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

Encuesta Digital Trust Insights 2026: Hallazgos Latinoamérica

62%

está aumentando la inversión en riesgos cibernéticos en respuesta a la volatilidad geopolítica

#1

la seguridad de la nube es la principal prioridad en inversión cibernética para líderes de seguridad

Top 2

desafíos para implementar la IA para la ciberdefensa son las brechas de conocimientos y habilidades

La ciberseguridad se adentra en terreno desconocido. Un orden mundial en constante cambio y un entorno de amenazas, impulsados por los recientes avances tecnológicos exponenciales, están poniendo a prueba las estrategias cibernéticas.

Las organizaciones se enfrentan a la nueva realidad de la era posglobalización, marcada por alianzas fracturadas, instituciones globales debilitadas, impactos arancelarios y cadenas de suministro interrumpidas. Estamos presenciando avances tecnológicos sin precedentes que amplían las superficies de ataque e introducen nuevas ciberamenazas, muchas de ellas impulsadas por gobiernos.

Toda esta incertidumbre obliga a los ejecutivos a reevaluar sus capacidades, talento y tecnología. Más aún, los impulsa a revisar su estrategia cibernética, incluyendo dónde operan y con quién hacen negocios.

La encuesta Global Digital Trust Insights 2026 de PwC, realizada a 3,887 ejecutivos de empresas y tecnología en 72 países, revela cómo los líderes están gestionando esta era de incertidumbre, en qué aspectos se están quedando atrás y qué podrían hacer de forma diferente para afrontar mejor el desafío. Entre las principales conclusiones:

- **El riesgo geopolítico está moldeando la estrategia:** 62% de los líderes empresariales y tecnológicos clasifican la inversión en el riesgo cibernético entre sus tres principales prioridades estratégicas en respuesta a la incertidumbre geopolítica actual.
- **La resiliencia es un proceso en desarrollo:** Dado el panorama geopolítico actual, la mitad afirma que su organización es “muy capaz" de resistir ciberataques dirigidos a vulnerabilidades específicas.
- **Esperando problemas:** Solo 26% de las organizaciones invierte significativamente más en medidas proactivas (p. ej., monitorización, evaluaciones, pruebas, controles) que en medidas reactivas (respuesta a incidentes, multas, recuperación). Esa es la proporción ideal de gasto. La mayoría de las empresas (64%) invierten cantidades aproximadamente iguales en ambas categorías, lo que puede ser más costoso y arriesgado.
- **Agentes de IA para ciberdefensa:** La IA agentiva se encuentra entre las principales capacidades de seguridad de IA que las organizaciones priorizan durante los próximos 12 meses. Planean implementar estos agentes

en áreas clave como la seguridad en la nube, la protección de datos y la defensa y operaciones cibernéticas, entre otras.

- **El reloj cuántico está corriendo:** Aunque la computación cuántica se ubica entre las seis principales amenazas que las organizaciones se sienten menos preparadas para abordar, solo el 5% la prioriza en sus presupuestos.
- **Replanteando la crisis de talento cibernético:** La escasez de habilidades sigue siendo uno de los mayores obstáculos para el progreso cibernético. Más de la mitad (54%) prioriza las herramientas de IA y aprendizaje automático para ayudar a cerrar brechas de capacidad, y los servicios gestionados especializados se están convirtiendo en aceleradores estratégicos para proporcionar experiencia y escalabilidad.

Afrontar el momento actual requerirá una renovada urgencia, creatividad y enfoques distintos, no una mentalidad tradicional. Nuestro manual para directivos traduce las conclusiones de este año en medidas prácticas, ayudando a las partes interesadas a fortalecer sus prácticas fundamentales de seguridad e implementar acciones preparadas para el futuro, adaptadas a un mundo en constante evolución.

Tabla de contenido

01

Panorama de riesgos y amenazas

La geopolítica está transformando las vulnerabilidades cibernéticas

62%

está aumentando la inversión en riesgos cibernéticos en respuesta a la volatilidad geopolítica

55%

ha implementado la prevención de pérdida de datos en los principales canales de salida a nivel organizacional

Top 2

ciberamenazas que las organizaciones están menos preparadas para afrontar son los ataques a la nube y operaciones de piratería y filtración

Los riesgos cibernéticos actuales están condicionados tanto por la geopolítica como por las tecnologías disruptivas. Alianzas alteradas, disputas comerciales, instituciones internacionales debilitadas y otras tendencias desestabilizadoras en esta nueva era de competencia estratégica están transformando el entorno de amenazas, así como los métodos tradicionales de hacer negocios.

En respuesta a este clima geopolítico, el 62% de los líderes empresariales y tecnológicos han puesto la inversión en riesgos cibernéticos como una de sus tres principales prioridades estratégicas para el próximo año. También priorizan los cambios en las políticas comerciales y operativas (40%), la ubicación de infraestructuras críticas (31%) y las pólizas de seguros cibernéticos (29%). Con la disrupción como norma, la ciberseguridad es un factor clave para la resiliencia.

Cambios en la estrategia cibernética en respuesta al panorama geopolítico actual
(% que se ubicó en sus 3 áreas principales)

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

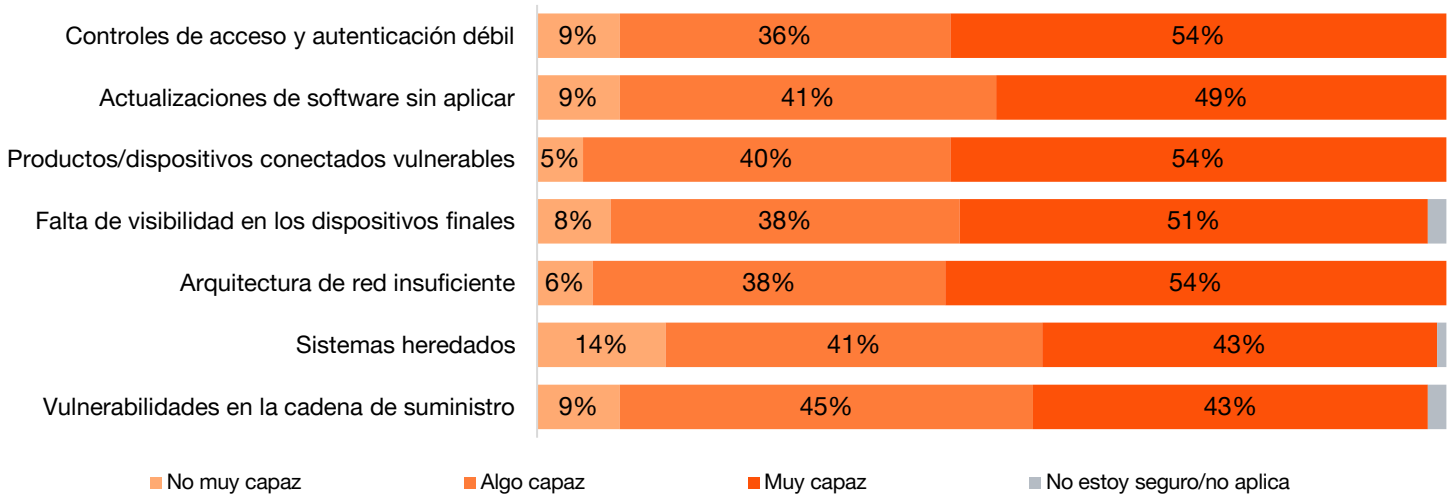
Sentirse seguro vs. estar seguro

Dado el panorama geopolítico actual, la confianza en la preparación cibernética parece estar en aumento. Aunque la mitad de los encuestados afirma que sus organizaciones son “muy capaces” de resistir ciberataques dirigidos a vulnerabilidades específicas, el 9 % considera que no lo está.

Según los datos, el 67 % de las empresas del sector de servicios financieros indica que su organización es muy capaz de enfrentar la falta de visibilidad en los dispositivos finales, mientras que el 66 % del sector de consumo señala estar muy preparado para abordar la autenticación débil y el control de acceso.

Los sistemas heredados se mantienen entre los puntos más vulnerables en todos los sectores.

