



Nuevo mundo, nuevas reglas: la ciberseguridad en una era de incertidumbre

Global Digital Trust Insights
2026: guía y conclusiones para
los altos ejecutivos



60 %

está aumentando la inversión en riesgos de ciberseguridad en respuesta a la volatilidad geopolítica.

Solo un 6 %

ha implementado plenamente todas las medidas de riesgo de datos encuestadas.

Top 2

Los vacíos de conocimiento y habilidades, entre los retos para implementar la IA en la ciberdefensa.

La ciberseguridad está entrando en un terreno desconocido. El orden mundial y el entorno de amenazas en rápida evolución, impulsados por los recientes avances exponenciales de la tecnología, están poniendo a prueba las estrategias de ciberseguridad.

Las organizaciones se enfrentan a la nueva realidad de una era de posglobalización, caracterizada por alianzas fracturadas, instituciones globales debilitadas, crisis arancelarias y cadenas de suministro interrumpidas. Estamos siendo testigos de avances tecnológicos sin precedentes que amplían la superficie de ataque e introducen nuevas amenazas cibernéticas, muchas de ellas patrocinadas por Estados.

Toda esta incertidumbre está obligando a los ejecutivos a reevaluar sus capacidades, talento y tecnología. Fundamentalmente, les está obligando a revisar su estrategia de ciberseguridad, incluyendo dónde operan y con quién hacen negocios.

La encuesta Digital Trust Insights 2026 de PwC, realizada a 3.887 ejecutivos de empresas y del sector tecnológico de 72 países, revela cómo los líderes están afrontando esta era de incertidumbre, en qué aspectos se están quedando cortos y qué podrían hacer de forma diferente para responder mejor al desafío. Entre las principales conclusiones se encuentran las siguientes:

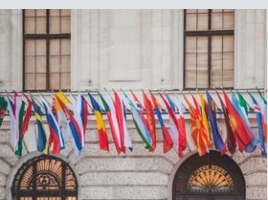
- **El riesgo geopolítico está determinando la estrategia:** el 60 % de los líderes empresariales y tecnológicos sitúan la inversión en ciberseguridad entre sus tres principales prioridades estratégicas en respuesta a la actual incertidumbre geopolítica.
- **La resiliencia es un trabajo en curso:** dada la situación geopolítica actual, aproximadamente la mitad afirma que su organización es, en el mejor de los casos, “algo capaz” de resistir los ciberataques dirigidos a vulnerabilidades específicas. Solo el 6 % se siente seguro con respecto a todas las vulnerabilidades analizadas.
- **A la espera de problemas:** solo el 24 % de las organizaciones está invirtiendo significativamente más en medidas proactivas (por ejemplo, supervisión, evaluaciones, pruebas, controles) que en medidas reactivas (respuesta a incidentes, multas, recuperación). Esa es la proporción de gasto ideal. La mayoría de las empresas (67 %) está invirtiendo aproximadamente las mismas cantidades en ambas categorías, lo que puede resultar más costoso y arriesgado.
- **Agentes de IA para la ciberdefensa:** el agente de IA se encuentra entre las principales capacidades de seguridad de IA que las organizaciones priorizarán en los próximos 12 meses. Tienen previsto implementar estos agentes para la seguridad en la nube, la protección de datos, la ciberdefensa y las operaciones, entre otras áreas prioritarias.

- **El reloj cuántico no se detiene:** la computación cuántica modificará por completo la velocidad en la cual se desarrollan todos los procesos digitales, por eso se encuentra entre las cinco principales amenazas que las organizaciones están menos preparadas para abordar, menos del 10 % le da prioridad en sus presupuestos y solo el 3 % ha implementado todas las principales medidas de resistencia a la computación cuántica incluidas en esta encuesta.
- **Reconsiderando la crisis de talento en ciberseguridad:** la escasez de habilidades sigue siendo uno de los mayores obstáculos para el progreso en ciberseguridad. Más de la mitad (53 %) está dando prioridad a las herramientas de inteligencia artificial y aprendizaje automático para ayudar a cerrar las brechas de capacidad, y los servicios gestionados especializados se están convirtiendo en aceleradores estratégicos para proporcionar experiencia y escala.

Responder a este momento exigirá renovar con urgencia, de forma creativa y con enfoques distintos, y no una mentalidad conservadora. Nuestro manual para altos directivos traduce los hallazgos de este año en medidas aplicables, ayudando a los grupos de interés a reforzar sus prácticas de seguridad fundamentales y a implementar medidas preparadas para el futuro, calibradas para un mundo en constante evolución.



Índice

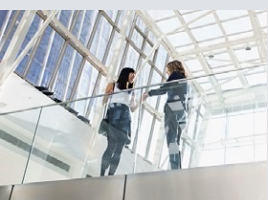


01

Panorama de riesgos y amenazas

La geopolítica está transformando las vulnerabilidades en entornos digitales

05

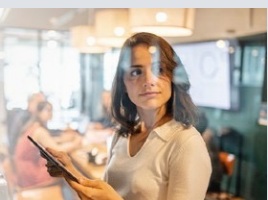


02

Estrategia y operaciones en ciberseguridad

Donde la inversión se une al impacto

09

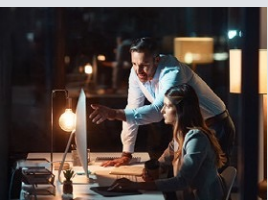


03

IA en ciberseguridad

De promesa a prioridad

13



04

Preparación para la computación cuántica

Preparación para amenazas de mayor nivel

17

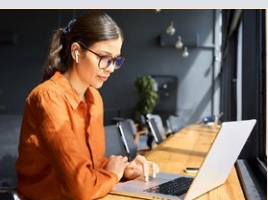


05

Talento y habilidades en ciberseguridad

Los servicios gestionados pasan a primera línea

21



06

Manual para altos ejecutivos

De la incertidumbre a la acción: qué pueden hacer los líderes ahora

25



01

**Panorama de riesgos
y amenazas**

La geopolítica está transformando las vulnerabilidades digitales

60 %

está aumentando la inversión en riesgos en ciberseguridad en respuesta a la volatilidad geopolítica.

Solo el 6 %

Se percibe “muy capaz” de resistir los ciberataques en todas las vulnerabilidades estudiadas, dado el panorama geopolítico.

Top 2

Los vacíos de conocimiento y habilidades, entre los retos para implementar la IA en la ciberdefensa.

Los riesgos de ciberseguridad actuales están determinados tanto por la geopolítica como por las tecnologías disruptivas. Las alianzas trastocadas, las disputas comerciales, el debilitamiento de las instituciones internacionales y otras tendencias desestabilizadoras en esta nueva era de competencia estratégica están remodelando el entorno de amenazas, así como los métodos tradicionales de hacer negocios.

En respuesta a este clima geopolítico, el 60 % de los líderes empresariales y tecnológicos a nivel global y el 62 % en América Latina, están convirtiendo la inversión en ciberseguridad en una de sus tres principales prioridades estratégicas para el próximo año. Además, están dando prioridad a los cambios en la ubicación de la infraestructura crítica (41 % global y 31 % en América Latina), las políticas comerciales y operativas (30 % global y 40 % América Latina) y las pólizas de seguros cibernéticos (39 % global y 29 % América Latina). Ahora que la disrupción es la norma, la ciberseguridad es una palanca fundamental para la resiliencia.

Los cambios en la estrategia de ciberseguridad en respuesta al panorama geopolítico actual
(% que lo clasificó entre sus tres áreas principales)



63 %

de los líderes empresariales y tecnológicos en Colombia está convirtiendo la inversión en riesgos de ciberseguridad entre sus tres principales prioridades estratégicas para el próximo año.

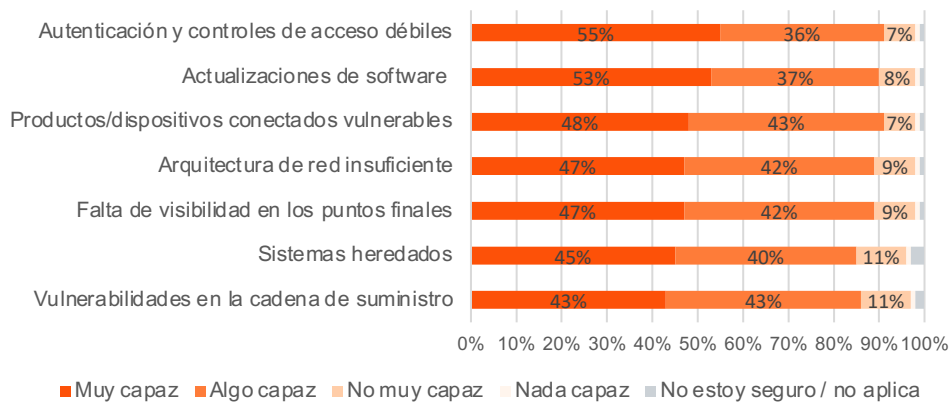
P2. En los próximos 12 meses, ¿cuáles de las siguientes áreas de la estrategia de ciberseguridad de tu organización cambiarán en respuesta al panorama geopolítico actual?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC.

