Cerrando las brechas hacia la resiliencia cibernética: manual de estrategia para la alta dirección.

Global Digital Trust Insights 2025

pwc

Conclusiones

2% Implementó acciones de resiliencia cibernética en su organización.

>50% De los CISO están involucrados en gran medida en actividades comerciales clave.

13% de brecha de confianza entre CISO/CSO y CEO con respecto al cumplimiento de las regulaciones de IA.

Dado que la superficie de ataque continúa expandiéndose gracias a los avances de la inteligencia artificial, dispositivos conectados, tecnologías en la nube y un entorno regulatorio en constante cambio, lograr resiliencia cibernética a nivel empresarial es fundamental. Sin embargo, a pesar de la conciencia generalizada de los desafíos, persisten brechas significativas.

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

La encuesta Global Digital Trust Insights 2025, que incluye a más de 4.000 directivos y responsables de tecnología de compañías de 77 países, ha revelado **brechas** importantes que las organizaciones deben superar para alcanzar una resiliencia cibernética adecuada:

- a pesar de las crecientes preocupaciones sobre el riesgo cibernético, solo el 2% de los ejecutivos dice que su empresa ha implementado acciones de resiliencia cibernética en su organización en todas las áreas encuestadas.
- las organizaciones se sienten menos preparadas para abordar las amenazas cibernéticas que les resultan más preocupantes, como los riesgos relacionados con la nube y las infracciones que pueden ocurrir a través de terceros con acceso a sus sistemas.
- menos de la mitad de los ejecutivos dicen que sus CISO están involucrados en gran medida en la planificación estratégica, los informes a la junta y la supervisión de las implementaciones de tecnología.
- los directores ejecutivos y los responsables de seguridad de la información tienen distintos niveles de confianza en la capacidad de su empresa para cumplir con las regulaciones, especialmente aquellas relacionadas con inteligencia artificial, resiliencia e infraestructura crítica.
- si bien los ejecutivos reconocen la importancia de medir el riesgo cibernético, menos de la mitad lo hace de manera efectiva y solo el 15% mide el impacto financiero de los riesgos cibernéticos en una medida significativa.

Estos puntos indican la necesidad de una mejor colaboración entre el nivel ejecutivo y de una inversión estratégica para fortalecer la resiliencia cibernética. Al abordar estas brechas y hacer de la ciberseguridad una prioridad empresarial, se puede establecer un puente hacia un futuro más seguro. Los CISO pueden ayudar a impulsar este resultado compartiendo conocimientos basados en la tecnología y explicando las prioridades cibernéticas en términos empresariales (costo, oportunidad, riesgo).

CONTENIDOS

Identificación de ciberamenazas y necesidad de una visión compartida para la preparación

66% califica a la ciberseguridad como el mayor riesgo para la mitigación, en comparación con el 48% de los ejecutivos de negocios.

42% considera las amenazas relacionadas con la nube como su ciberamenaza más preocupante.

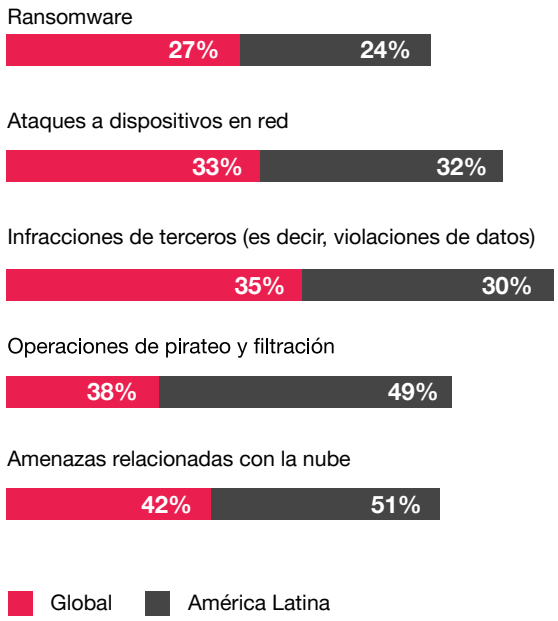
Top 2 “Ataques a la nube” y a “productos conectados”, son lo que los ejecutivos de seguridad se sienten menos preparados para abordar.

No están preparados para las amenazas más preocupantes

Las cuatro amenazas cibernéticas más preocupantes (con la nube, operaciones de piratería y fuga de información, infracciones de terceros y ataques a dispositivos en red) son las mismas que los ejecutivos de seguridad se sienten menos preparados para abordar. Esta brecha resalta la necesidad urgente de mejores inversiones y capacidades de respuesta más sólidas.

Existe también una brecha de percepción entre los ejecutivos de seguridad y el resto de la organización, ya que los CISO y CSO tienen más probabilidades de clasificar el ransomware entre sus tres amenazas más preocupantes. Esto puede reflejar su función, ya que este tipo de ataque es más central para las tareas cibernéticas/de TI y quienes desempeñan ese rol probablemente comprenden las vulnerabilidades mejor que sus pares comerciales. Esto refuerza aún más la importancia de un mejor intercambio de información entre los equipos de liderazgo para crear una alineación en las prioridades.