Capacidad para resistir un ciberataque importante



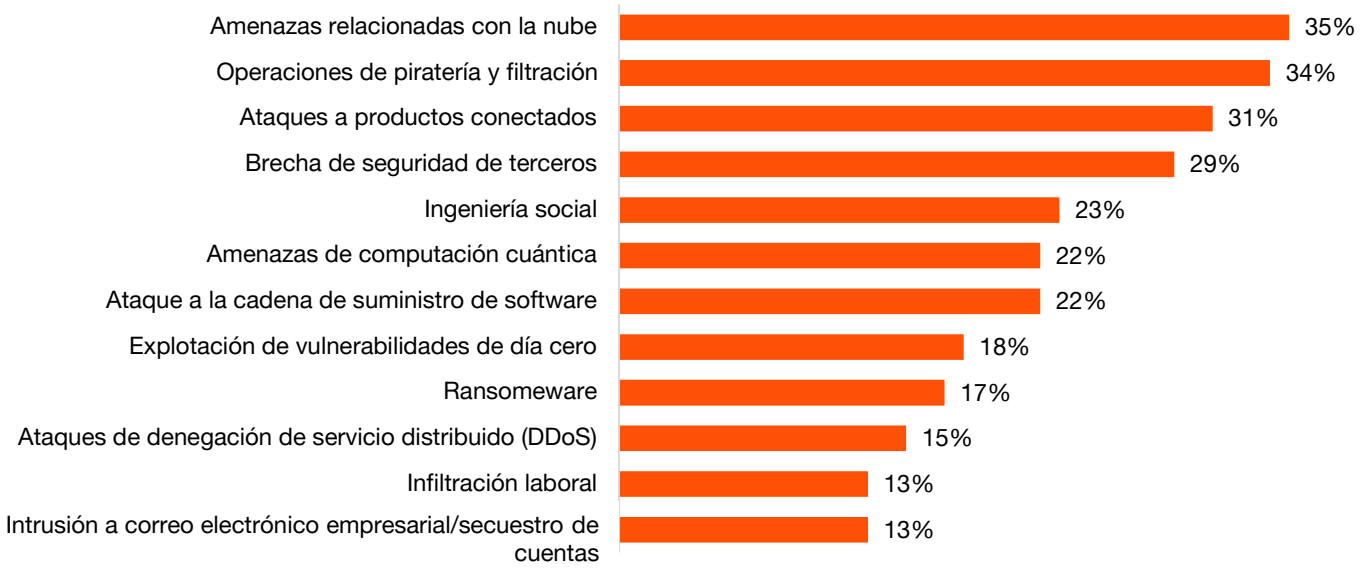
P3. Dado el panorama geopolítico actual, ¿qué tan capaz es su organización de resistir un ciberataque importante dirigido a las siguientes vulnerabilidades?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC

Brechas persistentes, riesgos crecientes

Más allá de las vulnerabilidades mencionadas, los líderes expresan preocupación por su capacidad para enfrentar amenazas específicas. Los ataques a la nube y a productos conectados siguen entre las principales preocupaciones, similar a los hallazgos del año pasado, ya más de una tercera parte de los líderes los ubica entre las tres principales ciberamenazas que su organización está menos preparada para afronta.

Estos riesgos no son nuevos, pero la expansión de los adversarios basados en IA, reflejan los desafíos persistentes para cerrar brechas críticas en gobernanza, control y visibilidad. Con el aumento de la complejidad de la tecnología y el ecosistema, muchas organizaciones se esfuerzan por mantener el ritmo, especialmente en dependencias de terceros y de la cadena de suministro.

Las organizaciones están menos preparadas para afrontar las ciberamenazas
(% que se ubicó entre sus 3 principales amenazas)



P1. ¿Cuál de estas ciberamenazas considera que su organización está menos preparada para afrontar en los próximos 12 meses?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC

Aprendiendo de la manera difícil

El año pasado, el 16% de los ejecutivos indicó que la filtración de datos más perjudicial de los últimos tres años costó a su organización menos de 500 mil dólares estadounidenses. Este año, más de una cuarta parte (29%) señala que el costo ha sido inferior a 100 mil dólares.

¿Quiénes son las más expuestas? El 42% de las empresas con ingresos superiores a 5 billones de dólares estima que el impacto superó 1 millón de dólares, mientras que el 35% de las compañías del sector de servicios financieros reporta costos menores a 100 mil dólares. Para estas organizaciones, la escala y la complejidad de sus operaciones incrementan la probabilidad de incidentes de alto costo.

Ante los retos de la recuperación, las organizaciones que han sufrido ataques significativos están aplicando las costosas lecciones aprendidas e implementando prácticas más estrictas de minimización de datos en toda la empresa.

02

Estrategia y operaciones cibernéticas

Donde la inversión se encuentra con el impacto

Solo 26%

gasta significativamente más en medidas de ciberseguridad proactivas que reactivas

79%

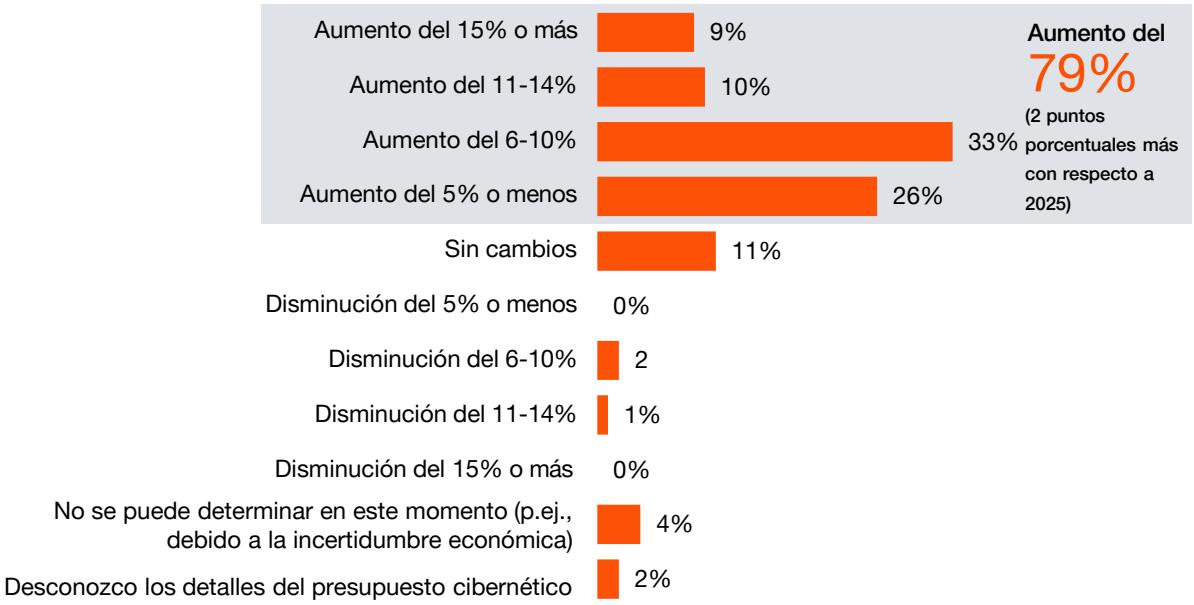
espera que su presupuesto cibernético aumente durante el próximo año

Solo 16%

mide de manera significativa el impacto financiero de los riesgos cibernéticos

¿Se están adaptando los presupuestos cibernéticos a los nuevos tiempos? El 78% de los encuestados afirman que su presupuesto cibernético aumentará durante el próximo año. Sin embargo, esta cifra prácticamente no ha variado respecto al año pasado (77%). Aunque los encuestados afirman estar incrementando la inversión en riesgos cibernéticos en respuesta al panorama geopolítico actual, esto podría ir en detrimento de otras prioridades de gasto.