Sentirse seguro vs. estar seguro

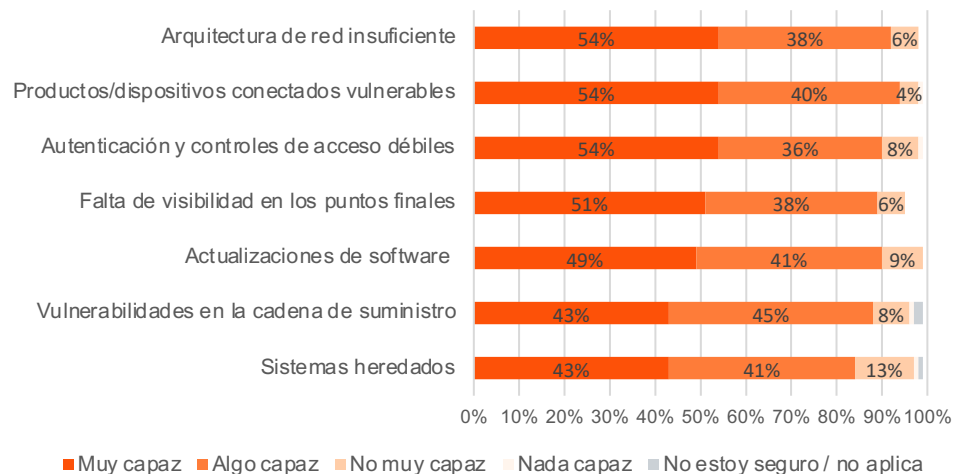
Dado el panorama geopolítico actual, la confianza en la preparación de amenazas está dividida. Si bien, aproximadamente la mitad de los encuestados afirma que sus organizaciones son “muy capaces” de resistir los ciberataques dirigidos a vulnerabilidades específicas encuestadas, otro grupo igual de grande afirma no estar preparado. Es más, solo el 6 % de todos los encuestados afirma estar capacitado o muy capacitado para hacer frente a todas estas amenazas.

Capacidad para resistir un ciberataque importante

Global



América Latina



P3. Dado el panorama geopolítico actual, ¿qué tan capacitada está tu organización para resistir un ataque a la ciberseguridad importante que apunte a las siguientes vulnerabilidades?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC.

Brechas persistentes, riesgos crecientes

Más allá de las vulnerabilidades mencionadas, los líderes están preocupados por su preparación ante determinados tipos de amenazas. A nivel global, los ataques a la nube y a productos conectados siguen siendo las principales preocupaciones, al igual que el año pasado, y aproximadamente un tercio de los líderes los sitúan entre las tres principales amenazas a la ciberseguridad para las que su organización está menos preparada.

Estos riesgos no son nuevos, pero con adversarios equipados con IA que van más allá de los límites, reflejan los desafíos constantes para cerrar brechas fundamentales en gobernanza, control y visibilidad. A medida que la tecnología y los ecosistemas digitales se vuelven más complejos, muchas organizaciones enfrentan desafíos para mantenerse al día, especialmente en lo relacionado con las dependencias de terceros y los riesgos asociados a la cadena de suministro

Amenazas a la ciberseguridad para las que las organizaciones están menos preparadas

(% que las clasificó entre sus tres principales amenazas)



P1. En los próximos 12 meses, ¿cuál de estas amenazas a la ciberseguridad es la que tu organización está menos preparada para afrontar?

Fuente: Encuesta Global Digital Trust Insights 2026 de PwC.

Aprender de los errores

Desde hace varios años, más de una cuarta parte de los ejecutivos nos dicen que la filtración de datos más perjudicial que han sufrido en los últimos tres años le ha costado a su organización al menos un millón de dólares ¿Las más expuestas? Las empresas con ingresos de USD\$5 billones o más (41 %), las empresas con sede en EE. UU. (37 %) y las empresas que operan en el sector de la tecnología, los medios de comunicación y las telecomunicaciones (33 %). Para ellas, la escala y la complejidad de las operaciones aumentan la probabilidad de que se produzcan incidentes de alto coste.

Dados los retos que plantea la recuperación, las organizaciones que han sufrido un ataque grave están poniendo en práctica las costosas lecciones aprendidas. Están haciendo más que otras para aumentar los presupuestos destinados a la ciberseguridad (88 %, frente al 78 % en general) y adoptar servicios gestionados para suplir las deficiencias críticas de habilidades (48 %, frente al 39 % en general). Además, son más propensas a cambiar las pólizas de seguro cibernético (49 %, frente al 39 % en general), posiblemente en respuesta al aumento de las primas y las expectativas de las aseguradoras. Asimismo, muchas están incorporando más prácticas de minimización de datos en toda la organización.

A low-angle shot of two business women standing on a glass-enclosed balcony or staircase in a modern skyscraper. The woman on the left is wearing a dark blue suit and is gesturing with her hand while talking to the woman on the right, who is wearing a light blue top and dark skirt. The background shows the intricate steel framework and glass panels of the building's interior, with bright light coming from the windows.

02

Estrategia y
operaciones de
ciberseguridad

Donde la inversión se une al impacto

Solo el
24 %

están invirtiendo significativamente
más en medidas de ciberseguridad
proactivas que en medidas reactivas.

78 %

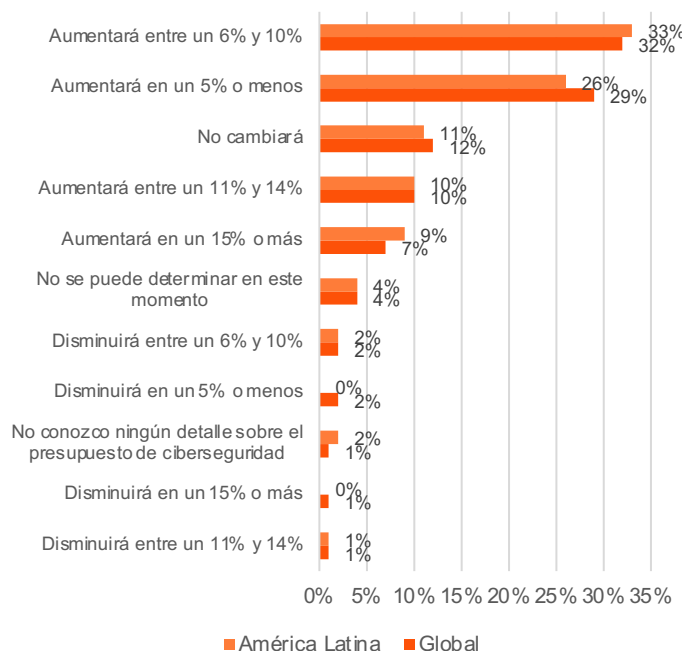
espera que su presupuesto para
ciberseguridad aumente durante el
próximo año.

Solo el
16 %

mide el impacto financiero de los
riesgos en ciberseguridad de manera
significativa.

¿Los presupuestos en ciberseguridad se adaptan a los nuevos tiempos? Casi ocho de cada diez encuestados afirman que su presupuesto en ciberseguridad aumentará durante el próximo año. Sin embargo, esta cifra prácticamente no ha variado con respecto al año pasado. Aunque los encuestados afirman que están aumentando la inversión en riesgos de ciberseguridad en respuesta al panorama geopolítico actual, es posible que esto se esté haciendo a expensas de otras prioridades de gasto.

Cambio en el presupuesto de ciberseguridad en 2026



P8. ¿Cómo cambiará el presupuesto de ciberseguridad de tu organización en 2026?

Base: Líderes de Seguridad, CFO y directores de finanzas

Fuente: Encuesta Global Digital Trust Insights 2026 de PwC.

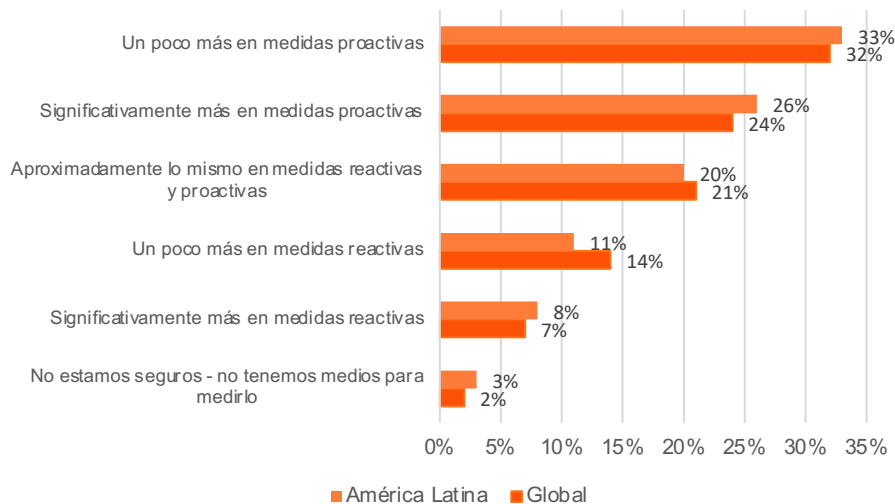
El coste de prevenir vs. el costo de reaccionar

La ciberseguridad tiene que ver con la preparación. Implica planificar con antelación e invertir en medidas proactivas como la supervisión, las evaluaciones, las pruebas, los controles y la formación, **antes de que se produzca una crisis**. La alternativa, que se basa principalmente en medidas reactivas (por ejemplo, respuesta, atención al cliente, reparación, recuperación, litigios y multas), es más costosa, arriesgada e insostenible.