La preocupación por la ciberamenaza frente a la preparación



Llamada de atención

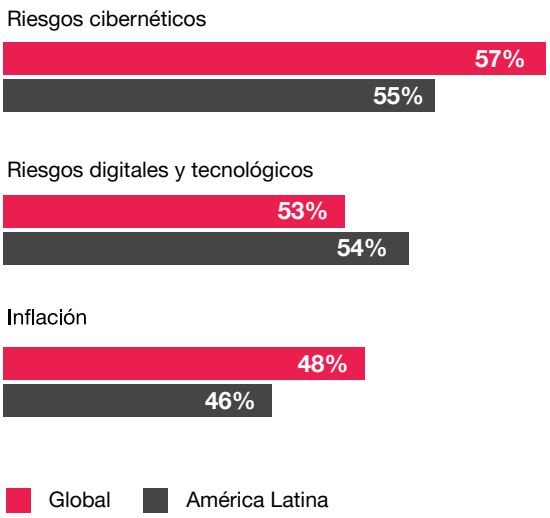
Una estrategia de inversión en ciberseguridad basada en amenazas es clave, prioriza las inversiones en los sectores más urgentes de riesgos cibernéticos y observa más de cerca dónde se están aplicando los recursos en términos de personas, procesos y capacidades de defensa.

Prioridades: la división estratégica

Los directivos están más preocupados por la coyuntura, esto es la inflación, regulaciones, conflictos geopolíticos, etc. Por su lado los responsables de tecnología clasifican los riesgos cibernéticos como su principal prioridad. Los tecnológicos clasifican los riesgos cibernéticos como su principal prioridad, probablemente debido a su proximidad al panorama de amenazas cibernéticas. Aun así, casi la mitad de los ejecutivos empresariales todavía clasifican los riesgos cibernéticos entre sus tres principales preocupaciones. Esto representa una oportunidad para que los CISO conecten la agenda de ciberseguridad con la empresarial.

Propiedades de mitigación de riesgos

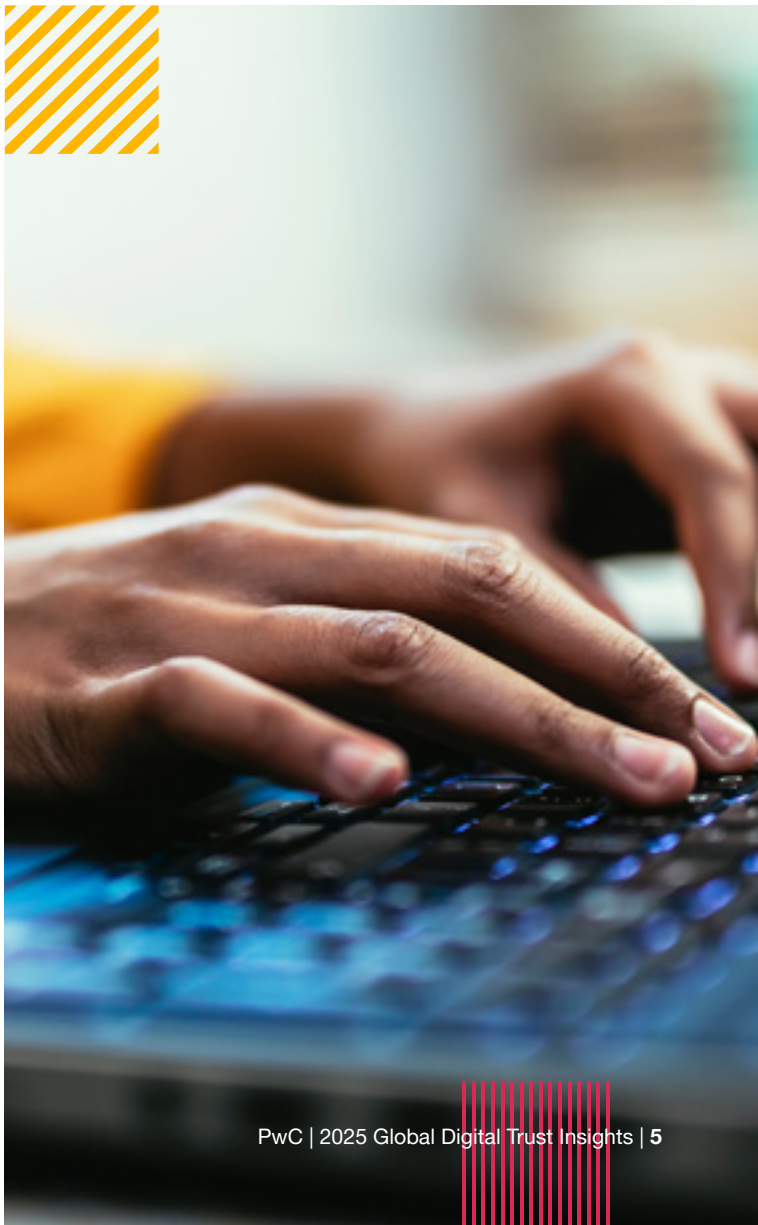
Mostrando % clasificado entre los tres primeros



El costo promedio global de la filtración de datos supera los 3 millones de dólares

Más de una cuarta parte de los ejecutivos nos dicen que su filtración de datos más dañina en los últimos tres años le costó a su organización al menos 1 millón de dólares. Este índice resultó más bajo que la encuesta del año pasado en organizaciones de todos los tamaños y en la mayoría de las regiones y sectores. En general, la filtración de datos promedio se estima en un costo de 3.32 millones de dólares.

Los de mejor desempeño, identificados como aquellos que respondieron que su organización tiene más probabilidades de demostrar prácticas de ciberseguridad de alta calidad de manera habitual, tenían menos probabilidades de experimentar filtraciones de datos en los últimos tres años.



Llamado a la acción de los ejecutivos

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

CISO: resalte al resto de la alta dirección las amenazas que más ponen en peligro su negocio, especialmente si es necesario reorientar los esfuerzos de inversión.

CIO y directores de tecnología (CTO): basándose en conversaciones con los ejecutivos de riesgo, evalúe cómo ciertas amenazas pueden dañar la seguridad de la información y la infraestructura en general y qué amenazas plantean las mayores barreras para la resiliencia.

CFO: obtenga información más profunda del CISO y el CRO sobre las prioridades de inversión y ciber más críticas.

