas de acceso a los datos, las filtraciones de datos y los desafíos de integración.** A medida que los actores de amenazas evolucionan, también deben hacerlo las estrategias de seguridad en la nube, por lo que la inversión sostenida es crucial para mitigar estos riesgos intensificados.

Llamada a la acción

Invertir en ciberseguridad es invertir en confianza. Ya sea que se trate de **proteger la nube, salvaguardar los datos o abordar los riesgos emergentes,** su compromiso con estas áreas determinará la confianza de las partes interesadas y la resiliencia de su organización.

Ciberseguridad y confianza: la nueva ventaja competitiva

Las organizaciones consideran cada vez más la ciberseguridad como un factor diferenciador clave para obtener una ventaja competitiva: el 72 % de los ejecutivos colombianos (57 % para global) menciona la confianza del cliente, y el 67 % en Colombia (49 % a nivel global) la integridad y la lealtad a la marca como áreas de influencia. **A medida que aumentan las amenazas digitales, una postura sólida en materia de ciberseguridad no solo tiene que ver con la protección, sino con la construcción de una reputación en la que los clientes y las partes interesadas puedan confiar.** En un momento en el que la confianza es primordial, las empresas que priorizan la ciberseguridad están mejor posicionadas para destacarse como líderes tanto en seguridad como en integridad.



Fuente: Global Digital Trust Insights 2025

Llamada a la acción

La ciberseguridad no se limita a proteger los datos, sino que también abarca la protección de la marca. **En un entorno competitivo, la confianza lo es todo.** Reforzar ahora las medidas de seguridad ayudará a que la organización se destaque como líder en integridad de datos.

Llamado a la acción de los ejecutivos

Dado que las inversiones en ciberseguridad están destinadas a aumentar, **es esencial que todos los miembros de la alta dirección alineen sus estrategias con los riesgos más urgentes de la organización.** Los ejecutivos deben realizar inversiones que no solo aborden las vulnerabilidades actuales, sino que también generen confianza y resiliencia.

CIO, CTO y CISO: deben traducir el caso de negocios para las prioridades de inversión en protección de datos y seguridad en la nube a los CFO en función del valor comercial de los resultados clave (por ejemplo, reducir el tiempo para recuperar datos críticos para la misión o parchar un sistema).

CFO: deben determinar el valor comercial de la protección de datos y la seguridad en la nube para ganar la confianza de las partes interesadas y tomar decisiones de inversión en ciberseguridad más informadas.

CDO: deben colaborar con los ejecutivos de tecnología, seguridad y finanzas para identificar las prioridades más importantes en materia de seguridad e integridad de los datos a fin de orientar la estrategia de inversión en seguridad de la información y de la nube. Confirmar la calidad y la preparación de los datos es una necesidad para aumentar las inversiones en seguridad.

Estrategia y liderazgo digital

¿Su estrategia y liderazgo digital impulsan una resiliencia real?

Solo el 2%

a nivel global **ha implementado acciones de ciberresiliencia** en toda su organización.

Solo el 27%

en Colombia (21 % para global) **asigna el presupuesto de ciberseguridad** a los principales riesgos de la organización.

Alrededor del 50%

de los CISO colombianos (menos del 50 % a nivel global) participa en **gran medida en la planificación estratégica** de las inversiones en ciberseguridad.

Para gestionar las amenazas del futuro, **las inversiones por sí solas no son suficientes: las organizaciones también deben mejorar su estrategia y liderazgo en materia de ciberseguridad.** Desde los esfuerzos de resiliencia retrasados, hasta las deficiencias en la participación de los CISO en las decisiones estratégicas, existen áreas claras en las que se necesita una alineación estratégica. **Para lograrlo, las organizaciones deben emular las prácticas líderes en ciberseguridad** de sus pares con mejor desempeño. También deben ir más allá de abordar las amenazas conocidas e implementar un enfoque ágil y seguro por diseño para los negocios, que se esfuerce por generar confianza y resiliencia duradera.

El trabajo del CISO es contextualizar y conectar las amenazas existentes con las vulnerabilidades dentro de la organización. Eso significa educar a las personas sobre las amenazas que la empresa está preparada para enfrentar y aquellas para las que no está preparada. Con un enfoque que priorice la educación, suele haber más cooperación en toda la organización.

