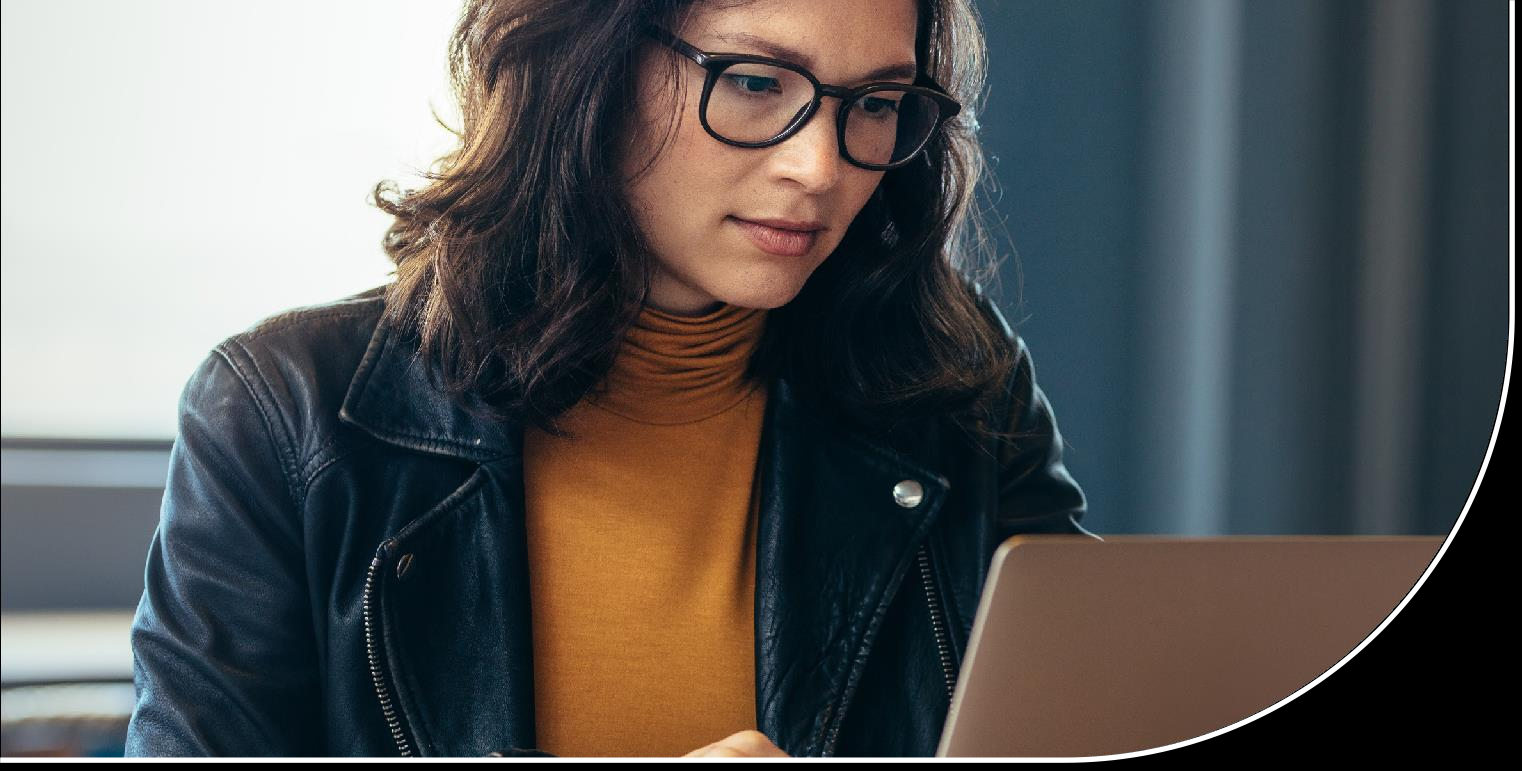
pwc

El libro de jugadas de la C-Suite:

Situar la seguridad en el epicentro de la innovación

Conclusiones del Global Digital Trust Insights 2024



Seguridad en el epicentro de la innovación: ese no es el mundo en el que vivimos hoy, pero ¿y si lo fuera?

Mientras aumentan el entusiasmo y los presupuestos para programas de seguridad de vanguardia, el progreso en la mejora real de la seguridad es lento, incluso está estancado.