CEO: reúnase periódicamente con el CRO y el CISO para comprender los vectores de amenaza que más preocupan. Asegúrese de recibir informes periódicos sobre los esfuerzos actuales de mitigación de amenazas.

El equilibrio entre oportunidades y riesgos

67% dice que GenAI ha aumentado su superficie de ataque durante el último año.

78% ha aumentado su inversión en GenAI en los últimos 12 meses.

72% ha aumentado su gestión de riesgos e inversión en gobernanza de la IA.

Si bien el rápido avance de la IA generativa (GenAI) está generando nuevas oportunidades en todas las industrias, también presenta riesgos de ciberseguridad. A medida que las organizaciones adoptan GenAI y otras tecnologías emergentes, los directivos deben abordar vectores de ataque más complejos.

Una superficie de ataque en evolución

Los ejecutivos de seguridad informan que GenAI (67%) y las tecnologías en la nube (66%) han ampliado la superficie de ataque cibernético durante el último año, lo que hace que las empresas sean más vulnerables a amenazas sofisticadas.

También están ampliando la superficie de ataque otras tecnologías, como los dispositivos conectados y la tecnología operativa (OT), que afectarán a sectores como la fabricación, atención sanitaria y la energía. A medida que más dispositivos se interconectan, la seguridad de estos sistemas se vuelve más difícil. Además, aunque la computación cuántica todavía está en una etapa preliminar, el 42% de los ejecutivos de seguridad informan que ya les ha hecho abordar vulnerabilidades.

Llamada de atención

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

Aprovechar GenAI para la ciberdefensa: oportunidades y desafíos

Las tres formas principales en que están aprovechando GenAI incluyen la detección y respuesta a amenazas, la inteligencia de amenazas y la detección de malware/phishing.

Sin embargo, a pesar de estas oportunidades, las organizaciones enfrentan varios obstáculos al incorporar GenAI en sus estrategias de ciber-defensa:

Dificultad para incorporarse a los sistemas/procesos existentes **(39%)**.

Falta de confianza en GenAI por parte de las partes interesadas internas **(39%)**.

Controles internos y gestión de riesgos inadecuados **(38%)**.

Falta de políticas internas estandarizadas que regulen su uso **(37%)**.

Llamada de atención

GenAI puede transformar sus defensas cibernéticas, pero solo si supera los desafíos de integrarla, confiar en ella y administrarla de manera efectiva, aplicando prácticas de IA responsable. De lo contrario, corre el riesgo de quedarse atrás en la carrera contra los actores amenazantes.

GenAI lidera las prioridades de inversión en ciberseguridad

Reconociendo los crecientes riesgos cibernéticos, el 78% de los ejecutivos ha incrementado su inversión tecnologias ciber en GenAI, centrándose especialmente en la gobernanza.

Las empresas también están empezando a invertir en preparación cuántica. Aunque su adopción aún está a años de distancia, ya existe un imperativo creciente de buscar tecnologías resistentes a la tecnología cuántica y medidas de seguridad postcuánticas para combatir las amenazas futuras que plantee esta tecnología en las manos equivocadas.

Llamado a la acción de los ejecutivos

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

CISO: ayude a impulsar la estandarización en todo el parque tecnológico para integrar la IA en las defensas cibernéticas. Aplique los derechos de acceso usuario por usuario para identificar posibles vectores de ataque.

CIO y CTO: desarrollen una evaluación del impacto de la IA para educar a los ejecutivos de negocios sobre dónde tiene más sentido invertir e implementar. Preparen sus plataformas para la escalabilidad a medida que crece el uso de GenAI.

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

Directores de datos (CDO): mejoren sus protocolos de gobernanza de datos y evalúen los riesgos de privacidad de datos en relación con las leyes de privacidad y las pautas de los reguladores.

Directores jurídicos principales (CLO) y asesores jurídicos generales (GC): colaboren con otros equipos de riesgo y cumplimiento para protegerse contra usos secundarios indebidos de los datos y una posible exposición legal.

Un mundo cibernético altamente regulado: ¿Están realmente preparadas las empresas?

Según datos globales, la normativa sobre ciberseguridad ayudó al 75% de las organizaciones:

29% desafió a nuestra organización a reforzar el programa actual de gestión de riesgos cibernéticos, los procesos y los enfoques de gobernanza.

26% ayudó a establecer barandillas para la innovación tecnológica y los esfuerzos de transformación.

16% ayudó a nuestra organización a ser más resistente al imponer un marco para todo el sector.

Los marcos regulatorios exigen a las empresas que cumplan rápidamente con una cantidad cada vez mayor de requisitos. Una oleada de nuevas regulaciones (DORA, Ley de Resiliencia Cibernética, Ley de Inteligencia Artificial, CIRCIA, Ley de Ciberseguridad de Singapur, etc.), subraya la urgencia de que las organizaciones adapten sus prácticas a mayores expectativas. A medida que las empresas abordan estas demandas, se enfrentan a una brecha crítica en la confianza entre los CISO/CSO y los CEO con respecto a su capacidad para lograr el cumplimiento total.