David Bruyea
Director de seguridad de la información
de Moneris

La implementación parcial no es suficiente

A pesar de la creciente preocupación por el riesgo de seguridad, la mayoría de las empresas tiene dificultades para implementar plenamente la resiliencia digital en sus prácticas básicas. Una revisión de doce acciones de resiliencia en personas, procesos y tecnología indica que el 52 % o menos de los ejecutivos colombianos (42 % para global) cree que sus organizaciones han implementado plenamente alguna de dichas acciones. Más preocupante aún es que solo el 2 % en el mundo dice que se han implementado las doce acciones de resiliencia en toda su organización. **Esto deja una vulnerabilidad evidente: sin resiliencia en toda la organización, las empresas siguen estando en peligro por su exposición a las crecientes amenazas que podrían comprometer toda la operación.**

Las siguientes son solo algunas acciones clave que podrían potenciarse con la gestión interorganizacional:

- Establecer un equipo de resiliencia (solo el 25 % de los líderes colombianos y el 34 % de los ejecutivos globales dice que esto se ha implementado en toda la organización);
- desarrollar un manual de recuperación digital para escenarios de pérdida de TI (solo el 32 % de los ejecutivos colombianos y el 35 % en global dice que esto se ha implementado en toda la organización); y
- mapear dependencias tecnológicas (solo el 25 % en Colombia y el 31 % en global dice que esto se ha implementado en toda la organización).

Implementación de acciones de resiliencia cibernética en toda la organización en Colombia

Personas

- Informes a las partes interesadas externas (reguladores, inversores) — 35 %
- Establecimiento de un equipo de resiliencia con miembros de funciones como continuidad empresarial, ciberseguridad y gestión de crisis — 25 %
- Establecimiento de relaciones con las fuerzas de seguridad locales para ayudar con el análisis y la respuesta — 27 %

Tecnología

- Implementación de soluciones tecnológicas de recuperación cibernética (incluidas copias de seguridad inmutables) — 35 %
- Mapeo de dependencias tecnológicas — 31 %
- Implementación de herramientas para una mayor visibilidad de los activos de tecnología operativa (OT) — 22 %
- Implementación de computación cuántica para la ciberdefensa y la resiliencia — 15 %

Procesos

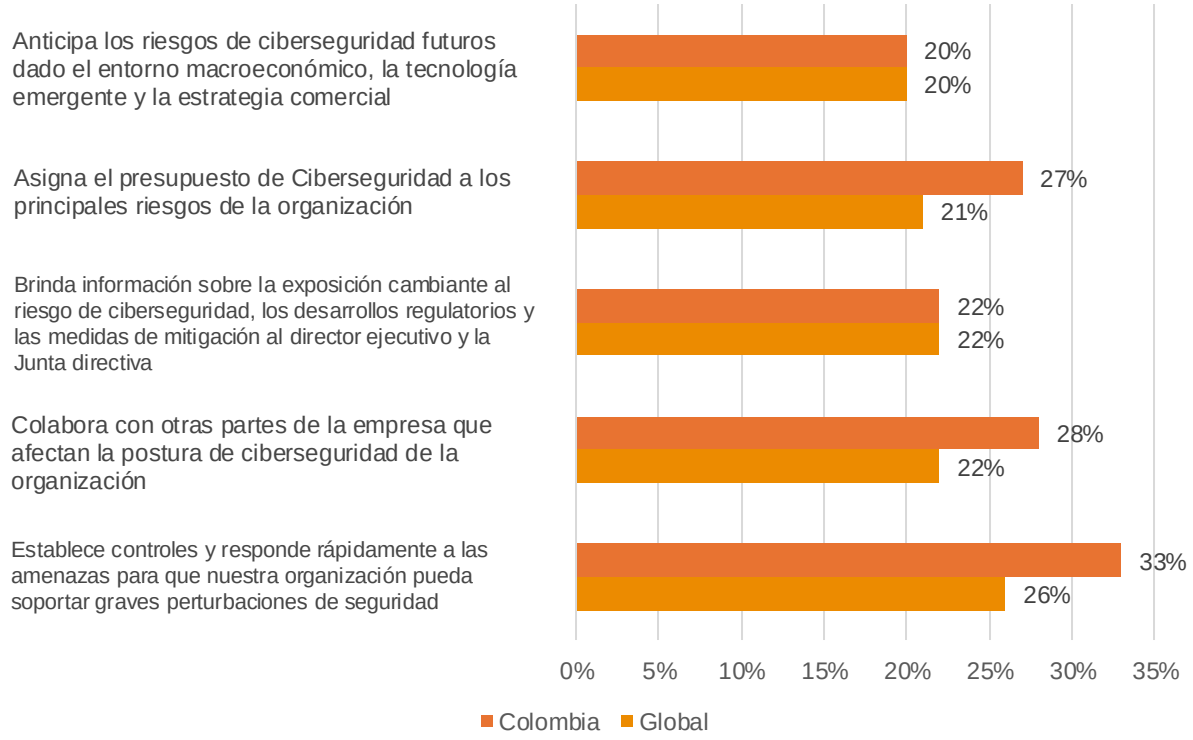
- Identificación de procesos empresariales críticos — 52 %
- Desarrollo de un manual de recuperación cibernética para escenarios de pérdida de TI — 32 %
- Establecimiento de protocolos con los principales proveedores de tecnología para coordinar las respuestas a incidentes — 27 %
- Ejecución de ejercicios de mesa y simulaciones — 40 %
- Compartir información con pares de la industria, a través de procesos formales, para prevenir riesgos sistémicos — 25 %