Dos tercios (67 %) de las organizaciones a nivel global y un poco menos de dos tercios en América Latina (64 %) afirma que su ratio de costes proactivos/reactivos es prácticamente igual, es decir, que gastan aproximadamente lo mismo en medidas de ciberseguridad proactivas y reactivas, o ligeramente más en cualquiera de ellas. Pocas (24 %), a nivel global, se encuentran en la situación ideal de invertir significativamente más en medidas proactivas. Es más, es probable que esas cifras subestimen el verdadero coste de reaccionar. Mientras que el gasto proactivo se incluye en el presupuesto del responsable de seguridad y es fácil de controlar, los costes reactivos se dispersan por toda la empresa: legales, comunicaciones, operaciones, TI, producto, marketing, relaciones gubernamentales, e incluyen costos más difíciles de cuantificar, como la pérdida de oportunidades y el daño a la reputación.

En este sentido, el gasto en medidas proactivas no servirá de nada si se centra en los riesgos equivocados o no es lo suficientemente ágil como para adaptarse a las nuevas condiciones. Una verdadera preparación requiere un profundo conocimiento del panorama de riesgos y amenazas, que sirva de base para la estrategia en ciberseguridad de la empresa, el personal que contrata y los procesos, sistemas y herramientas que adopta.

Gasto en medidas reactivas frente a medidas proactivas Comparativo Global vs. América Latina



29 %

de los líderes empresariales y tecnológicos en Colombia declara gastar “aproximadamente lo mismo” en medidas proactivas y reactivas.

P13. ¿Tu organización dedica más recursos a medidas de ciberseguridad reactivas o proactivas?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC

Correlacionar las prioridades de inversión con la preparación

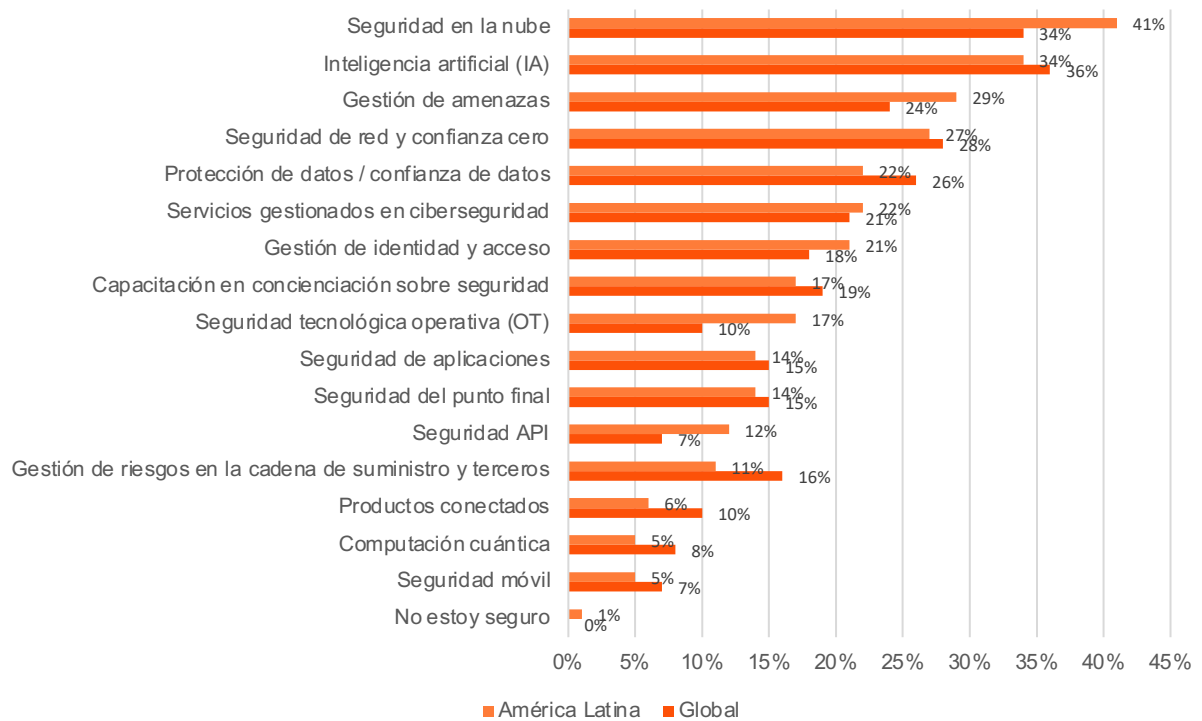
A nivel global y en América Latina, la inteligencia artificial y la seguridad en la nube son las dos principales prioridades presupuestarias en materia de ciberseguridad para el próximo año. No es de extrañar. Como se ha señalado anteriormente, la nube también encabeza la lista de amenazas en las que los líderes se sienten menos preparados para abordar. Se está reconociendo la brecha entre el riesgo y la preparación, y la financiación está siguiendo el mismo camino.

Pero el panorama no está completo. Los ataques a productos conectados ocupan el segundo lugar, a nivel global, entre las áreas en las que las organizaciones se sienten menos preparadas, pero son muy pocas las que le asignan presupuesto. Este desajuste sugiere que algunas amenazas siguen pasando desapercibidas.

Los servicios gestionados de ciberseguridad son otra prioridad de financiación para muchas organizaciones a nivel global. Las empresas de alto crecimiento están dando un paso más allá, ya que el 30 % las sitúa entre sus tres principales prioridades de inversión. Esto refleja una estrategia para aprovechar la experiencia externa y cubrir las brechas críticas en preparación de ciberseguridad.

Inversiones que las organizaciones están priorizando al asignar sus presupuestos de ciberseguridad

Comparativo Global vs. América Latina (% que los situó entre sus tres principales prioridades)

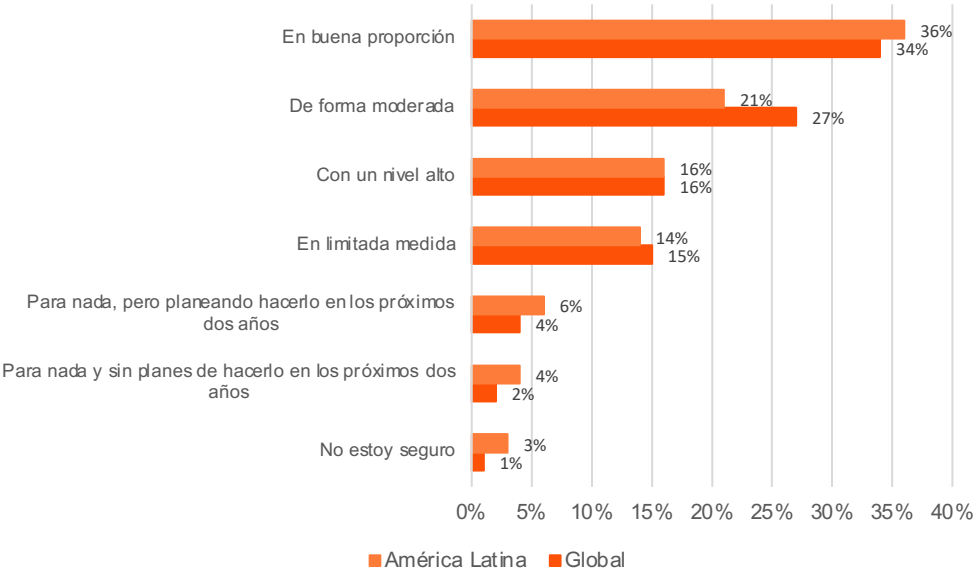


P9. ¿A cuáles de las siguientes inversiones estás dando prioridad a la hora de asignar el presupuesto en ciberseguridad de tu organización para los próximos 12 meses?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC.