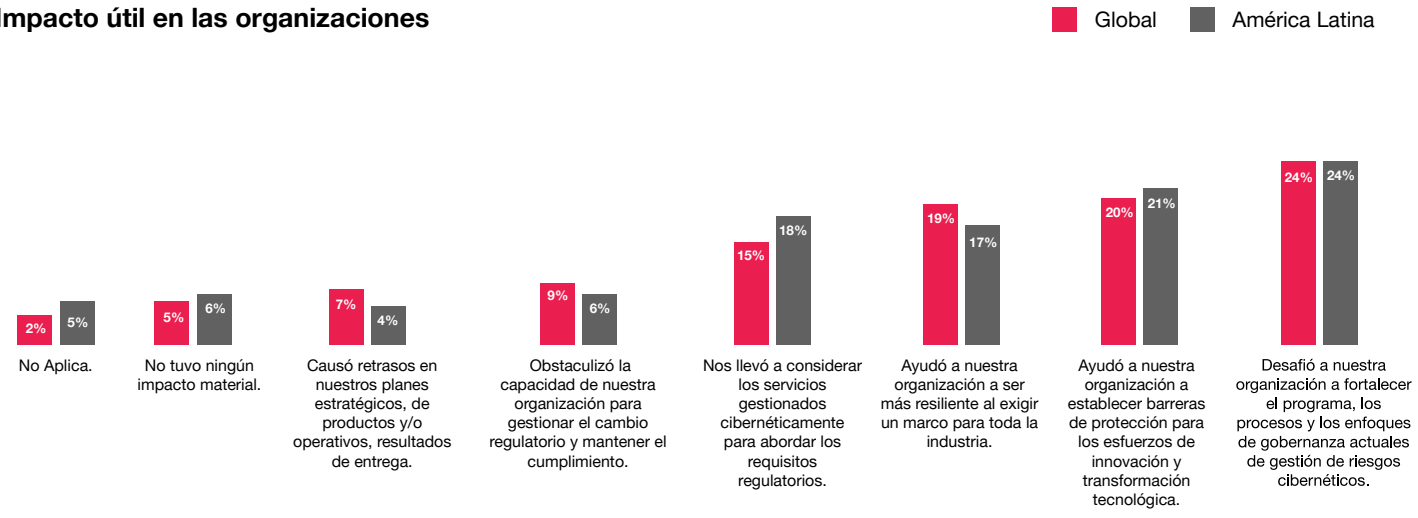
Regulaciones cibernéticas impulsan un cambio positivo

Las regulaciones cibernéticas están demostrando ser un importante impulsor de la inversión en ciberseguridad, ya que el 96% de los ejecutivos reconoce que los requisitos regulatorios los han impulsado a mejorar sus medidas de seguridad. Además, el 78% cree que las regulaciones han ayudado a desafiar, mejorar o aumentar su enfoque de ciberseguridad. Esto indica que, a pesar de las dificultades de cumplimiento, las regulaciones están sirviendo para madurar aún más las capacidades en todas las industrias.

Llamada de atención

Organizaciones que adoptan requisitos regulatorios tienden a beneficiarse de marcos de seguridad más sólidos y un enfoque más consistente frente a las amenazas emergentes. El cumplimiento debe considerarse como una oportunidad de marcar casillas, sino como una oportunidad para construir a largo plazo resiliencia y confianza con las partes interesadas.

Impacto útil en las organizaciones



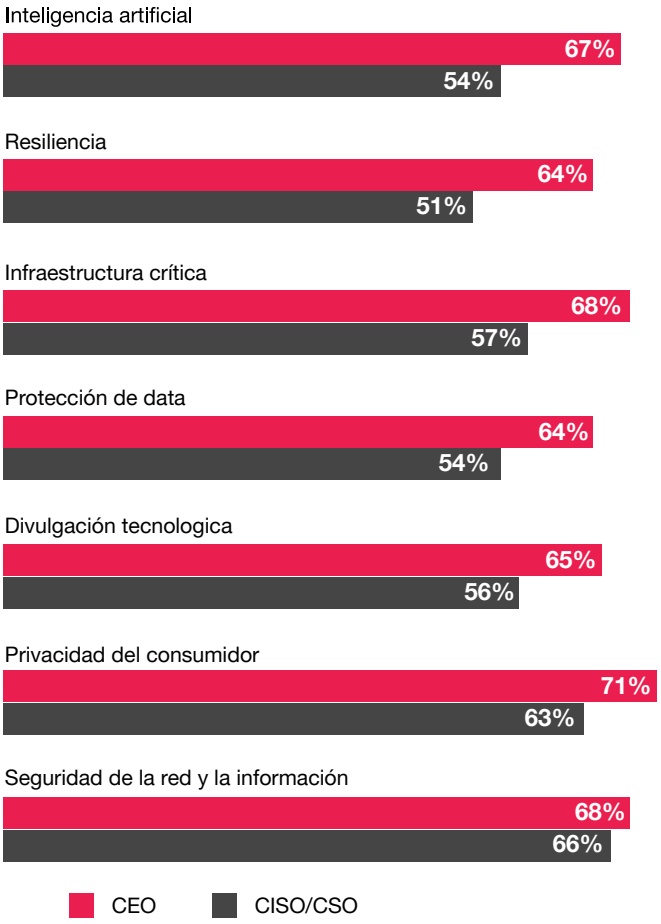
Brecha de confianza: los CISO se sienten menos seguros que los directores ejecutivos sobre el cumplimiento cibernético

A pesar de la creencia de que las regulaciones cibernéticas están ayudando a las organizaciones, existe una diferencia significativa entre la confianza de los CEO y los CISO/CSO en su capacidad para cumplir con estas regulaciones. Las brechas más grandes involucran el cumplimiento de los requisitos de IA, resiliencia e infraestructura crítica.

Los CISO, en la primera línea de la ciberseguridad, son menos optimistas que los CEO sobre la capacidad de su organización para cumplir con estos requisitos regulatorios. Dado que están más en sintonía con las dificultades operativas cotidianas, las limitaciones de recursos y las posibles vulnerabilidades que pueden obstaculizar el cumplimiento de las normas cibernéticas, es fundamental que comuniquen estos riesgos de manera más eficaz al equipo de liderazgo. ¿Qué los impide? Entre los obstáculos potenciales se incluyen las barreras a la participación de los CISO en las decisiones estratégicas y la incapacidad para justificar la cantidad de inversión necesaria en ciberriesgos.