Llamada a la acción

La falta de resiliencia digital pone en riesgo a la organización. **Tomar medidas a nivel de toda la empresa es fundamental —a través de la tecnología, de los procesos y del personal—** para transformar las defensas y estar preparados para los desafíos que se avecinan.

La resiliencia digital es una prioridad ¿Por qué tantas empresas están rezagadas en áreas críticas?

Numerosas empresas aún están rezagadas a la hora de demostrar prácticas de ciberseguridad punteras. **Solo uno de cada cinco ejecutivos señala que las pone en práctica de forma habitual.** Por ejemplo, solo el 20 % en Colombia y a nivel global suele anticipar los riesgos futuros, y solo el 27 % de los encuestados colombianos (21 % en global) suele asignar el presupuesto de ciberseguridad a los principales riesgos de la organización. **Este retraso podría deberse a varios factores, entre ellos, la falta de previsión estratégica, recursos insuficientes o un enfoque reactivo en lugar de proactivo en materia de ciberseguridad.**

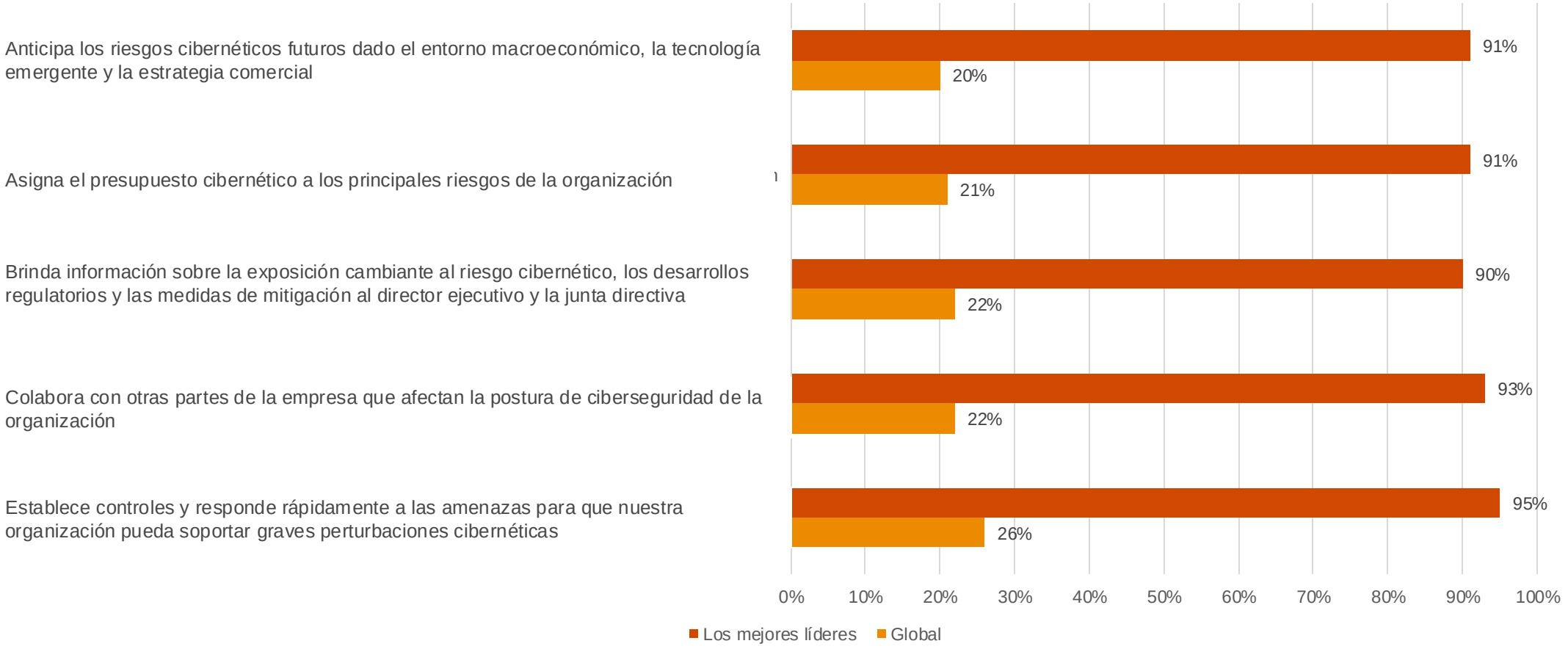


Fuente: Global Digital Trust Insights 2025

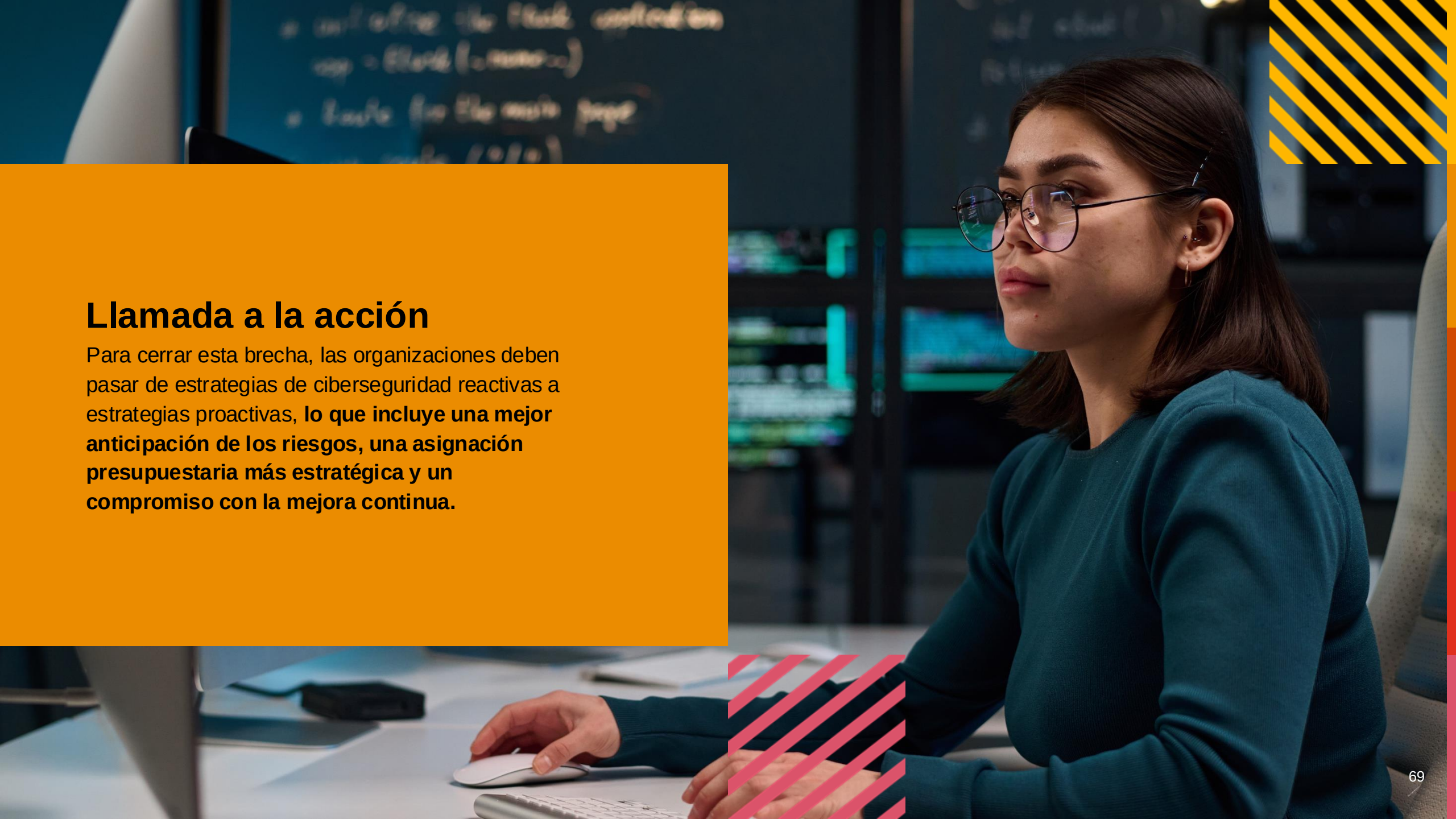
Los mejores artistas eclipsan al resto de manera constante y significativa