Cambio en el presupuesto cibernético en 2026



P8. ¿Cómo cambiará el presupuesto cibernético de su organización en 2026?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC

El costo de prepararse vs. reaccionar

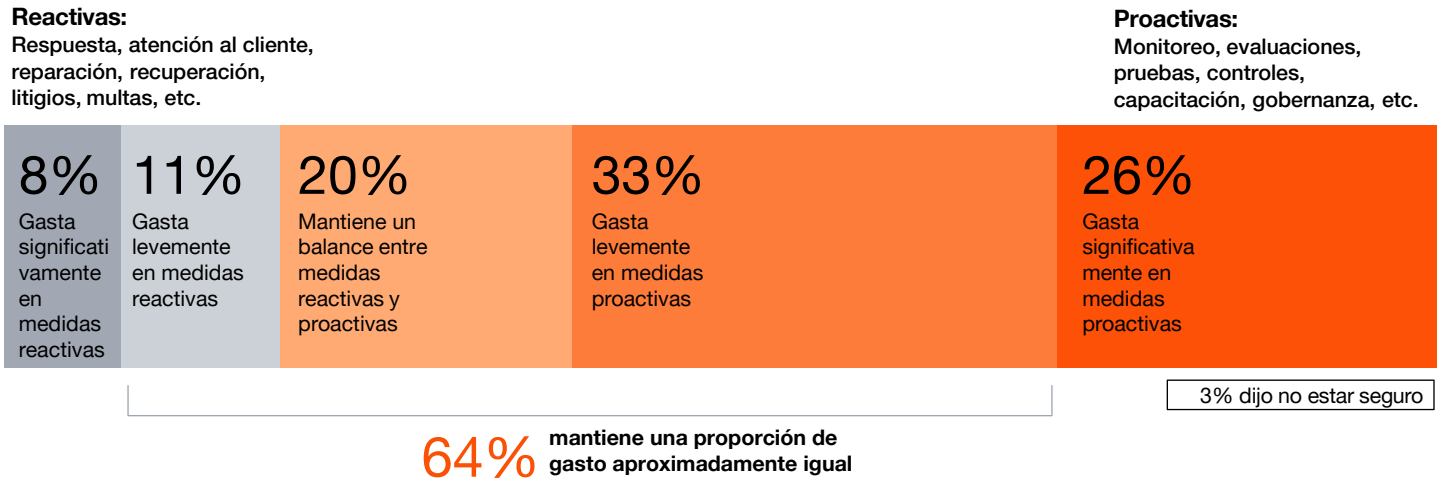
La ciberseguridad se fundamenta en la preparación. Esto implica planificar con antelación e invertir en medidas proactivas como la monitorización, las evaluaciones, las pruebas, los controles y la formación, antes de que se produzca una crisis. La alternativa, basada principalmente en medidas reactivas (p. ej., respuesta, atención al cliente, remediación, recuperación, litigios y multas), es más costosa, arriesgada e insostenible.

El 64% de las organizaciones afirman que su relación de costos proactivos/reactivos es prácticamente igual: gastan aproximadamente lo mismo en medidas cibernéticas proactivas y reactivas, o un poco más en cualquiera de ellas. Solo el 26% está en el punto óptimo de invertir significativamente más en medidas proactivas. Además, es probable que esas cifras subestimen el costo real de la reacción. Si bien el gasto proactivo se incluye en el presupuesto del responsable de seguridad y es fácil de rastrear, los costos reactivos se distribuyen por toda la empresa (legal, comunicaciones, operaciones, TI, etc.) e incluyen

costos más difíciles de cuantificar, como oportunidades perdidas y daño a la reputación.

Invertir en medidas proactivas no servirá de nada si se enfoca en los riesgos equivocados o no es lo suficientemente ágil para adaptarse a nuevas condiciones. Una preparación real exige un conocimiento profundo del panorama de riesgos y amenazas, que influya en la estrategia cibernética de la empresa, en el personal que contrata y en los procesos, sistemas y herramientas que adopta.

Gasto en medidas reactivas vs proactivas



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

Mapeo de prioridades de inversión frente a la preparación

La IA y la seguridad en la nube son las dos principales prioridades presupuestarias en materia de ciberseguridad para el próximo año. No es de extrañar, pues la nube, como se mencionó antes, también encabeza la lista de amenazas frente a las cuales los líderes se sienten menos preparados para abordar. Se está reconociendo la brecha entre el riesgo y la preparación, y la financiación está en consonancia.

Pero el panorama no está completo. Los ataques a productos conectados son la segunda área donde las organizaciones se sienten menos preparadas, y aun así muy pocas están asignando presupuesto para ello. Esta disparidad sugiere que algunas amenazas aún pasan desapercibidas.

Los servicios gestionados de ciberseguridad son otra prioridad de financiación para muchas organizaciones. El 22% de los encuestados los sitúa entre sus tres principales prioridades de inversión. Esto refleja una estrategia orientada a aprovechar la experiencia externa y cerrar brechas críticas en la preparación para la ciberseguridad.

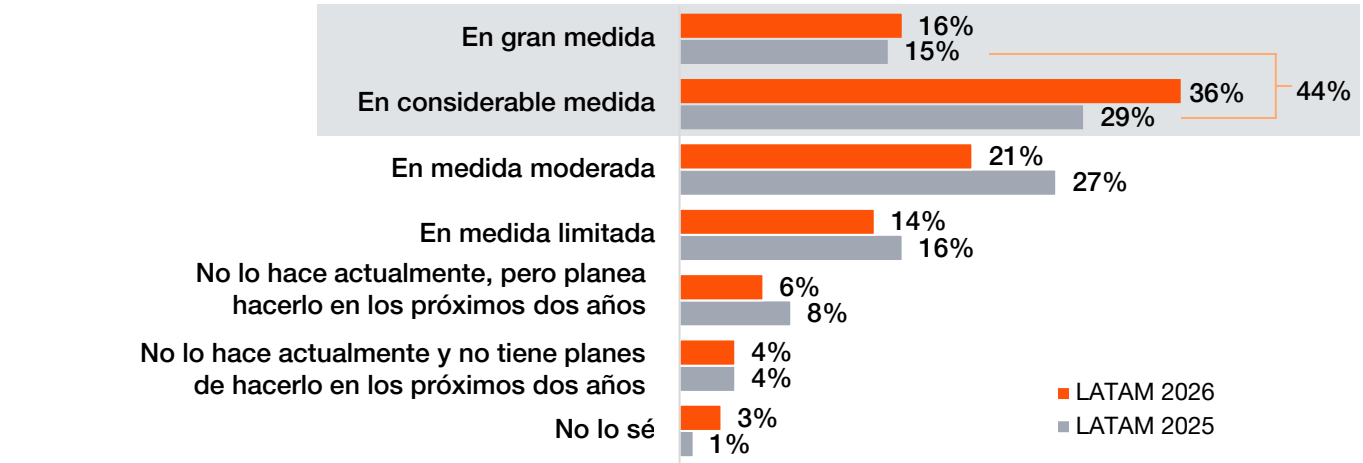
Inversiones que las organizaciones priorizan al asignar sus presupuestos de ciberseguridad
(% que las ubicaron en sus 3 prioridades principales)

P9. ¿Cuáles de las siguientes inversiones priorizará al asignar el presupuesto cibernético de su organización en los próximos 12 meses?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC

Ponerle precio al riesgo cibernético

Cada vez más organizaciones priorizan sus riesgos con cifras. Más de la mitad (52%) de ellas afirma utilizar la cuantificación del riesgo cibernético para medir el impacto financiero en una medida significativa o amplia, frente al 44% del año pasado. Sin embargo, si se analiza más a fondo, solo el 16% lo hace de manera significativa. Los líderes empresariales necesitan información fiable y práctica sobre los informes de riesgo cibernético para evaluar las amenazas a las que se enfrenta la organización y determinar la mejor manera de responder.

Medición del impacto financiero asociado a riesgos cibernéticos



P12. ¿En qué medida su organización evalúa actualmente el impacto potencial de los riesgos cibernéticos?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC

03

IA en ciberseguridad

De promesa a prioridad

#1

la seguridad de la nube es la principal prioridad en inversión cibernética para líderes de seguridad

#1

la capacidad de seguridad en IA priorizada por los líderes de seguridad es la búsqueda de amenazas

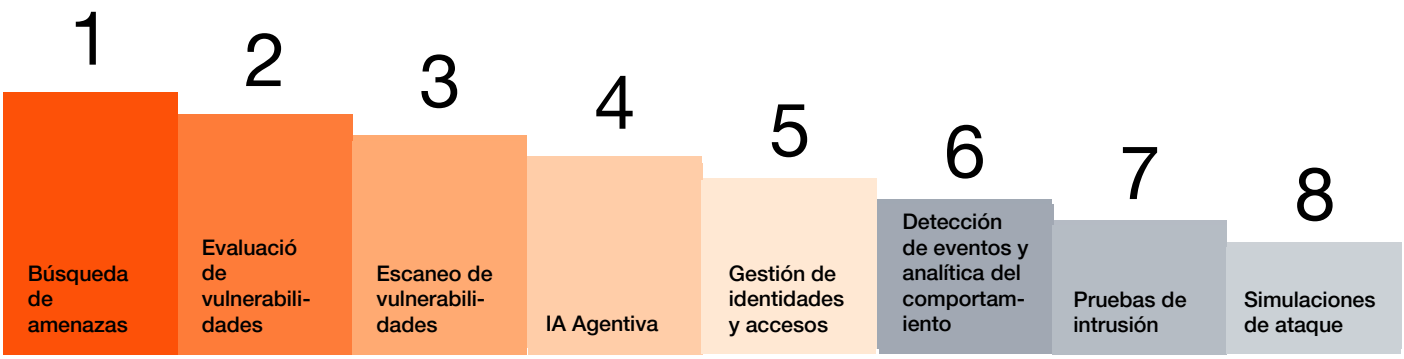
Top 3

áreas prioritarias para la IA agentiva son la protección de datos, la ciberdefensa, y la seguridad en la nube

El potencial de la IA para transformar las capacidades cibernéticas es claro y de gran alcance. Por ello, ocupa el primer puesto en varias de las categorías que analizamos. La habilitación mediante IA de capacidades cibernéticas claves es la principal prioridad para la asignación de presupuestos de ciberseguridad, el uso de servicios gestionados de ciberseguridad y la atención a la falta de talento en ciberseguridad.