Confianza en el cumplimiento normativo de la organización

Mostrando un % alto de confianza para el CEO frente al CISO/CSO



Llamada de atención

Los directores ejecutivos deben asegurarse de que los CISO no solo sean escuchados, sino que también cuenten con los recursos y el apoyo necesarios para cumplir con las exigencias regulatorias. Los CISO deben proporcionar información respaldada por datos y presentar argumentos comerciales para elevar el cumplimiento normativo a un imperativo estratégico.

Llamado a la acción ejecutivo

A medida que los requisitos normativos siguen dando forma al panorama de la ciberseguridad, es vital que los ejecutivos de los niveles más altos se mantengan a la vanguardia de los temas de cumplimiento normativo y aprovechen las regulaciones como catalizador de la innovación.

Crear una alineación entre los equipos de seguridad, las funciones de riesgo y el liderazgo ejecutivo es crucial para mantener la preparación para el cumplimiento normativo e impulsar mejoras estratégicas.

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

CFO: verificar la precisión e integridad de las divulgaciones regulatorias de la gestión de riesgos cibernéticos y el enfoque del programa. Desarrollar una comprensión clara de la materialidad y el impacto específico de un incidente cibernético, incorporando la cuantificación del riesgo para evaluar y comunicar con precisión las amenazas potenciales.

CEO: comprender las responsabilidades de supervisión para guiar los esfuerzos de cumplimiento, incluida cualquier coordinación necesaria entre diferentes unidades de negocios. Identificar preguntas clave para hacer a los CISO para cerrar cualquier brecha de conocimiento sobre el enfoque de cumplimiento.

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

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

Cómo liberar el potencial de la cuantificación del riesgo cibernético

15% está midiendo el impacto financiero de los riesgos cibernéticos para tomar medidas significativas.

87% dice que asignar recursos a áreas de alto riesgo es de gran importancia.

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

La medición del riesgo cibernético es fundamental pero limitada

Si bien los ejecutivos coinciden en que medir el riesgo cibernético es crucial para priorizar la inversión (89%) y asignar recursos a las áreas de mayor riesgo (87%), solo el 15% de las organizaciones realmente lo están haciendo en una medida significativa (por ejemplo, cuantificación extensa del riesgo cibernético con automatización e informes exhaustivos).

En el caso de las organizaciones que sí miden el riesgo, 7 de cada 10 ejecutivos indican que utilizan evaluaciones del enfoque de seguridad para cuantificar el riesgo residual teniendo en cuenta la eficacia de los controles clave, como el cumplimiento de la corrección de vulnerabilidades, las revisiones de acceso de los usuarios y la finalización de la formación. Sin embargo, la adopción de prácticas de cuantificación de riesgos cibernéticos más holísticas sigue siendo limitada.

Llamada de atención

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

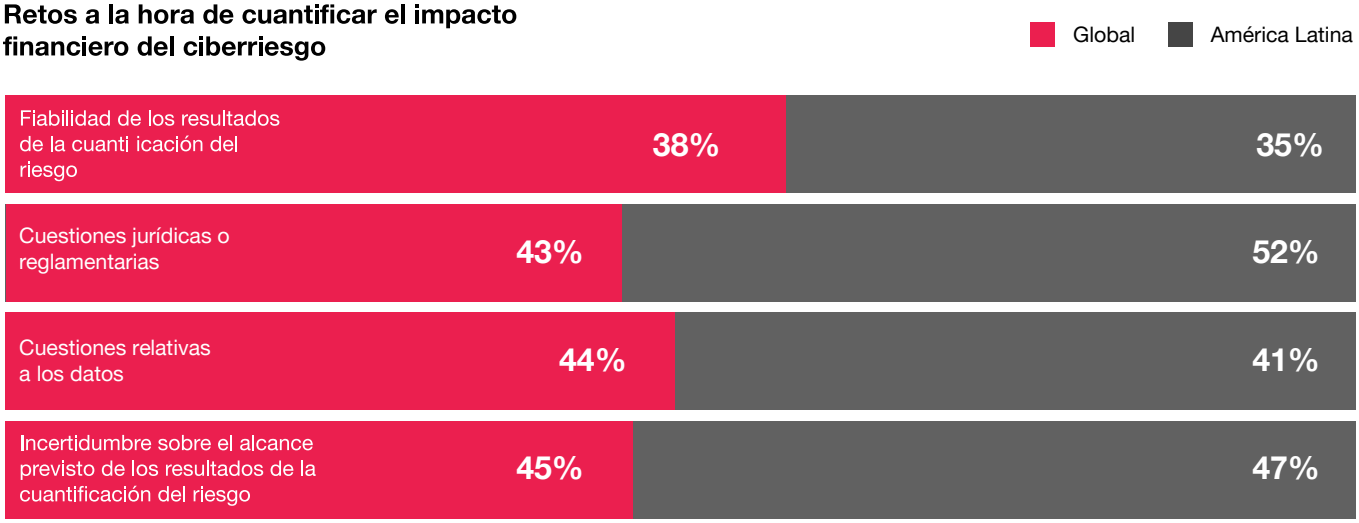
¿Cuáles son los obstáculos para una implementación más amplia?

Los problemas de datos, la incertidumbre sobre el alcance y las preocupaciones legales ocupan los primeros lugares de la lista de obstáculos para implementar la cuantificación del riesgo cibernético. La falta de confianza en la fiabilidad de los resultados de la cuantificación es otro de los obstáculos. Otro factor que complica aún más la adopción es la brecha entre lo que esperan lo que esperan la alta dirección y lo que ofrecen los CISO.