La encuesta Global Digital Trust Insights 2024 de PwC, realizada a 3.876 ejecutivos de empresas y de tecnología de las mayores compañías mundiales (el 30% de los encuestados tiene unos ingresos de US$10.000 millones o más), muestra un considerable margen de mejora en ciberseguridad.

Tenga en cuenta estas conclusiones. Los costes de las filtraciones y el número de filtraciones de gran cuantía siguen aumentando. Aunque los ataques a la nube son la principal preocupación cibernética, alrededor de un tercio de las organizaciones no tienen un plan de gestión de riesgos para hacer frente a los retos de los proveedores de servicios en la nube. Sólo la mitad está "muy satisfecha" con sus capacidades tecnológicas en áreas clave de ciberseguridad. Más del 30% de las empresas no siguen sistemáticamente lo que deberían ser prácticas estándar de ciberdefensa.

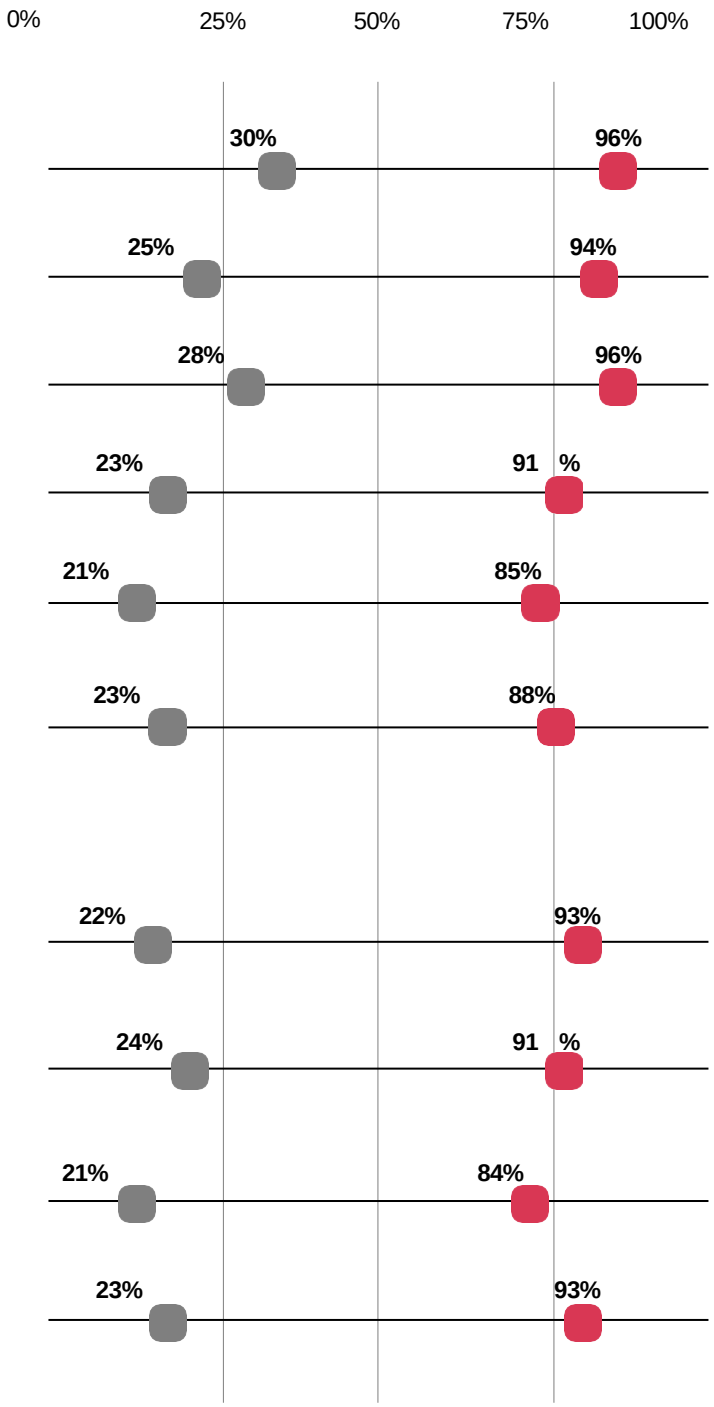
Imagine un mundo con la seguridad en el epicentro de la innovación, el campo donde florecen las ideas brillantes y las ambiciones audaces. Imagínese al Oficial de Seguridad de la Información (CISO, su sigla en inglés) allí mismo, trabajando para proteger las grandes ambiciones y los valiosos activos de la organización.