Analizamos esta cuestión más a fondo para identificar un grupo de ejecutivos de alto rendimiento que ‘habitualmente’ demuestran estos comportamientos. **Existe una brecha de sesenta y nueve puntos porcentuales mayor en todos los comportamientos entre los ejecutivos de alto rendimiento y nuestros encuestados globales.** Los ejecutivos de alto rendimiento tienen más probabilidades de tener mayor confianza en la capacidad de su organización para cumplir con las regulaciones y han implementado acciones clave de resiliencia en toda su organización.

Diferencias en el comportamiento de los equipos de ciberseguridad entre los de mejor desempeño y todos los líderes



Fuente: Global Digital Trust Insights 2025



Llamada a la acción

Para cerrar esta brecha, las organizaciones deben pasar de estrategias de ciberseguridad reactivas a estrategias proactivas, **lo que incluye una mejor anticipación de los riesgos, una asignación presupuestaria más estratégica y un compromiso con la mejora continua.**

Prioridades estratégicas: velocidad, confianza y seguridad para las partes interesadas

En los próximos doce meses más de un tercio de los ejecutivos espera trabajar para reducir los tiempos de respuesta a incidentes e interrupciones. **Otros objetivos principales son: aumentar la confianza en la capacidad de los líderes para gestionar las amenazas y mejorar las experiencias tanto de los clientes como de los empleados**; estas metas reflejan un mayor impulso, no solo para mitigar los riesgos de forma más ágil, sino para generar confianza y proteger a los clientes y empleados.

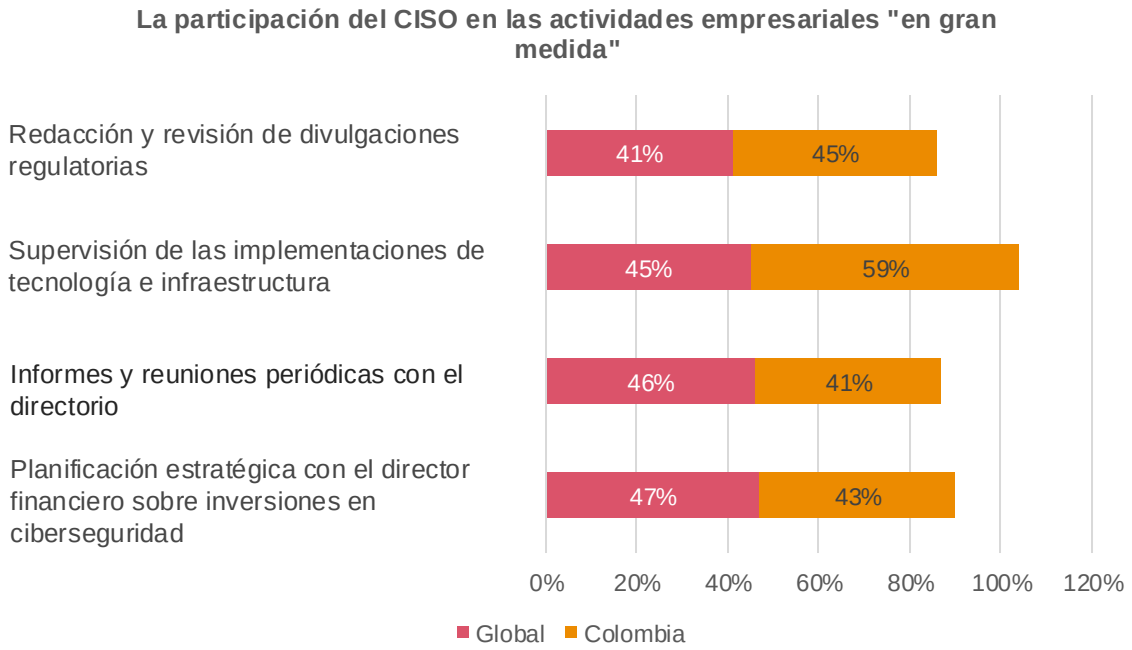
Fuente: Global Digital Trust Insights 2025

Llamada a la acción

Las respuestas rápidas no son solo un objetivo, son una necesidad. **Las reacciones tardías a las amenazas pueden costar más que solo tiempo;** pueden erosionar la confianza y afectar gravemente al negocio. La velocidad y la confianza en el liderazgo deben ser prioridades innegociables.