Llamada de atención

Las barreras para la adopción y el uso de la cuantificación del riesgo cibernético pueden estar frenando el progreso. Las organizaciones no pueden permitirse el lujo de permitir que estos desafíos obstaculicen la toma de decisiones críticas. Enfrente estos obstáculos, genere confianza en la cuantificación del riesgo cibernético e intégrela por completo en su proceso estratégico.

Retos a la hora de cuantificar el impacto financiero del ciberriesgo



Llamado a la acción ejecutivo

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

CISO: considere comenzar de a poco con un resultado específico en mente. Aproveche la información que tiene dentro de su organización (por ejemplo, efectividad de los controles, madurez, datos de incidentes o pérdidas). Las nuevas herramientas pueden ayudar con la cuantificación del riesgo, pero no son un requisito. Defina su programa y busque tecnologías habilitadoras para respaldar lo que ha diseñado.

CISO y CRO: muestre a los ejecutivos de la alta dirección los resultados de medición de riesgo financiero más impactantes de las herramientas y prácticas de cuantificación. Estos ejemplos pueden ayudar a persuadir a la dirección para que priorice y asigne los recursos adecuados a las áreas de mayor riesgo.

CEO: trabaje con su CISO y CRO para obtener una comprensión más profunda del valor comercial de la cuantificación del riesgo cibernético y los costos potenciales y las oportunidades perdidas por no medir los riesgos cibernéticos.

Invertir en resiliencia, generar confianza

77% espera que su presupuesto cibernético aumente el próximo año.

48% de los ejecutivos de empresas priorizan la protección y la confianza en los datos como la principal inversión en ciberseguridad para el próximo año

34% de los ejecutivos de tecnología dan prioridad a la seguridad en la nube como principal inversión tecnologica durante el próximo año.

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

Llamada de atención

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

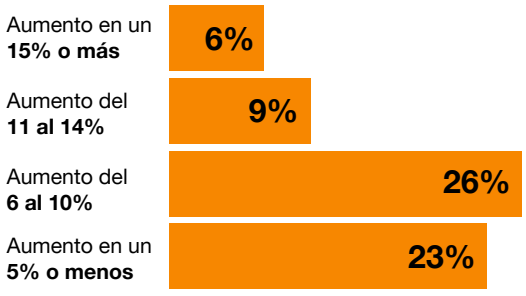
Se espera que los presupuestos cibernéticos aumenten el próximo año

Los presupuestos cibernéticos se mantienen en línea con el año pasado en las organizaciones más pequeñas invirtiendo un mayor porcentaje de sus recursos en comparación con las organizaciones más grandes. Esto probablemente refleja que las organizaciones más pequeñas están tratando de ponerse al día en áreas en las que las más grandes ya han invertido mucho.

Las organizaciones más grandes, aunque expresan inquietudes sobre las amenazas emergentes y la resiliencia, están adoptando un enfoque más medido para sus inversiones, probablemente debido a que cuentan con marcos de seguridad más establecidos.

Más de tres cuartas partes de los ejecutivos esperan que el presupuesto cibernético de su organización aumente el próximo año. Esa cifra es mayor (82%) en el caso de las organizaciones de América del Norte y del sector de tecnología, medios y telecomunicaciones (TMT).

Cambio en el presupuesto cibernético en 2025



Invertir en lo más importante: la confianza en la nube y los datos van de la mano

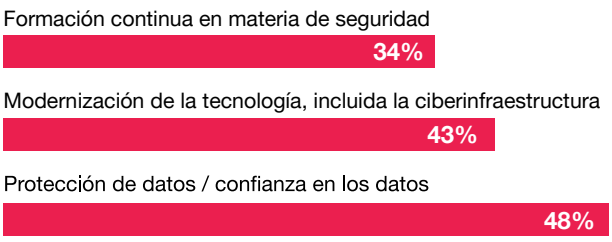
Durante los próximos 12 meses, las organizaciones priorizarán la protección de datos, confianza y la seguridad en la nube por sobre otras inversiones cibernéticas. Entienden que proteger la información confidencial es vital para mantener la confianza de las partes interesadas y la integridad de la marca.

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

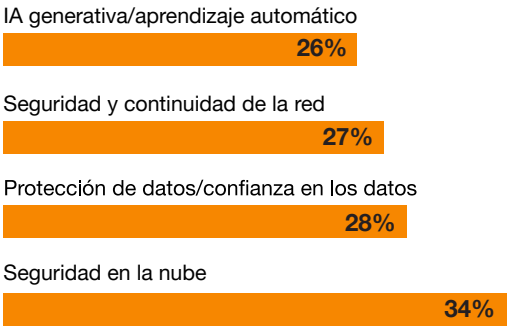
Los ejecutivos de empresas dicen que la protección de datos y la confianza son su principal prioridad de inversión en tecnología **(48%)**, seguida de la modernización y optimización tecnológica **(43%)**.

Para los ejecutivos de tecnología, la seguridad en la nube sigue siendo su principal prioridad **(34%)**, siguiendo la misma tendencia del año pasado. La protección de datos y la confianza es la siguiente **(28%)**.

Prioridades de inversión tecnológica para los líderes empresariales



Prioridades de inversión en tecnología para los líderes tecnológicos



¿Por qué la seguridad en la nube sigue demandando atención? A pesar de los años de inversión, la rápida adopción de tecnologías en la nube, la consolidación de hiperescaladores y el auge de las configuraciones híbridas y "multicloud" han concentrado el riesgo en el entorno de la nube.

Esta concentración aumenta el impacto potencial de las configuraciones incorrectas de acceso a los datos, las violaciones de datos y los desafíos de integración. A medida que los actores de amenazas evolucionan, también deben hacerlo las estrategias de seguridad en la nube, por lo que la inversión continua es crucial para mitigar estos riesgos intensificados.