Fijar el precio al riesgo en ciberseguridad

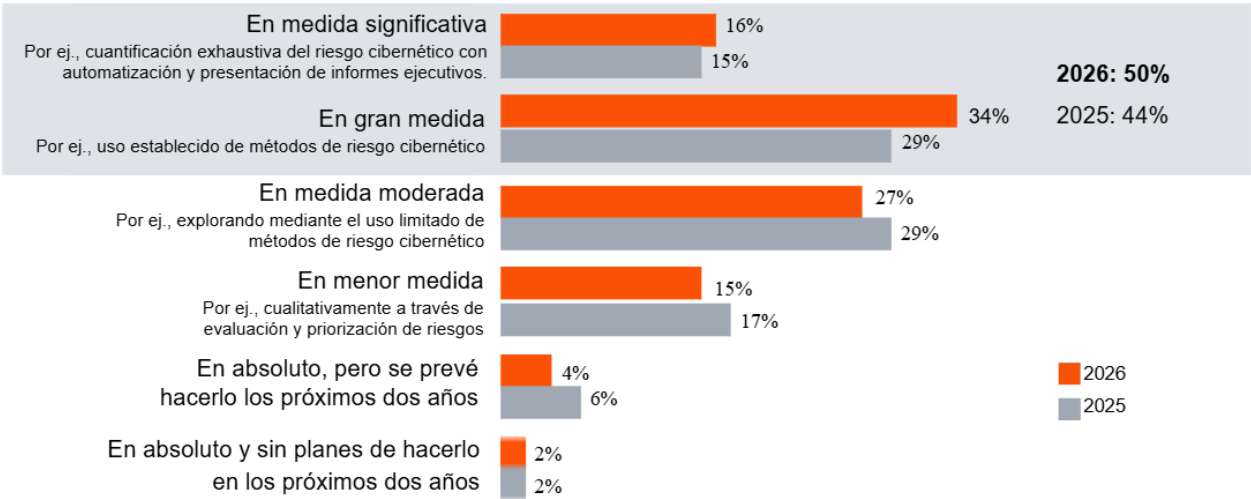
Cada vez más organizaciones respaldan sus riesgos con cifras. La mitad afirma ahora utilizar la cuantificación del riesgo en ciberseguridad para medir el impacto financiero de forma significativa o considerable— frente al 44 % del año pasado. Tanto en global como en América Latina, la mitad de los encuestados informa que utiliza la cuantificación del riesgo de ciberseguridad para medir el impacto financiero en “buena proporción o “de forma moderada”. Sin embargo, al analizar más a fondo, solo 16 % lo hace en “un nivel alto”.

Medición del impacto financiero de los riesgos en ciberseguridad
Comparativo Global vs. América Latina



P12. ¿En qué medida mide actualmente tu organización el impacto financiero potencial de los riesgos en ciberseguridad (es decir, la cuantificación del riesgo)?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC.

Medición del impacto financiero de los riesgos cibernéticos



P12. ¿En qué medida mide actualmente tu organización el impacto financiero potencial de los riesgos en ciberseguridad (es decir, la cuantificación del riesgo)?
Base: Líderes de seguridad, CFO, CEO, CRO y el Directorio=2.673, DTI25: Líderes de seguridad, CFO, CEO, CRO y el Directorio=2.570
Fuente: Perspectivas Globales sobre la confianza Digital 2026.

03

La IA en la ciberseguridad

De promesa a prioridad

#1

la prioridad de inversión en ciberseguridad para los responsables de seguridad es la IA.

#1

la capacidad de seguridad de IA priorizada por los responsables de seguridad es la búsqueda de amenazas.

Top 3

áreas prioritarias para agentes de IA seguridad en la nube, protección de datos y ciberdefensa.

El potencial de la IA para transformar las capacidades digitales es evidente y de gran alcance. Por eso ocupa el primer lugar en varias categorías de nuestra encuesta. La habilitación de capacidades digitales clave mediante la IA es la máxima prioridad a la hora de asignar presupuestos de ciberseguridad, utilizar servicios gestionados de ciberseguridad y abordar las carencias de talento en ciberseguridad.

Para reforzar las capacidades de seguridad habilitadas por la IA durante los próximos 12 meses, los responsables de seguridad a nivel global (48 %) y en América Latina (58 %) consideran que la búsqueda de amenazas es su máxima prioridad. Además, persiguen otras capacidades, como soluciones de agentes (35 %, global; 34 %, América Latina), detección de eventos (36 %, global; 30 %, América Latina) y análisis de comportamiento (36 %, global; 30 %, América Latina), gestión de identidades y accesos (36 %, global; 33 %, América Latina), y análisis y escaneo de vulnerabilidades (38 %, global; 42 %, América Latina).

El agente de IA entre las capacidades de seguridad de IA más prioritarias
Comparativo Global vs. América Latina (Ordenadas según quienes las clasificaron como su máxima prioridad)



P18. ¿Cuál de las siguientes capacidades de seguridad de IA priorizará tu organización en los próximos 12 meses?
Base: Líderes de seguridad = 1.740
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC.

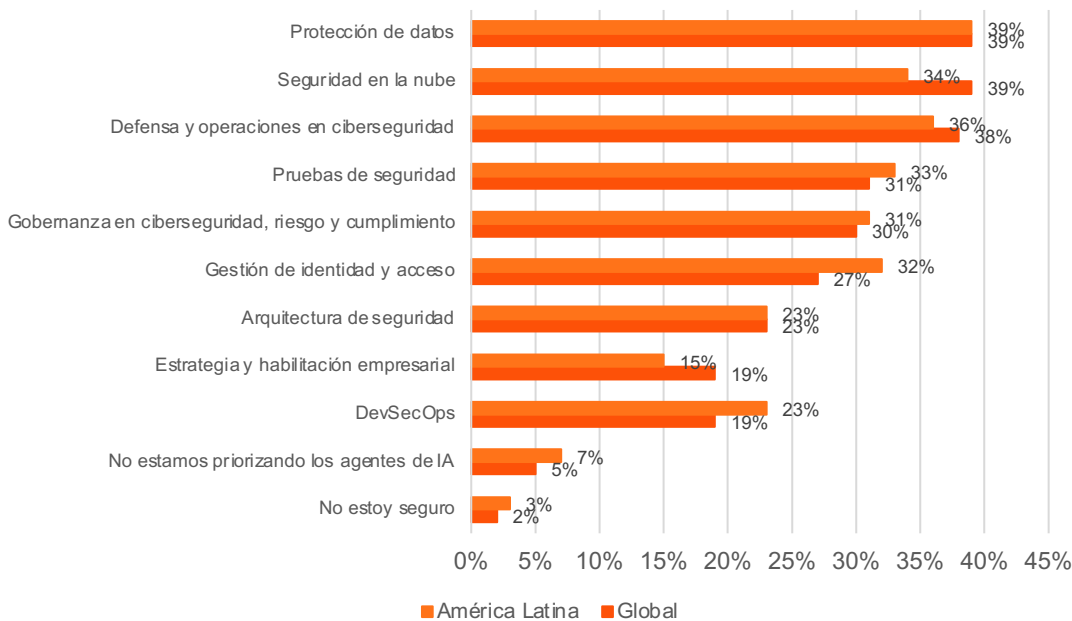
Agentes de cambio en la ciberdefensa

Las empresas están reconociendo que **los agentes de IA** —sistemas autónomos y orientados a objetivos, capaces de ejecutar tareas con una intervención humana limitada— tienen un enorme potencial para transformar sus programas de ciberseguridad. Estos sistemas de IA ya no son solo herramientas que proporcionan análisis, sino que están evolucionando hacia asistentes digitales que pueden actuar de forma independiente, colaborar con equipos humanos e incluso iniciar respuestas de seguridad, lo que impulsa tanto la eficiencia como la productividad.

Por eso los responsables de seguridad sitúan a los agentes de IA entre las principales capacidades de seguridad de IA que sus organizaciones priorizarán en los próximos 12 meses.

¿Dónde tienen previsto implementar estas soluciones de agentes? La seguridad en la nube, la protección de datos y la ciberdefensa, y las operaciones se sitúan como las principales áreas prioritarias de seguridad para los agentes de IA durante el próximo año. Otras áreas prioritarias son las pruebas de seguridad, la gobernanza, el riesgo, el cumplimiento (GRC) cibernético y la gestión de identidades y accesos.

Prioridades del agente de IA para aumentar la eficiencia y la productividad
Comparativo Global vs. América Latina (Porcentaje que situó entre sus tres prioridades principales)



P19. ¿En cuáles de las siguientes áreas dará prioridad tu organización a la IA agencial para aumentar la eficiencia y la productividad en los próximos 12 meses?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC.



Gestión del riesgo de los datos de IA

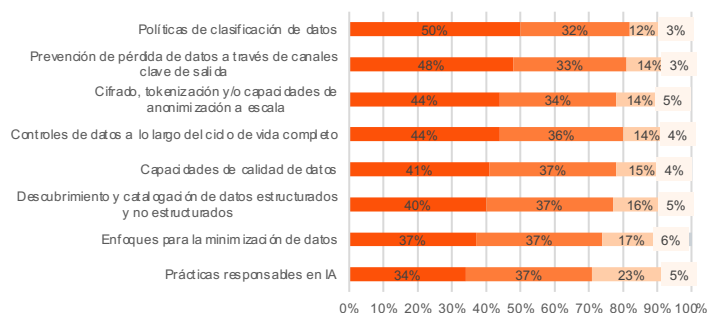
El despliegue y el uso exitoso de la IA no pueden darse sin prácticas sólidas de gestión **de riesgos de datos**. Esto se debe a que las soluciones de IA eficaces dependen del acceso a conjuntos de datos seleccionados y de alta calidad, así como de una gobernanza y una seguridad sólidas en toda la empresa para confirmar que esos conjuntos de datos se utilizan en el contexto adecuado.