Para reforzar sus capacidades de seguridad basadas en IA durante los próximos 12 meses, los líderes de seguridad priorizan la detección de amenazas. También buscan otras capacidades como soluciones de agentes, detección de eventos y análisis de comportamiento, gestión de identidades y accesos, y análisis y evaluación de vulnerabilidades.

La IA agentiva se encuentra entre las capacidades de seguridad de IA prioritarias
(ordenadas según su prioridad principal)



P18. ¿Cuál de las siguientes capacidades de seguridad en IA priorizará su organización durante los próximos 12 meses?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC

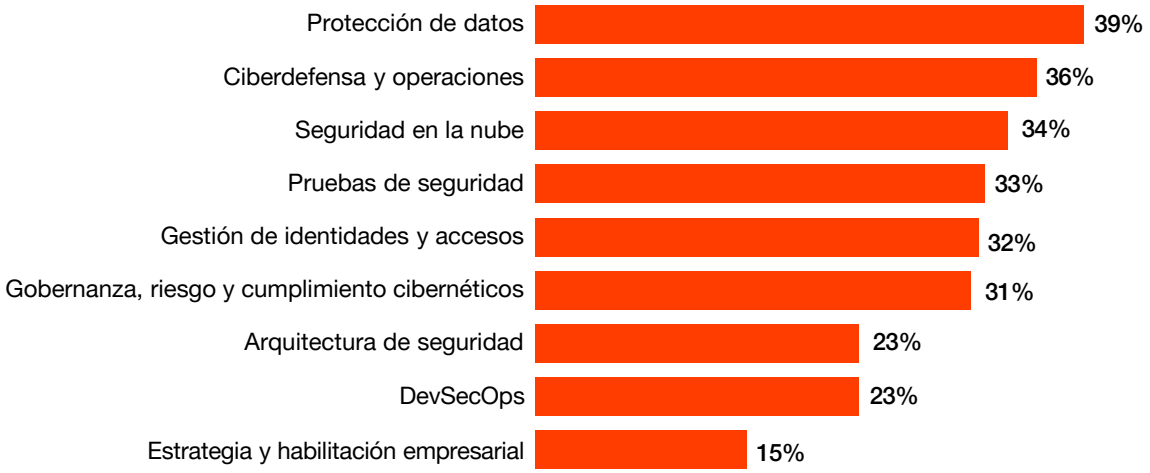
Agentes de cambio en la ciberdefensa

Las empresas reconocen que los agentes de IA (sistemas autónomos, orientados a objetivos, capaces de ejecutar tareas con mínima intervención humana) tienen un enorme potencial para transformar sus programas cibernéticos. Estos sistemas de IA ya no son solo herramientas de análisis, sino que se están convirtiendo en asistentes digitales capaces de actuar de forma independiente, colaborar con equipos humanos e incluso iniciar respuestas de seguridad, impulsando la eficiencia y la productividad.

Es por eso por lo que los líderes de seguridad clasifican a los agentes de IA entre las principales capacidades de seguridad de IA que sus organizaciones priorizarán durante los próximos 12 meses.

¿Dónde planean implementar estas soluciones de agentes? La seguridad en la nube, la protección de datos, la ciberdefensa y las operaciones se posicionan como las principales áreas de seguridad prioritarias para los agentes de IA el próximo año.

Prioridades de la IA Agentiva para aumentar la eficiencia y la productividad
(% que se clasificaron entre sus 3 principales prioridades)



P19. ¿En cuál de las siguientes áreas priorizará su organización la IA agentiva para aumentar la eficiencia y la productividad durante los próximos 12 meses?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC

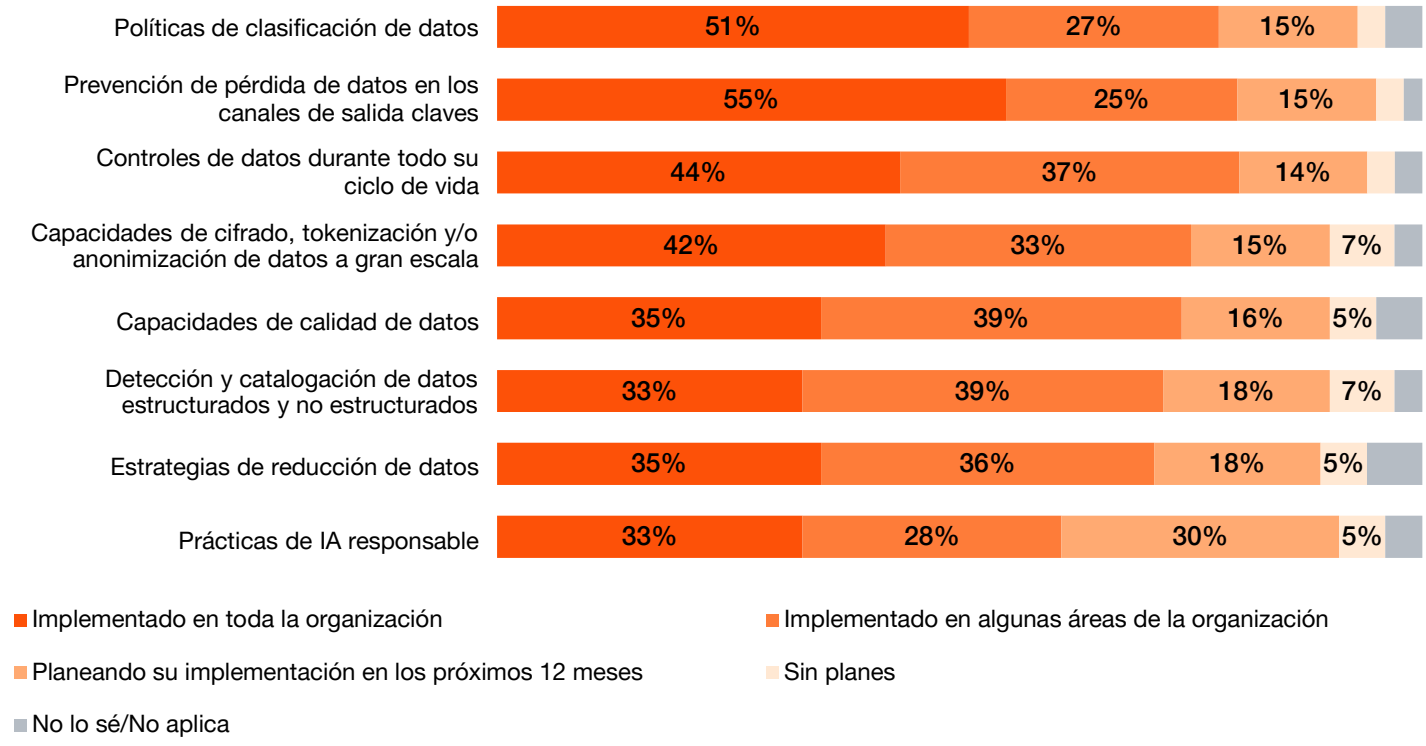
Gestión del riesgo de datos en IA

La implementación y el uso exitosos de la IA no son posibles 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 sólida gobernanza y seguridad a nivel empresarial para garantizar que dichos conjuntos de datos se utilicen en el contexto adecuado.

¿Están las organizaciones a la altura del desafío? Al preguntarles sobre su progreso en la implementación de diversas medidas de riesgo de datos en toda la empresa, solo la mitad ha implementado por completo políticas de clasificación de datos (51%) y prevención de pérdida de datos en los canales principales (55%), mientras que otras medidas obtuvieron una puntuación aún más baja. Es más, solo el 6% ha implementado todas las medidas encuestadas en toda la empresa.