Llamada de atención

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

Ciberseguridad y confianza: la nueva ventaja competitiva

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

Posicionar la ciberseguridad como ventaja competitiva

Llamada de atención

Su ciberseguridad no consiste únicamente en proteger los datos, sino también su marca. En un entorno competitivo, la confianza lo es todo. Refuerce sus medidas de seguridad ahora para ayudar a su organización a destacarse como líder en integridad de datos.

Llamado a la acción ejecutivo

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

CIO, CTO y CISO: explican las prioridades de inversión en seguridad de la nube y protección de datos a los CFO basándose en el valor comercial de los resultados clave (por ejemplo, reducir el tiempo de recuperación de datos críticos o aplicar parches a un sistema).

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

CDO: colaboran con los ejecutivos de tecnología, seguridad y finanzas para identificar las prioridades de seguridad e integridad de datos más esenciales para guiar la estrategia de inversión en seguridad de la información y la nube. Asegurar la calidad y la preparación de los datos es necesario para aumentar las inversiones en seguridad.

¿Su estrategia y liderazgo cibernéticos impulsan una resiliencia real?

2% Solo el 2% ha implementado acciones de resiliencia cibernética en toda su organización en las áreas evaluadas.

21% Solo el 21% suele asignar presupuesto cibernético a los principales riesgos de la organización.

50% Menos del 50% de los CISO participan en la planificación estratégica de inversiones cibernéticas.

Para gestionar las amenazas del futuro, las inversiones por sí solas no son suficientes: las organizaciones también deben mejorar su estrategia y liderazgo en materia de ciberseguridad.

Desde los esfuerzos de resiliencia rezagados hasta las deficiencias en la participación de los CISO en las decisiones estratégicas, hay áreas específicas que necesitan una alineación estratégica. Para lograrlo, las organizaciones deben emular las prácticas líderes en ciberseguridad de sus pares con mejor desempeño. También deben superar la simple respuesta a las amenazas conocidas e implementar un enfoque ágil y seguro para los negocios, que se esfuerce por generar confianza y resiliencia duradera.

La implementación parcial no es suficiente

A pesar de la creciente preocupación por el riesgo cibernético, la mayoría de las empresas tienen dificultades para implementar plenamente la resiliencia cibernética en sus prácticas básicas. Un análisis de 12 acciones de resiliencia en las áreas de personal, procesos y tecnología indica que el 42% o menos de los ejecutivos cree que sus organizaciones han implementado plenamente alguna de esas acciones.

Más preocupante aún es que solo el 2% afirma que se han implementado las 12 acciones de resiliencia en toda su organización. Esto deja una vulnerabilidad evidente: sin resiliencia las empresas siguen expuestas peligrosamente a las crecientes amenazas que podrían comprometer toda la operación.

Éstas son sólo algunas áreas clave que podrían beneficiarse de una atención interorganizacional:

Establecer un equipo de resiliencia (solo el 34% de los ejecutivos dice que esto se ha implementado en toda la organización).

Desarrollar un manual de recuperación de ciberseguridad para escenarios de pérdida de TI (solo el 35% dice que esto se ha implementado en toda la organización).

Mapear las dependencias tecnológicas (solo el 31% dice que esto se ha implementado en toda la organización).

Tecnología

Despliegue de la computación cuántica para la ciberdefensa y la resiliencia

Implementación de herramientas para una mayor visibilidad de los activos de tecnología operativa (OT)

Asignación de dependencias tecnológicas

Implantación de soluciones tecnológicas de ciberrecuperación (incluidas las copias de seguridad inmutables)

Global América Latina

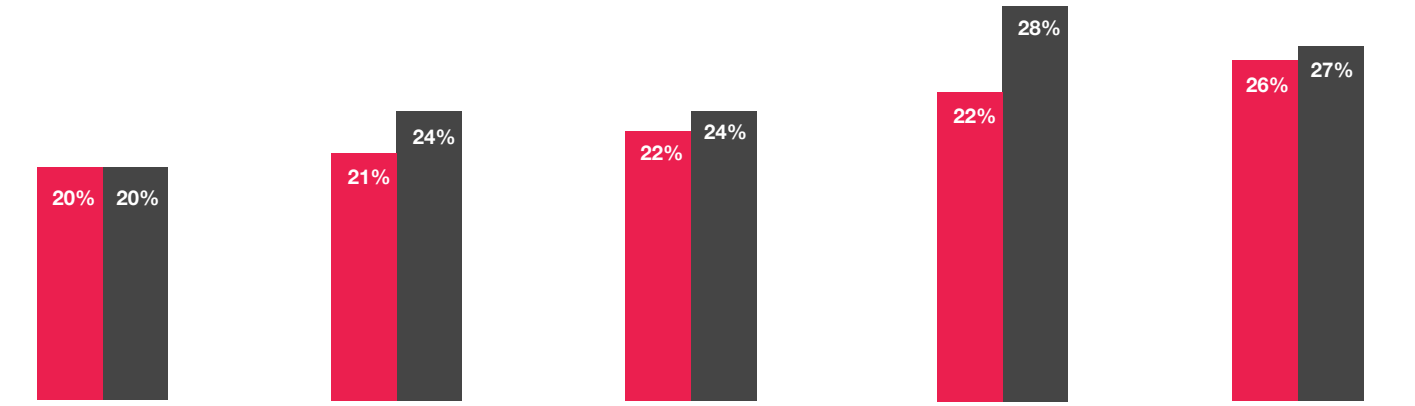
Llamada de atención

La falta de resiliencia cibernética pone en riesgo a su organización. Tome medidas a nivel de toda la empresa a través de la tecnología, procesos y el personal para transformar sus defensas y prepararse para los desafíos que se avecinan.

La ciber resiliencia es una prioridad clave. ¿Por qué tantas empresas están atrasadas en este punto?