Hemos observado que 179 encuestados parecen estar haciendo precisamente eso. Este 5% —nuestros guardianes de la confianza digital— está cosechando beneficios que otros no están obteniendo. Sufren menos infracciones y los ataques que sufren no son tan costosos. Gestionar el riesgo es más fácil porque han racionalizado sus soluciones de seguridad. Y se han posicionado para una mayor productividad y un crecimiento más rápido, superando a la competencia a medida que se sumergen en las nuevas tecnologías con la confianza de que están bien protegidas.

Conozca a nuestros “administradores de la confianza digital”

Top 5% Todos los encuestados

Porcentaje que afirma que sus equipos cibernéticos “usualmente” (entre el 80% y el 100% de las veces) hace esto



Defensa

Responden rápidamente a las amenazas para que nuestra organización pueda emerger con más fuerza de las perturbaciones

Incorporan funciones de seguridad y privacidad de datos en productos, servicios y relaciones con terceros

Establecen controles en toda la organización para evitar graves perturbaciones cibernéticas

Asignan presupuesto cibernético a los principales riesgos de la organización

Mantienen relaciones con el sector público en todos los niveles administrativos para aumentar la resiliencia

Colaboran con otras partes del negocio que afectan a la postura de ciberseguridad de la organización (por ejemplo, ingeniería de software, gestión de productos, adquisiciones, marketing, etc.)

Disposición al crecimiento

Anticipan los futuros riesgos cibernéticos, teniendo en cuenta el entorno macroeconómico y la estrategia empresarial

Comunican nuestra estrategia y prácticas cibernéticas de forma que ayude a nuestra organización a ganarse la confianza de clientes y socios comerciales

Aceleran la transformación digital y otras iniciativas importantes de nuestra organización (por ejemplo, el diseño de la seguridad y la privacidad en nuevos productos y servicios)

Aportan conocimientos sobre la exposición a los riesgos cibernéticos cambiantes y las medidas de mitigación al director general y al consejo de administración

P26. Indique la frecuencia con la que el equipo de ciberseguridad de su organización hace lo siguiente. Base: 3.876 encuestados.
Fuente: PwC, 2024 Global Digital Trust Insights.

Con la tecnología ahora en el corazón del negocio, salvaguardarla equivale a salvaguardar la empresa. Es por eso que en 2023 PwC creó un libro de jugadas para ejecutivos C-level para ayudarles a centrarse en las preguntas que deben responder con su CISO.

Hemos actualizado este libro de jugadas para 2024. Es probable que este sea un año decisivo. La ciberseguridad se enfrenta a cuatro grandes cambios, cada uno de los cuales podría ser perturbador por sí mismo.

- La insistencia de la C-suite en modernizar y mejorar la infraestructura tecnológica y las inversiones en un año de recorte de gastos e incertidumbre macroeconómica.
- El aumento de las ciberamenazas híbridas y la difuminación de la línea que separa el espionaje de la ciberdelincuencia, lo que propulsa la ciberdefensa al ámbito de la seguridad nacional.
- Una nueva tecnología innovadora (IA generativa) que aporta nuevas amenazas y promesas sin precedentes para la defensa.
- Normativas que exigen transparencia sobre incidentes cibernéticos y prácticas de gestión de riesgos que podrían marcar el comienzo de una nueva era de transparencia y colaboración.

Las empresas se reinventan. Los responsables políticos están pensando en nuevos enfoques regulatorios. ¿Son sus altos ejecutivos igual de innovadores a la hora de proteger sus organizaciones? ¿Hasta qué punto puede ser usted audaz y qué podría hacer de forma diferente?

9 grados de separación: los de mejor rendimiento *versus* el resto

Top 5% es:

6 veces más propenso a ya haber implementado iniciativas de ciberseguridad transformadoras de las que están obteniendo beneficios.

5 veces más propenso a estar muy satisfechos con sus capacidades tecnológicas cibernéticas actuales.

4 veces más propenso a actualizar continuamente su plan de gestión de riesgos para mitigar los riesgos de la nube.

9 veces más propenso a ser maduras en sus prácticas de ciberresiliencia.

Fuente: PwC, 2024 Global Digital Trust Insights.

Top 5% se inclina más por:

Invertir más en presupuesto cibernético, con un **85% aumentando su presupuesto cibernético en 2024** (frente al 79% general), de los cuales el 19% está aumentando el presupuesto cibernético en 2024 en un 15% o más, frente al 10% general.

Afirmar que la **brecha cibernética más perjudicial** de los últimos tres años les costó menos de US$ 100.000 (28% frente al 19% general).