¿Están las organizaciones preparadas para afrontar este reto? Cuando se les preguntó a los encuestados sobre sus avances en la implementación de diversas medidas de riesgo de datos en toda la empresa, solo alrededor de la mitad había implementado plenamente políticas de clasificación de datos a nivel global (50 %) y en América Latina (51 %) prevención de pérdida de datos en los principales canales de salida a nivel global (48 %) y en América Latina (55 %), mientras que otras medidas obtuvieron puntuaciones aún más bajas. Es más, solo el 6 % a nivel global había implementado todas las medidas encuestadas en toda la empresa.

Esta brecha en la preparación muestra el trabajo que tienen por delante las organizaciones para maximizar el potencial de sus datos y poder utilizarlos en soluciones de IA. Generar **una sólida confianza digital** mediante prácticas de datos transparentes, responsables y seguras será clave para aprovechar la innovación y el crecimiento impulsados por la IA.

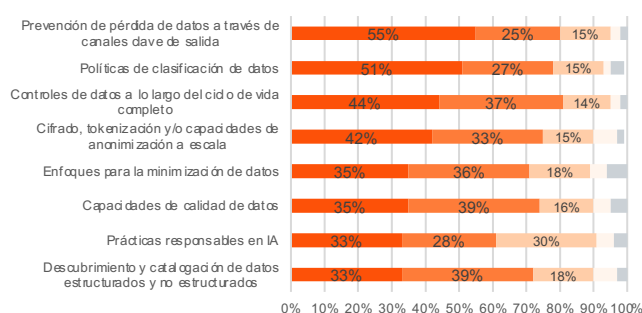
Aplicación de medidas para abordar el riesgo de los datos

Global



- Implementado en toda la organización
- Implementado en partes de la organización
- Planeando implementar en los próximos 12 meses
- Sin planes
- No seguro / no aplicable

América Latina



P5. ¿En qué medida ha implementado tu organización o tiene previsto implementar alguna de las siguientes medidas para abordar el riesgo de los datos en toda la empresa?
Base: responsables de seguridad, CFO, directores financieros, CDO, directores/GC/CLO, CRO, CAE y directores de auditoría interna = 2.395.
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC.

04

Preparación para la
computación cuántica

Preparación para amenazas de próximo nivel



Top 4

De las amenazas que las organizaciones están menos preparadas para abordar en la actualidad incluyen la computación cuántica.

49 %

de las organizaciones no han considerado ni han comenzado a implementar ninguna medida de seguridad resistente a la computación cuántica.

Solo el 8 %

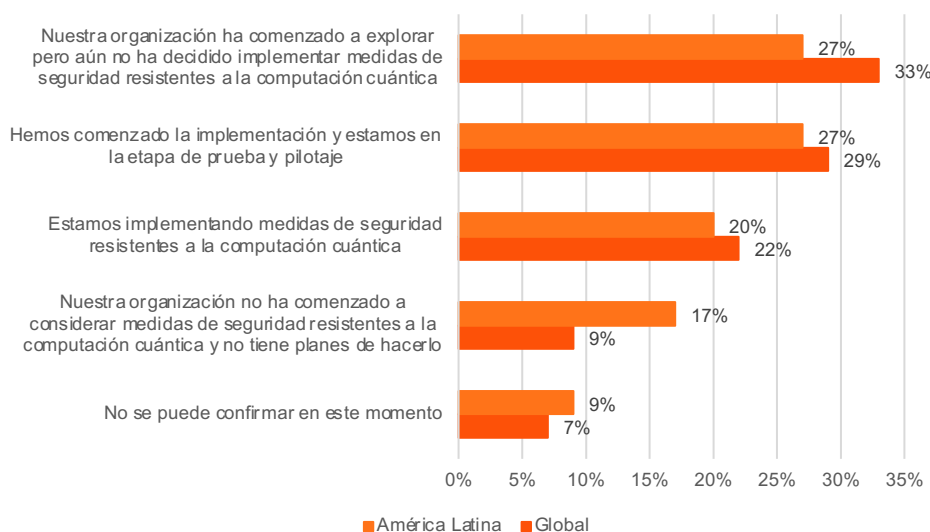
de los líderes de seguridad incluyen la preparación cuántica entre sus tres principales prioridades presupuestarias.

La cuenta atrás para la computación cuántica ha comenzado. Ya no es algo teórico, está saliendo de los laboratorios y ya está introduciendo nuevas formas de ayudar a resolver problemas complejos, como la modelización financiera y la optimización logística, al tiempo que está redefiniendo supuestos que se han mantenido durante décadas en materia de ciberseguridad.

Aunque la tecnología cuántica no supone una amenaza a la ciberseguridad inmediata, quienes retrasen la transición a **la criptografía poscuántica** podrían estar exponiendo sus datos confidenciales, sus servicios de autenticación y sus sistemas criptográficos. Dado que los plazos de implementación se prolongan durante años, sentar las bases para una seguridad resistente a la tecnología cuántica exige actuar hoy para evitar perturbaciones adversas mañana.

Algunas organizaciones están dando los primeros pasos (29 % a nivel global y un 27 % en América Latina) llegando a fase piloto y de pruebas. Sin embargo, solo el 22 % en global y 20 % en la región ha superado la fase piloto, y casi la mitad en global (49 %) y más de la mitad en América Latina (53 %) no ha considerado ni comenzado a implementar ninguna medida de seguridad resistente a la computación cuántica ¿Qué los frena? Para muchos, es la falta de comprensión de los riesgos poscuánticos, junto con los recursos internos limitados y las demandas competitivas.

Progreso en materia de seguridad resistente a la computación cuántica Comparativo Global vs. América Latina



29 %

de los líderes empresariales y tecnológicos en Colombia ha comenzado a explorar y a iniciado a implementar medidas seguras contra ataques cuánticos.

P21: ¿En qué punto se encuentra tu organización en lo que respecta a las medidas de seguridad resistentes a la computación cuántica?
Base: Todos los encuestados = 3.887

Fuente: Encuesta Global Digital Trust Insights 2026 de PwC.

Aumenta la preocupación por la cuántica, pero la preparación se queda atrás

La conciencia sobre las amenazas cuánticas está aumentando. La computación cuántica se encuentra ahora entre las cuatro principales amenazas para las que las organizaciones se sienten menos preparadas, lo que supone un avance de varios puestos con respecto al año pasado.

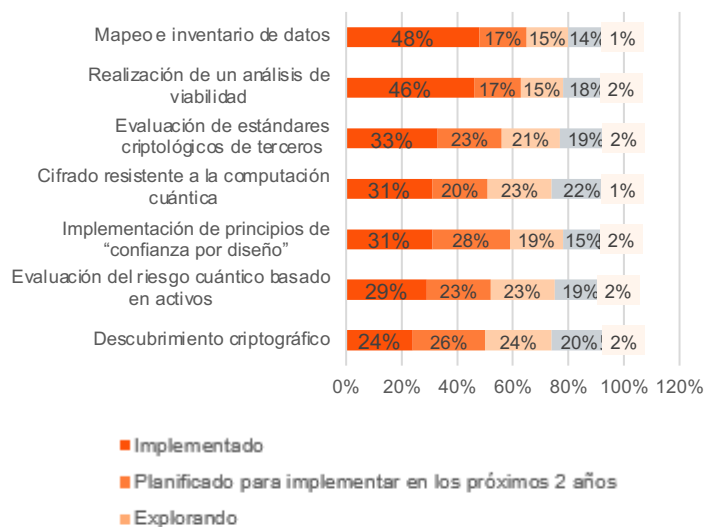
¿Pero estas preocupaciones se están traduciendo en acciones? Si bien, aproximadamente un tercio de los encuestados a nivel global ha implementado una o más medidas de seguridad resistentes a la computación cuántica, solo el 3 % ha implementado las siete medidas encuestadas. Aunque estas medidas no son exhaustivas, son prácticas fundamentales en un proceso de varios años que requieren atención inmediata. De cara al futuro, solo el 8 % de los responsables de seguridad incluyen la preparación para la computación cuántica entre sus tres principales prioridades presupuestarias para el próximo año.

Las organizaciones con ingresos superiores a USD\$ 5 billones son más propensas a haber implementado estas medidas, entre las que se incluyen un inventario de datos para mitigar el riesgo de “recoger ahora, descifrar después”, el descubrimiento criptográfico para identificar activos criptográficos vulnerables, la prueba e implementación de cifrado resistente a la computación cuántica y la realización de análisis de viabilidad y evaluaciones de riesgos cuánticos. Las empresas de mayor crecimiento también están reconociendo el desafío cibernético que plantea la computación cuántica y se están posicionando en consecuencia.

Pero siguen siendo la excepción. A medida que avanza la tecnología, la capacidad de adoptar rápidamente la criptografía resistente al quantum está llamada a convertirse en una capacidad empresarial determinante.

Implementación de medidas de seguridad resistentes a la computación cuántica

Global



América Latina



¿Por qué es difícil la criptografía poscuántica?

La preparación cuántica no es solo una actualización técnica, sino un cambio fundamental y estratégico hacia prácticas de seguridad preparadas para el futuro. ¿Cuáles son las principales barreras internas? Los vacíos en los conocimientos técnicos, el conocimiento institucional limitado y los sistemas heredados rígidos.