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

Implementación de medidas para abordar el riesgo de datos



P5. ¿En qué medida su organización ha implementado o planea implementar alguna de las siguientes medidas para abordar el riesgo de datos en toda la empresa?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC

04

Preparación para la computación cuántica

Anticipando amenazas de nueva generación

Top 4

amenazas que las organizaciones están menos preparadas para abordar ahora incluyen la computación cuántica

53%

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

Solo 5%

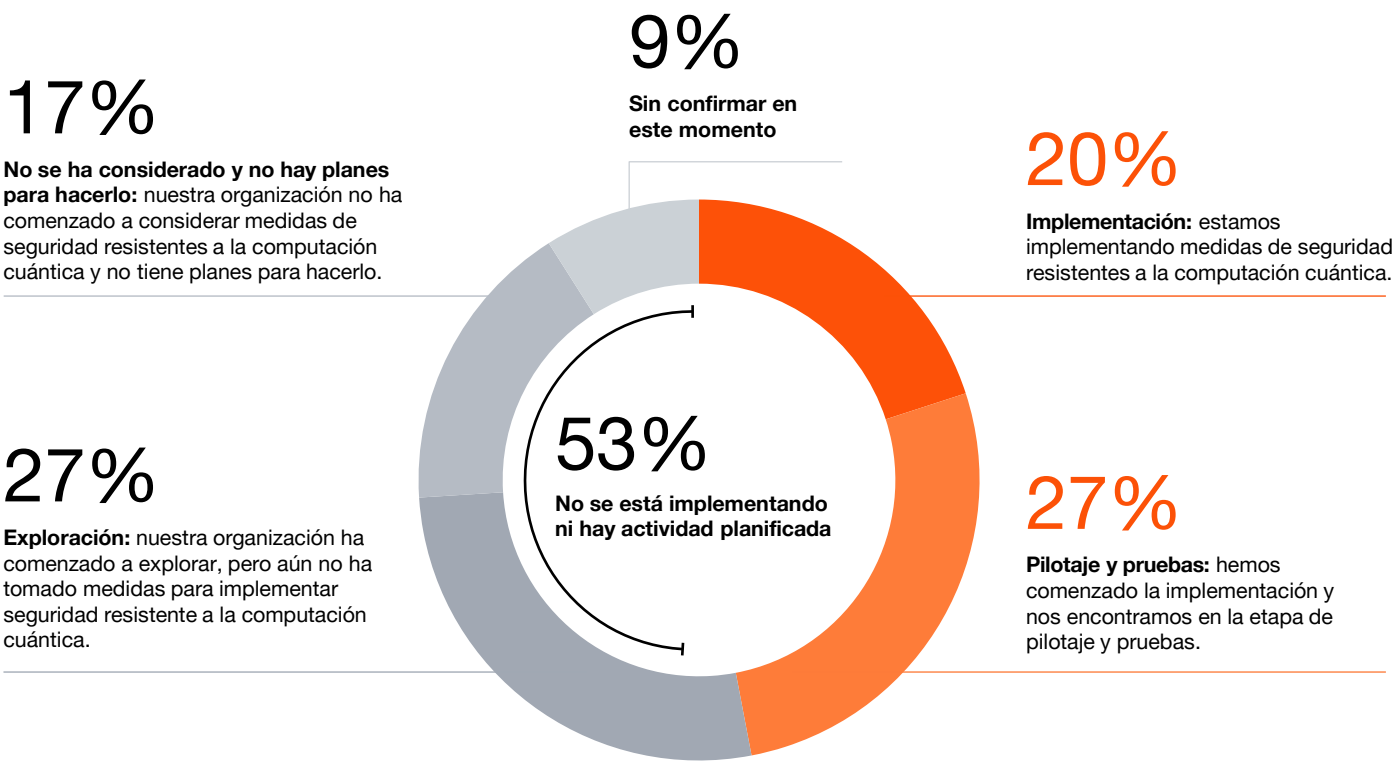
de los líderes de seguridad incluyen la preparación cuántica entre sus tres principales prioridades presupuestarias

La cuenta regresiva para la computación cuántica ha comenzado. Ya no es una teoría, sino que trasciende y ya introduce nuevas formas de resolver problemas complejos, como la modelización financiera y la optimización logística, a la vez redefiniendo suposiciones con décadas de antigüedad en ciberseguridad.

Aunque la criptografía cuántica no representa una amenaza cibernética inmediata, quienes se retrasen en la transición a la criptografía pos-cuántica podrían estar exponiendo sus datos confidenciales, servicios de autenticación y sistemas criptográficos. Con plazos de implementación que se extienden durante años, sentar las bases de una seguridad resistente a la cuántica exige actuar con prontitud hoy para evitar disrupciones adversas en el futuro.

Algunas organizaciones están logrando avances iniciales, con un 27% en fases piloto y de prueba. Sin embargo, solo el 20% ha superado la fase piloto, y más de la mitad (53%) no ha considerado ni comenzado a implementar medidas de seguridad resistentes a la tecnología cuántica. ¿Qué les frena? En muchos casos, se debe a la falta de comprensión de los riesgos pos-cuánticos, combinado con recursos internos limitados y demandas competitivas.

Avances en seguridad resistente a la computación cuántica



P21: ¿Qué tan avanzado está su organización en cuanto a la implementación de medidas de seguridad resistentes a la computación cuántica?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC

Crece la inquietud por la tecnología cuántica, aunque la preparación sigue rezagada

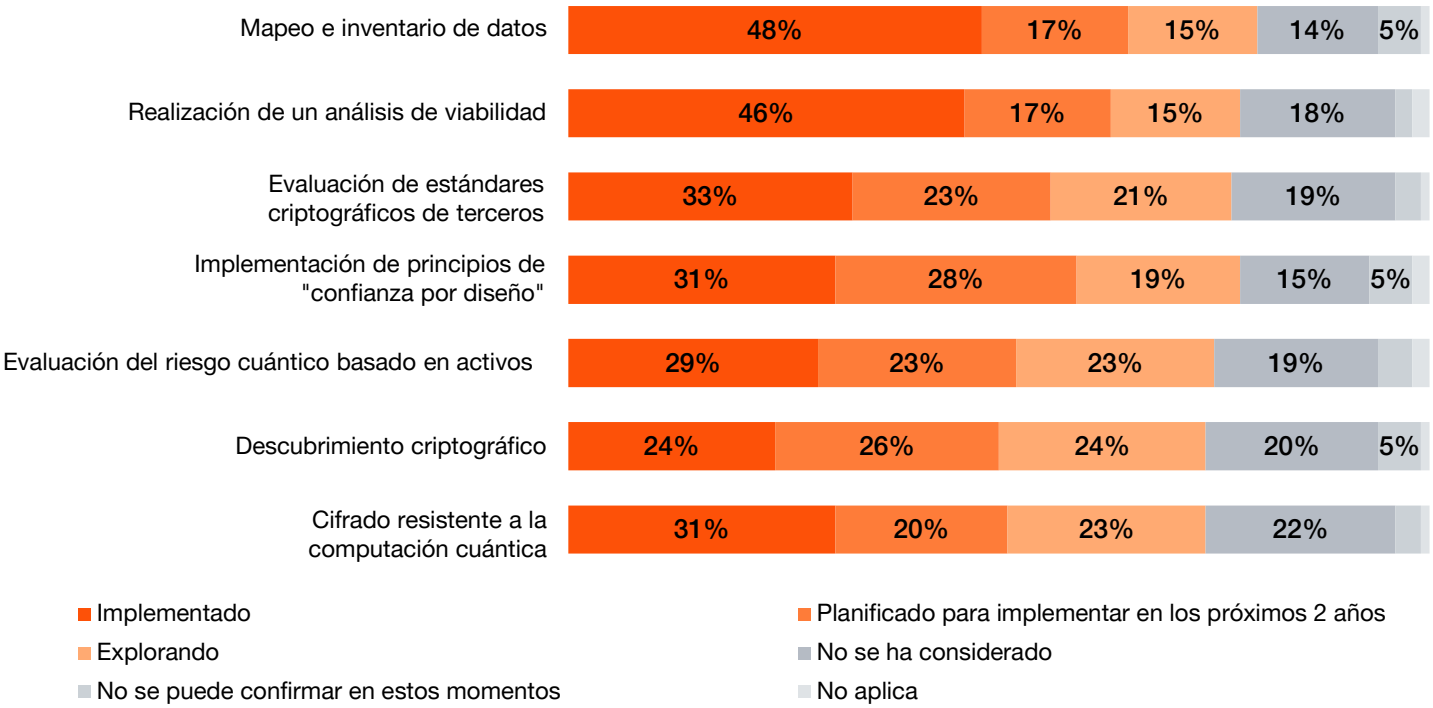
La conciencia sobre las amenazas cuánticas está creciendo. La computación cuántica se encuentra ahora entre las cuatro principales amenazas que las organizaciones se sienten menos preparadas para afrontar, un avance considerable respecto al año pasado.