Estar totalmente de acuerdo en que **su organización desarrollará nuevas líneas de negocio utilizando GenAI** (49% frente al 33% general).

Planear desplegar herramientas GenAI para la ciberdefensa (44% frente a 27%).

No estar de acuerdo con que "GenAI provoque un ciberataque catastrófico" (33% frente al 22% en general).

Gestión del ciberriesgo: madurar para la reinvención

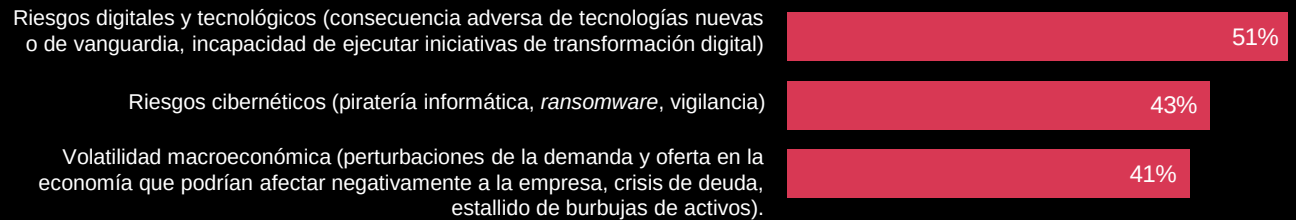
La innovación implica tomar medidas audaces, y no hay nada más alentador que saber que se ha hecho todo lo posible para mantener la seguridad, y que se han evaluado y abordado los riesgos cibernéticos más importantes.

Mitigar el ciberriesgo es una de las principales prioridades para 2024, según la encuesta Global Digital Trust Insights 2024 de PwC. Tras caer al cuarto puesto en la 26° CEO Survey del año pasado, ahora ocupa el segundo lugar para nuestros encuestados, solo por detrás de los riesgos digitales y tecnológicos en la lista de riesgos prioritarios. Y en la mente de nuestros encuestados, los riesgos digitales y tecnológicos son inextricables de los riesgos cibernéticos.

En el clima empresarial actual, simplemente no podemos hablar de transformación digital o reinvención sin mencionar la ciberseguridad al mismo tiempo. Los ataques a la nube y a los dispositivos conectados son las ciberamenazas que más preocupan a nuestros encuestados, dos tecnologías en el centro de la transformación empresarial actual.

Lo digital encabeza la lista de riesgos en dos aspectos

Prioridades de mitigación de riesgos en los próximos 12 meses (clasificadas entre las tres primeras)



P1. ¿Cuál de los siguientes riesgos está priorizando su organización para su mitigación en los próximos 12 meses? (Clasificados en los tres primeros puestos). Base: Todos los encuestados= 3.876
Fuente: PwC, 2024 Global Digital Trust Insights.

Estas ciberamenazas están conectadas entre sí. Una vez que los actores maliciosos penetran en los sistemas y redes, suelen causar estragos de tantas formas como sea posible.

Lo que puede comenzar como una brecha en la nube podría muy bien convertirse en una amenaza persistente avanzada, ya que los actores maliciosos acechan dentro de su sistema recopilando datos y buscando otras formas de hacer daño. Pueden extraer sus datos, lanzar un ataque de *ransomware* y filtrarlos ("hackear y filtrar") aunque pagues el rescate.

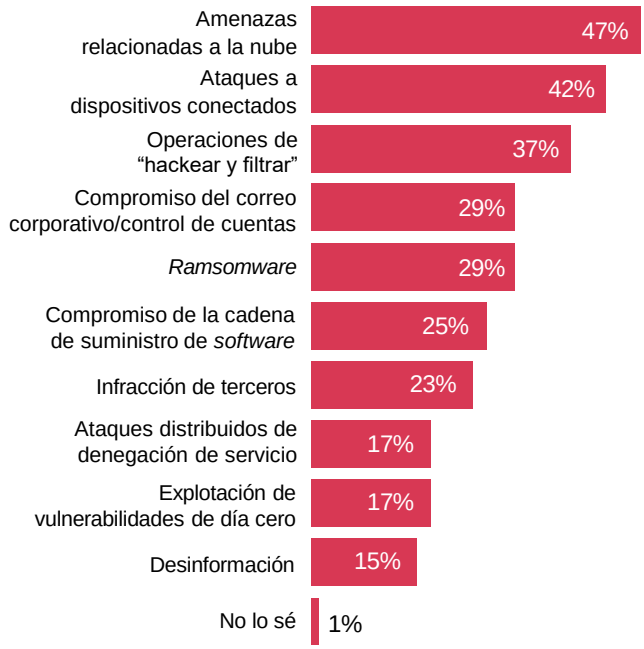
Cualquiera de estos incidentes sería problemático por sí solo. En conjunto, pueden devastar sus operaciones comerciales y su reputación. Las megabrechas aumentan en número, escala y coste. El porcentaje de los que informan de costes de US$ 1 millón o más por su peor brecha en los últimos tres años aumentó al 36% desde el 27% del año pasado.