A medida que las organizaciones establecen inventarios criptográficos para comenzar la transición a la criptografía resistente a la tecnología cuántica, deben identificar los algoritmos vulnerables en toda su pila tecnológica. Si bien se entiende ampliamente que el cifrado de clave pública es vulnerable dado el principio de “recoger ahora, descifrar después”, los responsables de seguridad deben ser conscientes de las tecnologías en las que confían para la autenticación y las firmas digitales que utilizan algoritmos criptográficos igualmente vulnerables.

Estos obstáculos dejan una cosa clara: incluso cuando se prioriza, iniciar un inventario criptográfico e implementar una criptografía resistente a la computación cuántica lleva tiempo. Y el tiempo es escaso. Las principales normas de cifrado del sector, como las del Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU., recomiendan descartar los algoritmos vulnerables antes de que los actores maliciosos adquieran capacidades de computación cuántica. Por eso es fundamental que las empresas cubran sus vacíos de conocimiento, evalúen sus dependencias criptográficas y elaboren una hoja de ruta para estar preparadas.

Retos para lograr la criptografía poscuántica

Comparativo Global vs. América Latina (Porcentaje que lo situó entre sus tres principales retos)



05

Talento y
habilidades en
ciberseguridad

Los servicios gestionados pasan a primera línea



Top 2

de los retos para implementar la IA en la ciberdefensa son las carencias de conocimientos y habilidades.

53 %

sitúa las herramientas de IA y aprendizaje automático entre sus tres prioridades principales para abordar las carencias de talento en ciberseguridad en los próximos 12 meses.

48 %

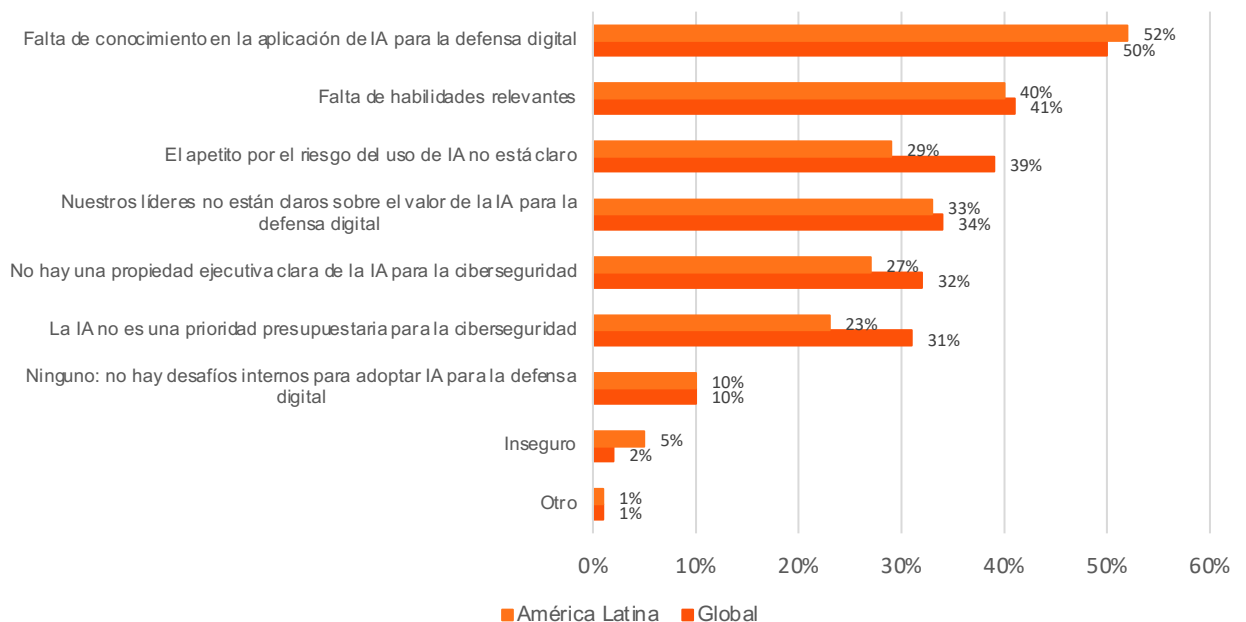
de las organizaciones que han sufrido un ataque grave están dando prioridad a los servicios gestionados para abordar las carencias de talento en ciberseguridad.

La escasez de personal especializado en ciberseguridad sigue obstaculizando el progreso, especialmente ahora que las organizaciones se esfuerzan por poner en marcha la IA, proteger entornos complejos y prepararse para las amenazas de próxima generación.

Las carencias de conocimientos y habilidades fueron las dos principales barreras para la implementación de la IA en la ciberdefensa durante el último año, lo que obligó a las organizaciones a replantearse cómo ampliar sus capacidades. A nivel global, muchas están explorando nuevas formas de adquirir competencias, entre ellas herramientas de IA (52 %), herramientas de automatización de la seguridad (48 %), consolidación de herramientas cibernéticas (47 %) y la mejora o el reciclaje de las competencias (47 %). También están dando prioridad a los servicios gestionados especializados, especialmente aquellas organizaciones que han sufrido un ataque importante (48 %).

Retos de la implementación de la IA para la ciberdefensa

Comparativo Global vs. América Latina (% que lo clasificó entre sus tres principales retos)



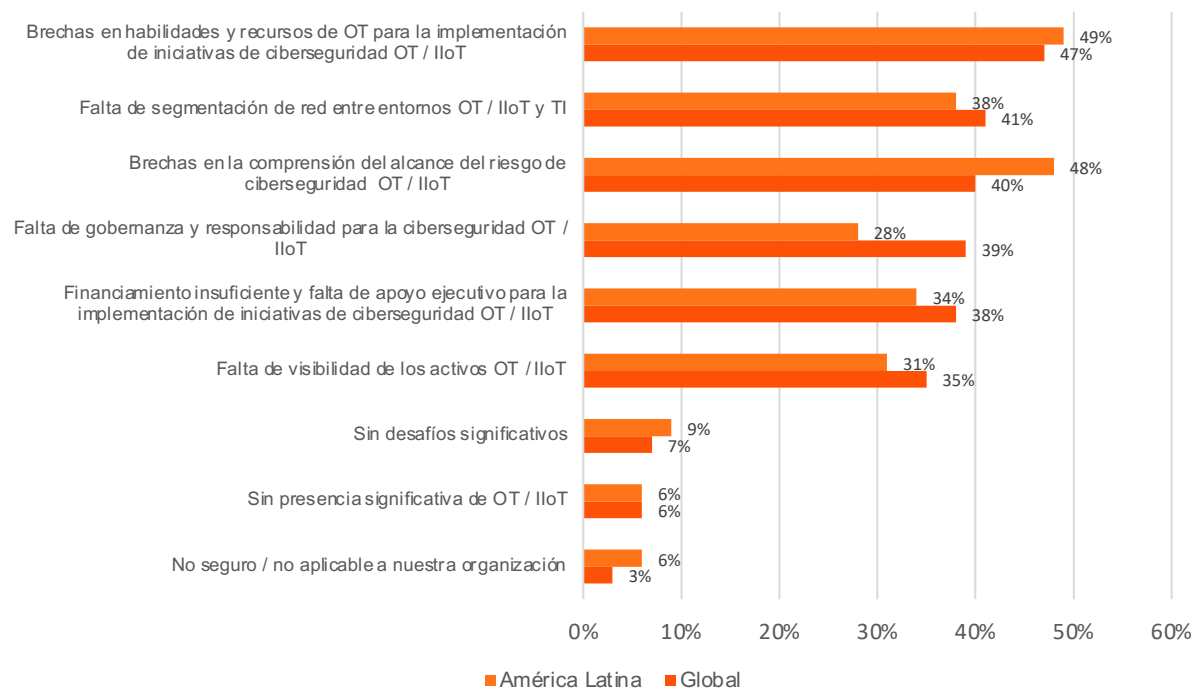
P20. ¿Cuáles han sido los mayores retos internos de tu organización a la hora de implementar la IA para la ciberdefensa en los últimos 12 meses?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC.

Se buscan: habilidades en tecnología operativa

La tecnología operativa (OT, por sus siglas en inglés) y el Internet industrial de las cosas (IIoT, por sus siglas en inglés) se han convertido en puntos críticos en el panorama actual de la seguridad. Casi la mitad (47 % global y 49 % en América Latina) de los líderes citan la falta de personal cualificado entre sus tres principales retos, mientras que el 39 % en global y 28 % en la región señala la falta de claridad en la gobernanza y la propiedad. En conjunto, estas discrepancias ponen de manifiesto un problema más profundo: muchas organizaciones siguen careciendo de la estructura y los conocimientos necesarios para gestionar con confianza unos sistemas operativos cada vez más conectados.

Obstáculos para la seguridad de los sistemas OT e IIoT

Comparativo Global vs. América Latina (% que los clasificó entre sus tres principales obstáculos)



P4. ¿Cuáles son los tres principales retos a los que se enfrenta tu organización a la hora de proteger los sistemas de tecnología operativa (OT) y/o el Internet industrial de las cosas (IIoT)?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC.