Muchas empresas aún están atrasadas en lo que respecta a demostrar prácticas líderes en materia de ciberseguridad. Solo 1 de cada 5 ejecutivos señala que las pone en práctica de manera habitual. Por ejemplo, solo el 20% suele anticipar los riesgos cibernéticos futuros y el 21% suele asignar el presupuesto cibernético a los principales riesgos de la organización. Este retraso podría deberse a varios factores, entre ellos, la falta de previsión estratégica, recursos insuficientes o un enfoque reactivo en lugar de proactivo en materia de ciberseguridad.

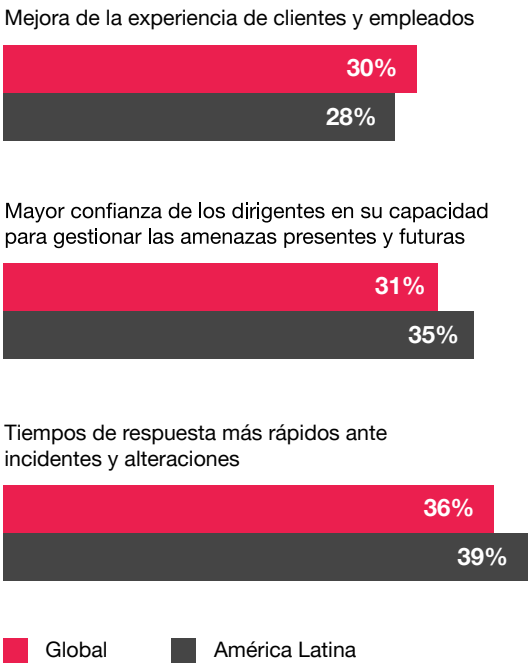
Comportamientos que "normalmente" realiza el equipo de ciberseguridad de una organización



Los ejecutivos más destacados sobresalen de manera constante y significativa en comparación con el resto.

Profundizamos en esta cuestión para identificar un grupo de ejecutivos que, de manera habitual, demuestran estos comportamientos. Se observa una diferencia de 69 puntos porcentuales en todos los comportamientos entre los ejecutivos más destacados y nuestros encuestados generales. Estos ejecutivos muestran una mayor confianza en la capacidad de su organización para cumplir con

Comportamientos que "normalmente" realiza el equipo de ciberseguridad de una organización



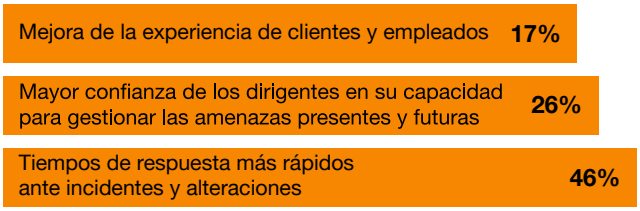
Llamada de atención

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

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

En los próximos 12 meses, más de un tercio de los ejecutivos espera trabajar para reducir los tiempos de respuesta a incidentes e interrupciones. Otros objetivos principales incluyen aumentar la confianza en la capacidad de los líderes para gestionar las amenazas y mejorar las experiencias tanto de los clientes como de los empleados. Estos objetivos reflejan un impulso más amplio no solo para mitigar los riesgos más rápidamente, sino también para generar confianza y proteger a los clientes y empleados.

Objetivos de la organización en materia de ciberseguridad y privacidad



Llamada de atención

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

Alineando la estrategia con la seguridad

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

Llamada de atención

De a su CISO un lugar en la mesa. Sus conocimientos son fundamentales para abordar de forma proactiva la ciberseguridad como un riesgo empresarial fundamental. Involucrarlo, ayuda a su organización a alinear su enfoque para proteger activos críticos e impulsar la resiliencia.

Llamada a la acción ejecutiva

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

CISO: presentar al resto de la alta dirección, el argumento comercial de por qué es imperativo que los CISO participen en la estrategia, planificación y supervisión de la estrategia de mitigación y resiliencia de riesgos cibernéticos.

CEO, CFO y CIO: participar en evaluaciones y ejercicios de resiliencia cibernética para comprender mejor las brechas y los enfoques que los CISO podrían enfrentar para integrar prácticas, estándares y controles líderes.

Acerca de este informe

El informe Global Digital Trust Insights 2025 se basa en una encuesta realizada por PwC entre mayo y julio de 2024, que reunió las opiniones de directivos y responsables de tecnología de compañías de 77 países.

Los encuestados operan en sectores muy diversos, como el industrial y de servicios; tecnología, medios de comunicación y telecomunicaciones; servicios financieros; retail y consumo masivo; energía, servicios públicos y recursos; salud; y servicios gubernamentales y públicos.

El desglose regional es el siguiente: Europa occidental (30%), América del Norte (25%), Asia Pacífico (18%), América Latina (12%), Europa central y oriental (6%), África (5%) y Oriente Medio (3%).

Global Digital Trust Insights conocida anteriormente como la Encuesta sobre el estado global de la seguridad de la información (GSISS, por sus siglas en inglés), se encuentra en su 27.° edición y es la encuesta anual sobre tendencias de ciberseguridad que más tiempo lleva realizándose.

Esta encuesta fue realizada por PwC Research, el Centro de Excelencia de PwC para investigación y análisis de mercado. Más información acá.

Contactos

Diego Taich
Socio,
PwC Argentina
diego.taich@pwc.com | LinkedIn

Sebastián Santana
Senior Manager,
PwC Argentina
sebastian.santana@pwc.com | LinkedIn

Rafael Pereira
Manager,
PwC Uruguay
rafael.p.pereira@pwc.com | LinkedIn

pwc

@PwC_Uruguay /PwCUruguay @pwc_uruguay @pwc_uruguay /pwc-uruguay