Pero, ¿se están convirtiendo estas preocupaciones en acciones? Si bien aproximadamente un tercio ha implementado una o más de las medidas de seguridad resistentes a la tecnología cuántica incluidas en la encuesta, solo el 3% ha adoptado las siete medidas propuestas. Aunque estos pasos no son exhaustivos, constituyen prácticas fundamentales dentro de un proceso de varios años que requiere atención inmediata.

Las organizaciones con ingresos superiores a 5 billones de dólares tienen mayor probabilidad de haber implementado estas medidas, incluyendo un inventario de datos para mitigar el riesgo de "recolectar ahora, descifrar después“ y la prueba e implementación de cifrado resistente a la tecnología cuántica. Las empresas con mayor crecimiento también reconocen el desafío que representa la computación cuántica y se preparan para enfrentarlo.

Sin embargo, siguen siendo la excepción. A medida que la tecnología avanza, la capacidad de adoptar rápidamente la criptografía resistente a la tecnología cuántica está destinada a convertirse en una competencia empresarial decisiva.

Implementación de medidas de seguridad resistentes a la computación cuántica



P22. ¿Qué tan avanzada está su organización en relación con las siguientes medidas de seguridad resistentes a la computación cuántica?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC

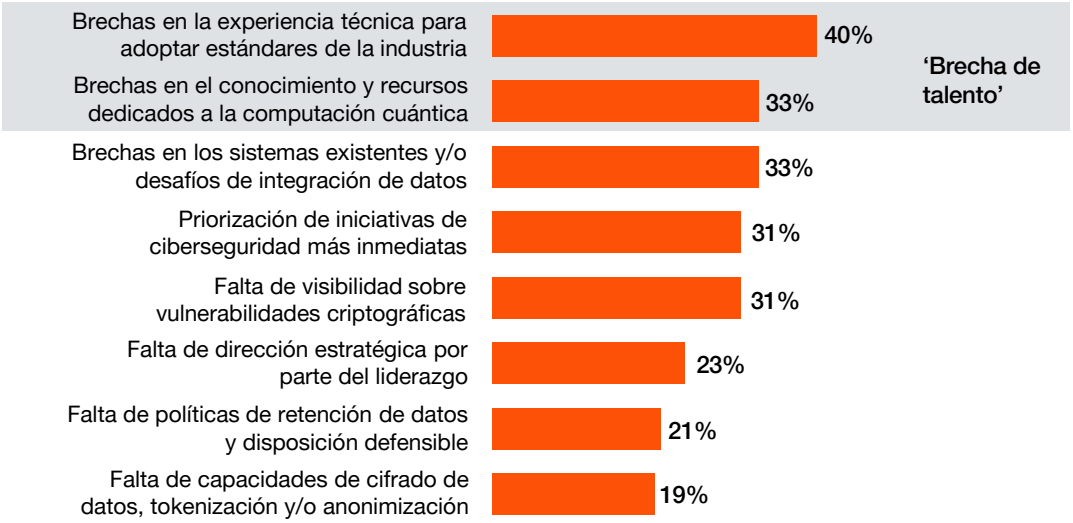
Por qué es difícil la criptografía post-cuántica

La preparación cuántica no es solo una actualización técnica, sino un cambio estratégico hacia prácticas de seguridad orientadas al futuro. Las principales barreras internas son la falta de experiencia técnica, el conocimiento institucional limitado y la rigidez de los sistemas obsoletos.

A medida que las organizaciones establecen inventarios criptográficos para iniciar la transición hacia la criptografía resistente a la tecnología cuántica, deben identificar los algoritmos vulnerables en su conjunto de tecnologías. Si bien se reconoce ampliamente que el cifrado de clave pública es vulnerable debido a la política de "recolectar ahora, descifrar después", los líderes de seguridad también deben ser conscientes de las tecnologías en las que confían para la autenticación y de las firmas digitales que utilizan algoritmos criptográficos igualmente vulnerables.

Estos obstáculos dejan algo claro: incluso con prioridad, implementar criptografía resistente a la computación cuántica requiere tiempo, y el tiempo es corto. Los estándares del Instituto Nacional de Estándares y Tecnología (NIST) recomiendan eliminar algoritmos vulnerables antes de que los actores de amenazas tengan capacidades cuánticas. Por eso es fundamental que las empresas cierren las brechas de conocimiento y evalúen sus dependencias criptografías y crear una hoja de ruta para la preparación.

Desafíos para lograr la criptografía post-cuántica
(% que se clasificaron entre sus 3 principales desafíos)



P23. ¿Cuáles son los mayores desafíos internos de su organización para lograr la criptografía post-cuántica en los próximos 12 meses?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC

05

Talento y habilidades cibernéticas

Los servicios gestionados pasan a la primera línea

Top 2

desafíos para implementar la IA para la ciberdefensa son las brechas de conocimientos y habilidades

54%

considera que las herramientas de IA y aprendizaje automático están entre sus tres principales prioridades para cerrar brechas de talento en ciberseguridad durante los próximos 12 meses.

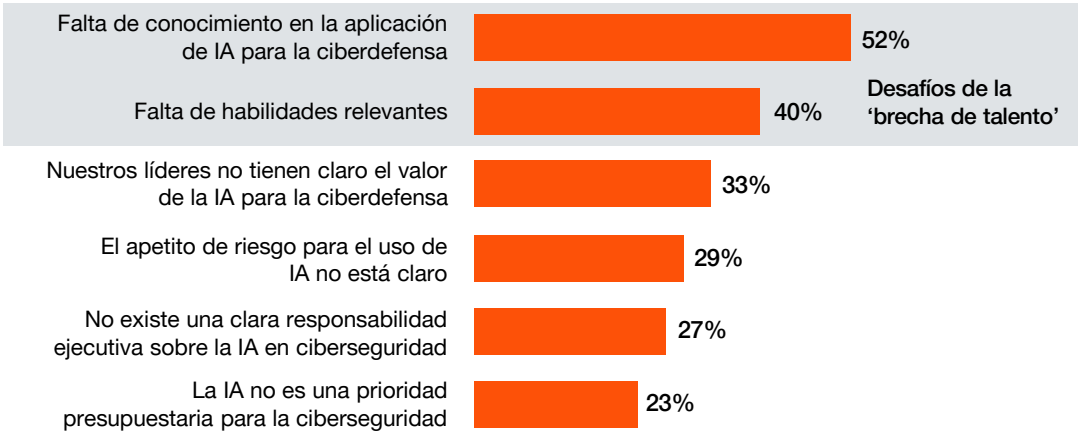
37%

de las organizaciones están priorizando la gestión de amenazas como área principal para utilizar servicios gestionados en los próximos 12 meses.

La escasez de personal en materia de ciberseguridad sigue impidiendo el progreso, especialmente a medida que las organizaciones se esfuerzan por poner en funcionamiento la IA, proteger entornos complejos y prepararse para las amenazas de próxima generación.

Las brechas de conocimiento y habilidades fueron las dos principales barreras para la implementación de IA para la ciberdefensa durante el último año, lo que obligó a las organizaciones a replantearse cómo escalar sus capacidades. Muchas están explorando nuevas maneras de mejorar sus competencias, incluyendo herramientas de IA y aprendizaje automático (54%), capacitación o recapacitación profesional (51%), herramientas de automatización de la seguridad (48%) y consolidación de herramientas cibernéticas (45%).