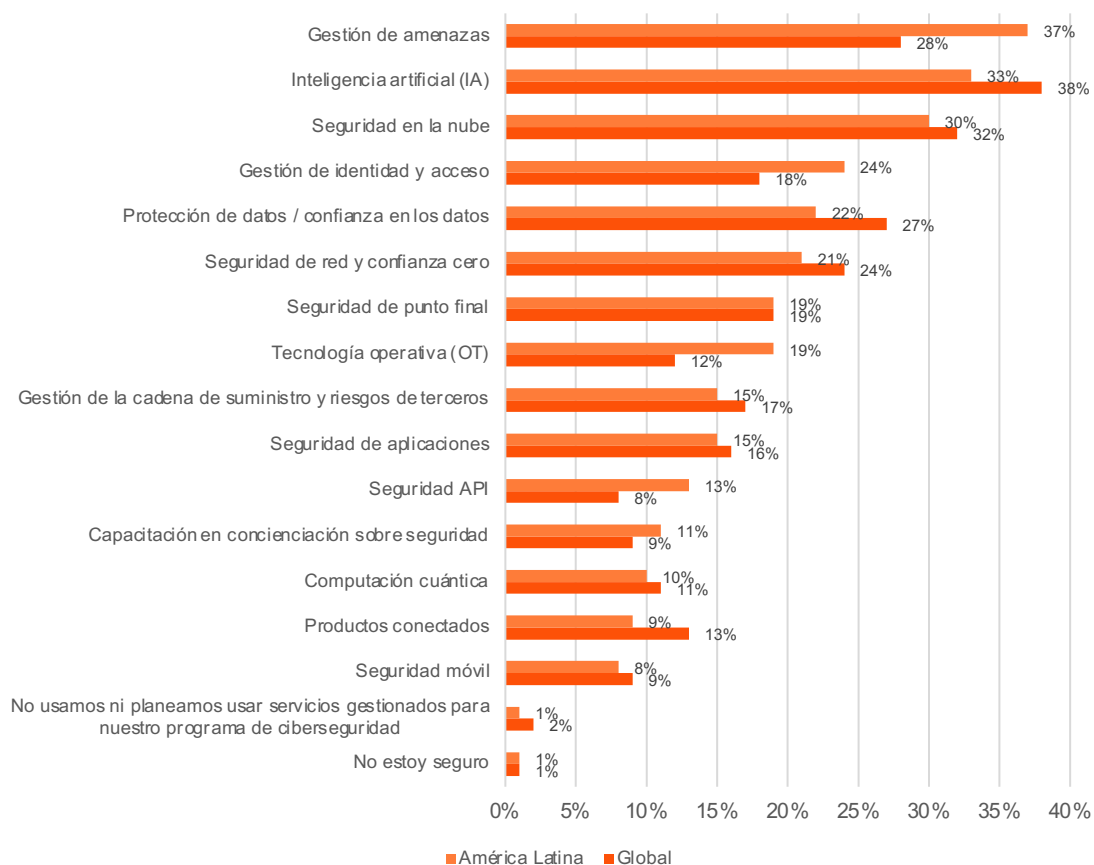
Los servicios gestionados como acelerador estratégico

A nivel global, la inteligencia artificial y la seguridad en la nube no solo representan las principales áreas de inversión en ciberseguridad, sino que también constituyen los principales casos de uso para los servicios gestionados especializados. En cambio, en América Latina, las prioridades se centran en la inteligencia artificial y la gestión de amenazas. Las organizaciones utilizan los servicios gestionados para algo más que externalizar capacidades. Se asocian con proveedores para modernizar la forma en que se suministran los sistemas críticos.

Los servicios gestionados se están convirtiendo en aceleradores estratégicos, que intervienen para compensar la falta de habilidades y proporcionar velocidad, escala y conocimientos especializados. En un entorno de amenazas cada vez más complejo, ofrecen una forma de modernizar las defensas sin desviar la atención de la innovación y el crecimiento.

Prioridades de ciberseguridad para el uso de servicios gestionados

Comparativo Global vs. América Latina (% que los clasificó entre sus tres prioridades principales)



P15. ¿Cuál de las siguientes áreas de tus programas de ciberseguridad, si hay alguna, es prioritaria para tu organización a la hora de utilizar servicios gestionados durante los próximos 12 meses?

Fuente: Encuesta Global Digital Trust Insights 2026 de PwC.



Manual para altos ejecutivos

De la incertidumbre a la acción

Qué pueden hacer los líderes ahora

La encuesta de este año muestra que las organizaciones con más visión de futuro están alineando la ciberseguridad con la estrategia empresarial y dando prioridad a la preparación frente a la reactividad.

Muchos ya han establecido prácticas fundamentales de gestión de riesgos en ciberseguridad mediante el refuerzo de una estructura de gobernanza que se ajusta a los principales marcos digitales, la incorporación de controles de riesgos ciberseguridad en toda la empresa y la priorización de las evaluaciones y los informes de riesgos.

Sin embargo, para estar preparados para el futuro, será necesario ir más allá de lo habitual. Eso significa afrontar la incertidumbre, tomar decisiones audaces pero informadas e incorporar la agilidad en la estrategia.

CISO/CSO

La capacidad no solo para traducir los complejos riesgos en ciberseguridad en riesgos empresariales, sino también para comunicar de manera eficaz que la ciberseguridad es una responsabilidad compartida, es clave para garantizar la aceptación y la colaboración de los altos directivos. Este entendimiento compartido ayudará a fomentar prácticas fundamentales de gobernanza, resiliencia, cumplimiento normativo y respuesta. De cara al futuro, se debe abordar de forma proactiva los nuevos riesgos promoviendo una mentalidad de seguridad desde el diseño y utilizando los datos para medir y mostrar dónde se necesitan más inversiones en ciberseguridad.

Fundamental

Cuantificar la exposición al riesgo geopolítico utilizando métricas vinculadas a infraestructuras críticas, operaciones globales y perturbaciones específicas del sector específicas de la industria, y compartir los resultados con la C-Suite.

Implementar modelos dinámicos de amenazas alineados con la inteligencia actual sobre regiones de alto riesgo, campañas de amenazas cibernéticas y tendencias de extorsión de datos.

Incorporar los principios **de IA responsable** en todas las implementaciones de IA y clasificar los sistemas de IA (incluidos los modelos, los agentes y sus identidades, las aplicaciones y los datos de entrenamiento) en función de su sensibilidad, criticidad y exposición.

Proteger la IA ampliando los controles de seguridad existentes a los sistemas de IA e identificando las lagunas en las que se requieren nuevas capacidades (por ejemplo, barreras de protección de IA o puertas de enlace LLM).

Reexaminar y actualizar periódicamente los modelos de gobernanza de riesgos en ciberseguridad para incorporar los riesgos tecnológicos en evolución, como la IA y la cuántica.

Fortalecer la gobernanza mediante indicadores clave de rendimiento (KPI, por sus siglas en inglés) aplicables que permitan realizar un seguimiento del rendimiento en la gestión de riesgos de terceros, de la cadena de suministro, heredados y basados en la nube.

Realizar ejercicios de simulación y simulacros para poner a prueba la toma de decisiones, determinar las vías de escalamiento y validar los pasos de recuperación.

Preparados para el futuro

Establecer la ciberseguridad como una responsabilidad compartida con la alta dirección y el consejo de administración incorporando debates sobre gobernanza, además de información sobre amenazas y resúmenes a nivel ejecutivo de las amenazas emergentes y las capacidades de los adversarios.

Poner en práctica la supervisión y la gobernanza de los agentes de IA mediante el descubrimiento, la clasificación, el mapeo de la exposición y la supervisión continua, incluidas las simulaciones adversarias.

Pasar de las evaluaciones puntuales de los proveedores a la supervisión continua de los riesgos de terceros.

Evaluar qué sistemas dependen de la criptografía y adoptar estándares criptográficos poscuánticos (PQC) cuando sea necesario.

Determinar si la empresa debe aprovechar los servicios gestionados mediante el desarrollo de un plan de servicios gestionados basado en el retorno de la inversión que refleje las necesidades de tecnología, habilidades y recursos.

Evaluar los datos y determinar qué debe estar preparado para la tecnología cuántica ahora, y luego trabajar con los equipos de gobernanza de datos en la adopción de la tecnología cuántica.

CTO/CIO

El enfoque fundamental en **ampliar la tecnología de forma segura** y abordar de manera proactiva las carencias de talento y formación proporciona un apoyo fundamental a la postura cibernética de la organización. Se debe seguir colaborando estrechamente con los líderes de seguridad para integrar los controles de riesgo y la gobernanza en toda la adopción de tecnología. De cara al futuro, este cargo liderará los esfuerzos para poner a prueba e integrar tecnologías emergentes como la inteligencia artificial y la computación cuántica con seguridad integrada, al tiempo que impulsa la innovación que anticipa y mitiga los riesgos cibernéticos futuros.

Fundamental

Ampliar la IA y otras tecnologías emergentes de forma segura, presupuestando e incorporando medidas de seguridad proactivas críticas.

Colaborar estrechamente con el CISO y el CRO para alinear el despliegue tecnológico con los requisitos de gestión de riesgos y cumplimiento normativo.