Elevando al CISO: alineando la estrategia con la seguridad

Muchas organizaciones pierden oportunidades críticas porque no involucran plenamente a sus CISO en iniciativas clave. **Menos de la mitad de los ejecutivos nos dicen que sus CISO participan en gran medida en la planificación estratégica de inversiones digitales,** la presentación de informes a la Junta directiva y la supervisión de implementaciones tecnológicas. Esta brecha deja a las organizaciones vulnerables a estrategias desalineadas y posturas de seguridad más débiles.



Fuente: Global Digital Trust Insights 2025

Llamada a la acción

Dé al CISO un lugar en la mesa. **Los conocimientos del CISO son fundamentales para abordar de forma proactiva la ciberseguridad como un riesgo empresarial fundamental;** involucrarlo al más alto nivel ayuda a que la organización alinee su enfoque para proteger activos críticos e impulse la resiliencia.

Llamado a la acción de los ejecutivos

Un liderazgo sólido en materia de ciberseguridad exige una visión estratégica y una alineación en toda la organización. **Cada ejecutivo tiene un papel que desempeñar en el impulso de esta alineación,** desde la integración del CISO en las decisiones clave hasta la priorización de los esfuerzos de resiliencia.

CISO: deben exponer al resto de los altos ejecutivos los motivos por los cuales es imperativo que los CISO participen en la estrategia, la planificación y la supervisión de la estrategia de resiliencia y mitigación de riesgos de seguridad digital.

CEO, CFO y directores de sistemas de información: deben participar en evaluaciones y ejercicios de resiliencia digital para comprender mejor las brechas y los enfoques que los directores de seguridad de la información pueden enfrentar para integrar prácticas, estándares y controles líderes.

Junta directiva: deben mantenerse informado acerca de los avances del programa de riesgo de ciberseguridad, especialmente los relacionados con la exposición a amenazas y riesgos digitales de sus organizaciones, para cumplir con las crecientes responsabilidades de supervisión y gobernanza.

Global Digital Trust Insights 2025 es una encuesta a 4.042 ejecutivos de empresas y tecnología realizada entre mayo y julio de 2024.

Acerca de la encuesta

Una cuarta parte de los ejecutivos pertenecen a grandes empresas con **ingresos de 5.000 millones de dólares**, o más. Los encuestados operan en una variedad de sectores,

21 % la industria y los servicios	**20 %** tecnología, medios de comunicación y telecomunicaciones
19 % servicios financieros	**17 %** mercados minoristas y de consumo
11 % energía, servicios públicos y recursos	**7 %** Salud
4 % gobierno y servicios públicos	

Los encuestados se encuentran en **setenta y siete países.** El desglose regional es el siguiente:

30 % Europa occidental

25 % Norteamérica

18 % Asia-Pacífico

12 % Latinoamérica

6 % Europa central y oriental

5 % África

3 % Oriente Medio

La encuesta Global Digital Trust Insights Survey, conocida anteriormente como la Encuesta sobre el estado global de la seguridad de la información (GSISS, por sus siglas en inglés), se encuentra en su **26.° año y es la encuesta anual sobre tendencias en materia de ciberseguridad que más tiempo lleva realizándose.** Asimismo, es la encuesta más extensa en el sector de la ciberseguridad, y la única que cuenta con **la participación de ejecutivos de alto nivel, no solo de ejecutivos de seguridad y tecnología.**

PwC Research, el centro de excelencia global de PwC para investigación y conocimiento de mercado formuló y aplicó esta encuesta.

Mauricio Arias

Socio de Consultoría en Tecnología,
PwC Colombia

Email

Carlos Andres Rodríguez

Director de Consultoría en Ciberseguridad
y Privacidad,

PwC Colombia

Email

Mauricio Sanchez

Gerente de Consultoría en Ciberseguridad
y Privacidad,

PwC Colombia

Email