Desafíos de implementación de IA para la ciberdefensa
(% que se clasificaron entre sus 3 principales desafíos)

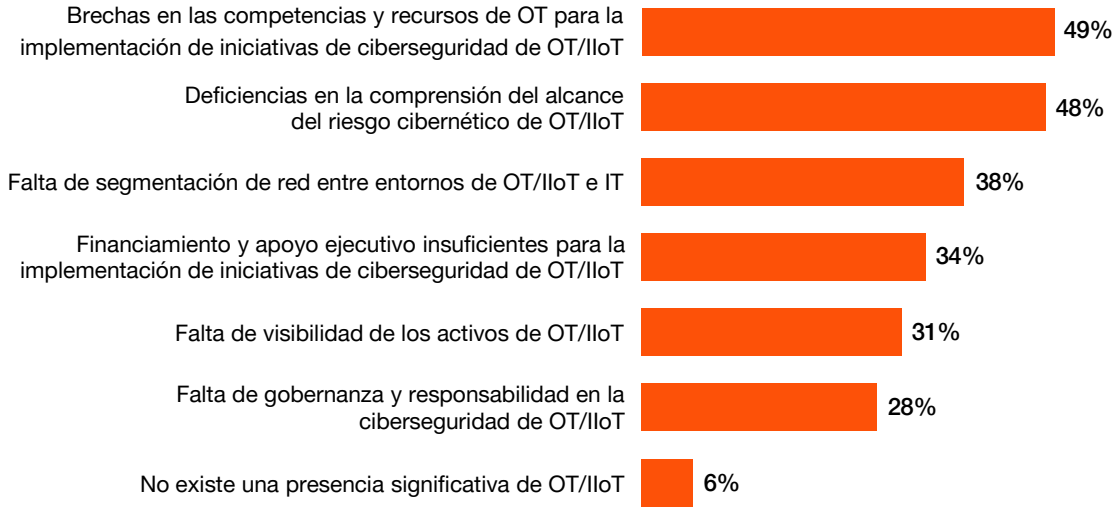


P20. ¿Cuáles han sido los mayores desafíos internos de su organización para la implementación de la IA en la ciberdefensa durante los últimos 12 meses?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC

Se busca: Habilidades en tecnología operativa

La tecnología operativa (OT) y el internet industrial de las cosas (IIoT) se han convertido en puntos de presión en el entorno actual de la seguridad. Casi la mitad (49%) de los líderes cita la falta de personal cualificado y recursos entre sus tres principales desafíos, mientras que el 28% señala la falta de claridad en la gobernanza y responsabilidad. En conjunto, estas discrepancias revelan un problema más profundo: muchas organizaciones aún carecen de la estructura y la experiencia necesarias para gestionar con confianza sistemas operativos cada vez más conectados.

Obstáculos para asegurar los sistemas OT e IIoT
(% que los clasificaron entre sus 3 principales obstáculos)



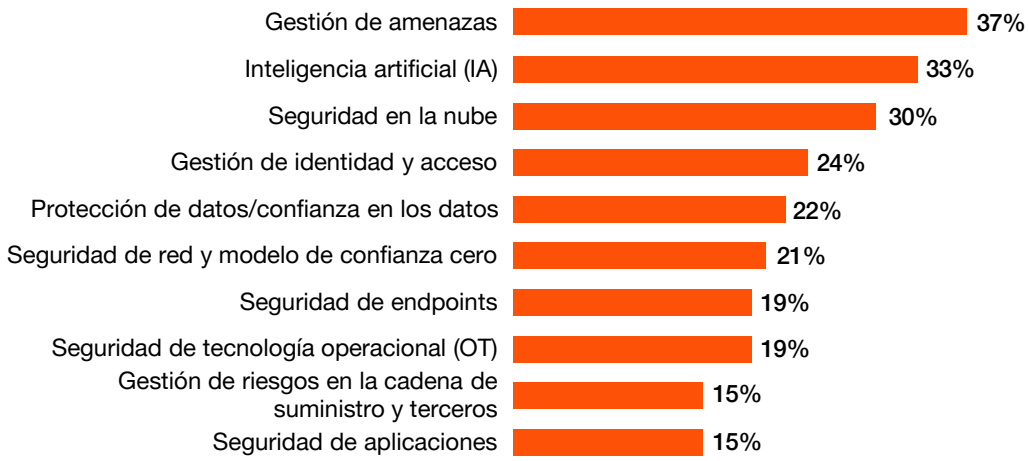
P4. ¿Cuáles son los 3 principales desafíos que enfrenta su organización para proteger la tecnología operacional (OT) y/o los sistemas del internet industrial de las cosas (IIoT)?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC

Los servicios gestionados como acelerador estratégico

La IA y la nube no solo representan las principales áreas de inversión en ciberseguridad, sino también los principales casos de uso para servicios de seguridad gestionada especializados. Las organizaciones recurren a estos servicios para mucho más que la simple externalización de capacidades: se están asociando con proveedores para modernizar la forma en que se entregan los sistemas críticos.

Los servicios gestionados se están convirtiendo en aceleradores estratégicos, que compensan la falta de habilidades y, además, ofrecen velocidad, escalabilidad y conocimiento especializado. En un entorno de amenazas cada vez más complejo, brindan una manera de modernizar las defensas sin desviar la atención de la innovación y el crecimiento.

Prioridades de ciberseguridad para el uso de servicios gestionados
(% que se clasificaron entre sus 3 principales prioridades)



P15. ¿Cuáles, si acaso, de las siguientes áreas de sus programas de ciberseguridad está priorizando su organización para utilizar servicios gestionados durante los próximos 12 meses?
Fuente: Encuesta Global Digital Trust Insights 2026 de PwC

Manual de estrategias para la alta dirección

De la incertidumbre a la acción

Cómo pueden actuar los líderes hoy

La encuesta de este año muestra que las organizaciones más vanguardistas están alineando la ciberseguridad con la estrategia comercial y priorizando la preparación sobre la reactividad.

Muchos ya han establecido prácticas fundamentales de gestión de riesgos cibernéticos, reforzando una estructura de gobernanza que se alinea con los principales marcos cibernéticos, incorporando controles de riesgos en toda la empresa y priorizando las evaluaciones y los informes.

Sin embargo, para estar preparado para el futuro, necesitará hacer más que seguir con su estrategia habitual. Esto significa afrontar la incertidumbre, tomar decisiones audaces pero informadas e integrar la agilidad en su estrategia.

CISO/CSO

Su capacidad no solo para traducir riesgos cibernéticos complejos en riesgos empresariales, sino también para comunicar eficazmente que la ciberseguridad es una responsabilidad compartida, es clave para lograr la aceptación y colaboración de la alta dirección. Este entendimiento común fomentará prácticas esenciales de gobernanza, resiliencia, cumplimiento normativo y respuesta. De cara al futuro, deberá abordar proactivamente los nuevos riesgos con una mentalidad de seguridad desde el diseño y utilizar datos para medir y evidenciar dónde se requieren mayores inversiones en ciberseguridad.

Fundamental
Cuantificar la exposición al riesgo geopolítico utilizando métricas vinculadas a infraestructura crítica, operaciones globales e interrupciones específicas de la industria y compartir los hallazgos con los altos ejecutivos.
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 modelos, agentes y sus identidades, aplicaciones y datos de entrenamiento) en función de la sensibilidad, la criticidad y la exposición.
Proteger la IA ampliando los controles de seguridad existentes a los sistemas de IA e identificar brechas donde se requieren nuevas capacidades (por ejemplo, salvaguardas de IA o puertos de LLM).
Reexaminar y actualizar periódicamente los modelos de gobernanza del riesgo cibernético e incorporar riesgos tecnológicos en evolución, como la IA y la cuántica.
Fortalecer la gobernanza a través de Indicadores clave de rendimiento aplicables que rastreen el desempeño en la gestión de riesgos de terceros, de la cadena de suministro, obsoletos y basados en la nube.
Ejecutar ejercicios de simulación para poner a prueba la toma de decisiones, determinar rutas de escalación y validar los pasos de recuperación.

Preparados para el futuro
Establezca la ciberseguridad como una responsabilidad compartida con los altos ejecutivos y la junta directiva, incorporando debates sobre gobernanza junto con conocimientos de inteligencia sobre amenazas y resúmenes ejecutivos sobre amenazas emergentes y capacidades adversas.
Ponga en práctica la supervisión y la gobernanza de los agentes de IA a través del descubrimiento, la clasificación, el monitoreo de exposición, incluidas simulaciones adversas.
Pase de las evaluaciones puntuales de proveedores al monitoreo continuo de riesgos de terceros.
Evalúe qué sistemas dependen de la criptografía y adopte estándares criptográficos post-cuánticos (PQC) donde sea necesario.
Determine si su empresa debe aprovechar los servicios gestionados desarrollando un plan de servicios administrados basado en el ROI monitoree las necesidades de tecnología, habilidades y recursos.
Evalúe sus datos y determine qué debería estar listo para la tecnología cuántica ahora, luego trabaje con sus equipos de administración de datos en la adopción cuántica.

CTO/CIO

Su enfoque en tecnología escalable y en la resolución proactiva de las brechas de talento y capacitación proporciona un apoyo esencial a la estrategia cibernética de la organización. Debe seguir colaborando estrechamente con el equipo de seguridad para integrar los controles de riesgos y la gobernanza durante la adopción de tecnología. De cara al futuro, liderará las iniciativas para probar e integrar tecnologías emergentes, como la IA y la computación cuántica, con seguridad integrada, a la vez que impulsa la innovación que anticipa y mitiga los futuros riesgos cibernéticos.