Garantizar la seguridad de la IA incorporando controles de gobernanza y riesgos cibernéticos en la planificación de la implementación de la IA desde el principio, en consonancia con los principios de seguridad desde el diseño.

Aplicar controles coherentes de identidad, acceso y políticas en plataformas de terceros, API e integraciones.

Aplicar una sólida gobernanza de IIoT y OT en su estrategia de arquitectura para obtener visibilidad y controles de extremo a extremo en entornos distribuidos.

Preparados para el futuro

Coordinación con los CISO y los responsables de datos para proteger los datos de formación confidenciales y reforzar la gobernanza de las entradas y salidas de los modelos de IA.

Alinear la adopción cuántica y las iniciativas piloto con estrategias de seguridad resistentes a la cuántica en toda la empresa, en colaboración con los responsables de seguridad.

Impulsar la adopción de herramientas de detección y respuesta de riesgos basadas en la automatización y la IA para aumentar la eficiencia operativa y la resiliencia.

Adoptar un marco de seguridad desde el diseño para los productos conectados a lo largo de todo el ciclo de vida operativo.

CRO

El enfoque en identificar los riesgos empresariales y emergentes, así como sus interdependencias con la ciberseguridad, es fundamental para proteger a la organización. Se debe seguir adaptando los controles a las vulnerabilidades cambiantes, al tiempo que confirma que los marcos de riesgo siguen siendo actuales. De cara al futuro, esta función seguirá requiriendo la integración de la IA, la cuántica y las exposiciones geopolíticas en una estrategia de gestión de riesgos adaptable y con visión de futuro que respalde la agilidad y la resiliencia de la organización.

Fundamental

Incorporar escenarios basados en amenazas en los registros de riesgos y los ciclos de pruebas de estrés, dando prioridad a las amenazas con vectores geopolíticos conocidos.

Evaluar los controles existentes para abordar estas exposiciones, adaptando las estrategias de mitigación actuales cuando sea necesario.

Cuantificar los riesgos relacionados con la inteligencia artificial y la tecnología cuántica mediante análisis de impacto empresarial personalizados, dando prioridad a las áreas con **automatización digital de la fuerza laboral**.

Apoyar los esfuerzos de cumplimiento normativo mediante la adaptación de la gestión de las amenazas cibernéticas a los requisitos reglamentarios.

Preparados para el futuro

Ampliar los modelos de riesgo de terceros para tener en cuenta la capacidad cuántica en los entornos de los proveedores y la resiliencia ante el uso indebido de la IA adversaria.

Aprovechar la IA para evaluar continuamente el riesgo ciberseguridad a gran escala, desde la cuantificación del riesgo ciberseguridad hasta las evaluaciones y la presentación de informes.

Desarrollar un marco de riesgo integrado en inteligencia (IIRF) que incorpore diversas perspectivas de inteligencia estratégica sobre amenazas en la puntuación de riesgos empresariales.

Probar herramientas de modelización predictiva de amenazas para simular amenazas emergentes y cuantificar los posibles impactos en el negocio durante los próximos 12 a 36 meses.

CFO

El papel fundamental a la hora de garantizar una presupuestación adecuada para medidas en ciberseguridad proactivas en iniciativas estratégicas e implementaciones tecnológicas es esencial para la resiliencia de la organización. Se debe seguir identificando ineficiencias y alineando los presupuestos con iniciativas en ciberseguridad de alto impacto. De cara al futuro, prepararse para los riesgos emergentes significa planificar de forma proactiva las necesidades presupuestarias futuras y fomentar **modelos de financiación basados en el retorno de la inversión**, de modo que la organización pueda invertir de forma inteligente en tecnologías y habilidades de seguridad.

Fundamental

Apoyar las inversiones estratégicas que impulsen la resiliencia a largo plazo, la ventaja competitiva y la preparación normativa.

Evaluar los costes a largo plazo de reaccionar ante incidentes de seguridad frente a invertir de forma proactiva en ciberdefensas, servicios gestionados, seguros, cumplimiento normativo, etc.

Recalibrar las métricas de retorno de la inversión en ciberseguridad para incluir el ahorro derivado de la prevención de incidentes, las multas normativas evitadas y la reducción del tiempo de respuesta.

Colaborar con los CISO, los CTO y los CIO para elaborar presupuestos eficaces destinados al desarrollo de competencias en ciberseguridad y la formación tecnológica.

Apoyar modelos de financiación sostenibles que equilibren los costes operativos con las inversiones estratégicas en ciberseguridad.

Preparados para el futuro

Defender la ciberseguridad como una función empresarial importante, vinculando los niveles de inversión a los objetivos de rendimiento a nivel directivo.

Crear una reserva de asignación de capital para "facilitadores de la resiliencia", incluidas las capacidades de respuesta ante explotaciones de día cero y el refuerzo poscuántico.

Desarrollar casos de negocio basados en el retorno de la inversión para los servicios de seguridad gestionados.

Identificar y reducir ineficiencias, como la redundancia de herramientas, y consolidar siempre que sea posible.

CEO

El compromiso continuo para garantizar que la ciberseguridad sea una prioridad empresarial sigue siendo esencial. Se debe seguir alineando las iniciativas empresariales con la estrategia de gestión de riesgos en ciberseguridad, al tiempo que se fomenta la colaboración entre todos los niveles y la alta dirección. De cara al futuro, esta función consistirá en crear alianzas influyentes y promover inversiones que permitan a la organización afrontar los nuevos retos cibernéticos.

Fundamental

Exigir la participación en escenarios ciberseguridad en reuniones ejecutivas fuera de la oficina, simulando perturbaciones específicas del sector y operaciones de amenazas híbridas.

Vincular la resiliencia cibernética a la generación de ingresos, como la seguridad de las plataformas digitales, la confianza en los datos de los clientes y el crecimiento transfronterizo.

Promover la innovación responsable, confirmando que los proyectos de inteligencia artificial y cuántica incorporen medidas éticas y de seguridad desde su inicio.

Comprender dónde se realizan las compensaciones presupuestarias en ciberseguridad y si esas compensaciones satisfacen la propensión al riesgo.

Hacer de la ciberseguridad una responsabilidad compartida en todos los niveles, desde la sala de juntas hasta la trastienda.

Mantener al directorio informado sobre las prioridades estratégicas del programa cibernético e involucrar a los directores para debatir las necesidades del programa.

Preparados para el futuro

Liderar alianzas multisectoriales para la estandarización poscuántica, las posturas de defensa conjunta y el intercambio de inteligencia sobre amenazas.

Promover la inversión en tecnologías emergentes (IA, cuántica) con seguridad diseñada desde el principio.

Institucionalizar las revisiones de previsión cuántica y geopolítica en los ciclos de planificación estratégica y las cartas de riesgo de la junta directiva.

Participar activamente en pruebas de resistencia para prepararse ante perturbaciones geopolíticas y tecnológicas.

Acerca de este informe

La encuesta Global Digital Trust Insights 2026 se ha diseñado para obtener las opiniones de 3.887 ejecutivos del ámbito empresarial y tecnológico, y se ha llevado a cabo entre mayo y julio de 2025.

Un tercio de los ejecutivos (33 %) proceden de grandes empresas con ingresos de US\$ 5.000 millones o más. Los encuestados operan en una amplia gama de sectores, entre los que se incluyen los servicios financieros (21 %); la fabricación industrial y la automoción (21 %); la tecnología, los medios de comunicación y las telecomunicaciones (19 %); el comercio minorista y los mercados de consumo (16 %); la sanidad (10 %); la energía, los servicios públicos y los recursos (9 %); y los servicios gubernamentales y públicos (4 %).

Los encuestados proceden de 72 países. El desglose regional de las respuestas es el siguiente: Europa Occidental (32 %), América del Norte (27 %), Asia-Pacífico (18 %), América Latina (11 %), Europa Central y Oriental (6 %), África (4 %) y Oriente Medio (3 %).

La encuesta Global Digital Trust Insights se conocía anteriormente como Global State of Information Security Survey (GSISS). Ahora, en su 28.^a edición, es la más antigua sobre tendencias en ciberseguridad. También es la encuesta más grande del sector de la ciberseguridad y la única en la que participan altos ejecutivos de empresas, y no solo ejecutivos de seguridad y tecnología.

PwC Research, el centro de excelencia global de PwC para la investigación y el análisis de mercados, ha llevado a cabo esta encuesta.



Contáctanos



Carlos Rodríguez

Director de Consultoría en Ciberseguridad,
PwC Colombia

carlos.andres.rodriguez.castillo@pwc.com
[LinkedIn](#)

En PwC, nuestro propósito es generar confianza en la sociedad y resolver problemas importantes. Somos una red de firmas en 149 países con más de 370,000 personas comprometidas con brindar calidad en los servicios de auditoría, consultoría e impuestos. Encuentra más información y contáctanos a través de nuestro sitio web: www.pwc.com/co.

© 2025 PricewaterhouseCoopers. PwC se refiere a las firmas colombianas que hacen parte de la red global de PricewaterhouseCoopers International Limited, cada una de las cuales es una entidad legal separada e independiente. Todos los derechos reservados.