Fundamental
Escalar la IA y otras tecnologías emergentes de forma segura, presupuestando e incorporando medidas de seguridad proactivas críticas.
Colaborar estrechamente con CISO y CRO para alinear la implementación de tecnología con la gestión de riesgos y los requisitos de cumplimiento.
Asegurar la IA mediante la incorporación de controles de gestión y de riesgo cibernético en la planificación de su implementación desde el inicio, alineándola con los principios de seguridad por diseño.
Aplicar controles consistentes de identidad, acceso y políticas en plataformas, API e integraciones de terceros.
Incorporar una administración sólida de IIoT y OT en su estrategia de arquitectura para obtener visibilidad y control de punta a punta en entornos distribuidos.

Preparados para el futuro
Coordine con los CISO y los líderes de datos para proteger los datos de capacitación confidenciales y reforzar la administración de entrada y salida de los modelos de IA.
Alinee la adopción y las iniciativas de proyectos piloto de tecnologías cuánticas con las estrategias empresariales de seguridad resistentes a la computación cuántica, en colaboración con el liderazgo de seguridad.
Impulse la adopción de herramientas de automatización y de detección y respuesta de riesgos basadas en IA para aumentar la eficiencia operativa y la resiliencia.
Adopte un marco seguro por diseño para productos conectados durante todo su ciclo de vida operativo.

CRO

Su enfoque en la identificación de riesgos empresariales y emergentes, así como en sus interdependencias con la ciberseguridad, es esencial para proteger a la organización. Debe continuar adaptando los controles a las vulnerabilidades en evolución y asegurarse de que los marcos de riesgo permanezcan actualizados. De cara al futuro, su función requerirá integrar las exposiciones relacionadas con la IA, la computación cuántica y la geopolítica en una estrategia de gestión de riesgos adaptativa y con visión prospectiva, que respalde la agilidad y la resiliencia organizacional.

Fundamental
Integrar escenarios basados en amenazas en los registros de riesgos y en los ciclos de pruebas de resistencia, priorizando 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 de la IA y la computación cuántica mediante análisis de impacto empresarial personalizados, priorizando las áreas con automatización de la fuerza laboral digital.
Apoyar los esfuerzos de cumplimiento al monitorear la gestión de amenazas cibernéticas con los requisitos regulatorios.

Preparados para el futuro
Amplie los modelos de riesgo de terceros para considerar la capacidad cuántica en los entornos de los proveedores y su resiliencia frente al uso indebido de IA adversarial.
Aproveche la IA para evaluar continuamente el riesgo cibernético a escala, desde la cuantificación y las evaluaciones hasta la elaboración de informes.
Desarrolle un marco de riesgo integrado con inteligencia (IIRF) que incorpore diversas perspectivas de inteligencia de amenazas estratégicas en la puntuación de riesgo empresarial.
Implemente pruebas piloto de herramientas de modelado predictivo de amenazas para simular amenazas emergentes y cuantificar los probables impactos comerciales durante los próximos 12 a 36 meses.

CFO

Su papel es clave en la asignación de un presupuesto adecuado para una gestión cibernética proactiva. Garantizar la seguridad en las iniciativas estratégicas y en la implementación tecnológica resulta esencial para la resiliencia organizacional. Es necesario continuar identificando ineficiencias y alineando los presupuestos con las iniciativas de mayor impacto en ciberseguridad. De cara al futuro, anticipar los riesgos emergentes implica planificar las necesidades presupuestarias y promover modelos de financiación basados en el retorno de la inversión (ROI), que permitan a la organización invertir de manera inteligente en tecnologías y capacidades de seguridad.

Fundamental
Apoyar inversiones estratégicas que impulsen la resiliencia a largo plazo, la ventaja competitiva y la preparación regulatoria.
Evaluar los costos a largo plazo de reaccionar a los incidentes de seguridad versus invertir proactivamente en defensas cibernéticas, servicios administrados, seguros, cumplimiento, etc.
Recalibrar las métricas del ROI cibernético para incluir ahorros en la prevención de incidentes, multas regulatorias evitadas y reducción del tiempo de respuesta.
Colaborar con CISO, CTO y CIO para presupuestar de manera eficaz el desarrollo de habilidades en ciberseguridad y la capacitación tecnológica.
Apoyar modelos de financiación sostenibles que equilibren los costos operativos con inversiones estratégicas en ciberseguridad.

Preparados para el futuro
Abogue por la ciberseguridad como una función empresarial importante, vinculando los niveles de inversión con los objetivos de desempeño a nivel de junta directa.
Establezca una reserva de asignación de capital para “facilitadores de resiliencia”, incluidas capacidades de respuesta a la explotación de día cero y post-cuántico.
Desarrolle casos de negocio basados en el retorno de la inversión (ROI) para servicios de seguridad gestionados.
Identifique y reduzca ineficiencias como redundancias de herramientas y consolide donde sea posible.

CEO

Su compromiso continuo para garantizar que la ciberseguridad sea una prioridad empresarial sigue siendo esencial. Debe seguir alineando las iniciativas empresariales con la estrategia de gestión de riesgos cibernéticos, fomentando al mismo tiempo la colaboración entre la Junta Directiva y los altos ejecutivos. De cara al futuro, su función consiste en forjar alianzas influyentes y promover inversiones que permitan a su organización afrontar los nuevos desafíos cibernéticos.

Fundamental
Alentar la participación en escenarios cibernéticos en reuniones ejecutivas fuera de la oficina, simulando interrupciones específicas del sector y operaciones de amenazas híbridas.
Vincular la resiliencia cibernética con la facilitación de ingresos, como la protección de las plataformas digitales, la confianza en los datos de los clientes y el crecimiento transfronterizo.
Abogar por la innovación responsable, confirmando que los proyectos de IA y cuántica incorporan medidas de seguridad y éticas desde el inicio.
Entender dónde se realizan compensaciones presupuestarias en materia cibernética y si esas compensaciones satisfacen el valor por el riesgo.
Hacer de la ciberseguridad una responsabilidad compartida en todos los niveles, desde la sala de juntas hasta el área administrativa.
Mantener informado a junta directiva sobre las prioridades estratégicas del programa de ciberseguridad e involucre a los directores para discutir las necesidades del programa.

Preparados para el futuro
Lidere alianzas multisectoriales para la estandarización post-cuántica, la adopción de posturas de defensa conjuntas y el intercambio de inteligencia sobre amenazas.
Impulse la inversión en tecnologías emergentes (IA, computación cuántica) con asegurando la integración de la seguridad desde el principio.
Institucionalice las revisiones prospectivas cuánticas y geopolíticas en los ciclos de planificación estratégica y en los estatutos de riesgo de los directorios.
Participe activamente en pruebas de resistencia para prepararse ante disrupciones geopolíticas y tecnológicas.

Acerca de la encuesta

La Encuesta Global Digital Trust Insights 2026 fue diseñada para recopilar las opiniones de 3,887 ejecutivos de negocios y tecnología, y se llevó a cabo entre mayo y julio de 2025.

Un tercio de los participantes (33%) proviene de grandes empresas con ingresos iguales o superiores a 5 billones de dólares. Los encuestados representan diversos sectores, entre ellos: Servicios financieros (21%); Manufactura industrial y automotriz (21%); Tecnología, medios de comunicación y telecomunicaciones (19%); Comercio minorista y consumo (16%); salud (10%); Energía, servicios públicos y recursos (9%); Gobierno y servicios públicos (4%).

Los participantes residen en 72 países. La distribución regional de las respuestas es la siguiente: Europa Occidental (32%), América del Norte (27%), Asia Pacifico (18%), América Latina (11%), Europa Central y Oriental (6%), África (4%) y Medio Oriente (3%).

La Encuesta Global Digital Trust Insights, anteriormente conocida como la Encuesta sobre el Estado Global de la Seguridad de la Información (GSISS), llega a su 28.ª edición como la encuesta anual con mayor trayectoria sobre tendencias en ciberseguridad. Además, es la más grande del sector y la única que incluye la participación de altos ejecutivos, no solo de líderes en seguridad y tecnología.

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

Contáctenos

Bismark Rodríguez

Socio Líder Regional de Consultoría

PwC Interaméricas
bismark.rodriguez@pwc.com

Edwin Orrico

Gerente Senior de Ciberseguridad y Privacidad

PwC Interaméricas
edwin.o.orrico@pwc.com

Susana Pino

Socio Líder Regional de Risk Assurance Services (RAS)

PwC Interaméricas
pino.susana@pwc.com

Isaac Rodríguez Rojas

Gerente de Ciberseguridad y Privacidad

PwC Interaméricas
isaac.rodriguez@pwc.com