El ritmo de reinvención e innovación empresarial mediante el uso de la tecnología no se está ralentizando. No cuando el 40% de los CEO piensa que sus empresas podrían dejar de ser económicamente viables dentro de una década si siguen por el camino actual.

El reto para la C-suite es el siguiente: ¿Está la gestión de riesgos cibernéticos de su organización a la altura de los cambios?

Todo está conectado, incluidos los ciberataques

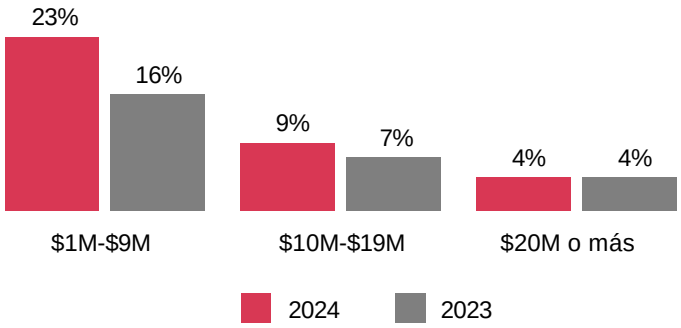
Principales ciberamenazas en los próximos 12 meses



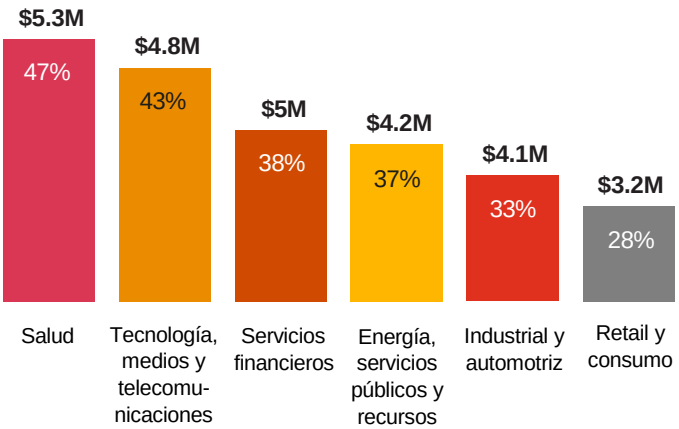
P3. En los próximos 12 meses, ¿cuál de las siguientes ciberamenazas preocupa más a su organización? (Clasificadas entre las tres primeras).
Base: Todos los encuestados= 3.876
Fuente: PwC, 2024 Global Digital Trust Insights.

Las filtraciones son cada vez más costosas

Costes estimados de la filtración de datos más perjudicial para las organizaciones en los últimos tres años
Porcentaje que afirma haber sufrido una filtración de más de US$ 1 millón: total 2024 = 36%, total 2023 = 27%



Coste medio de la filtración en millones y porcentaje de las filtraciones más perjudiciales que costaron US$ 1 millón o más, por sector



P5. En relación con la filtración de datos más perjudicial que haya sufrido en los últimos tres años, indique una estimación del coste para su empresa. Base de encuestados sobre seguridad, TI y directores financieros = 1.651
Fuente: PwC, 2024 Digital Trust Insights.

Simplificación de las ciberherramientas: la perdición de los malos actores

La modernización y la optimización encabezan las prioridades de ciberinversión para 2024. Casi la mitad (49%) de los líderes empresariales eligieron la modernización tecnológica, incluida la de la infraestructura cibernética, y el 45% la optimización de las tecnologías e inversiones existentes.

En nuestra encuesta de 2022 descubrimos que a los CEO en particular les preocupaba mucho que sus organizaciones se hubieran vuelto demasiado complejas para protegerlas. En ese momento, el 32% había consolidado los proveedores de tecnología en un esfuerzo por simplificar, así como realinear su combinación de servicios gestionados e internos.

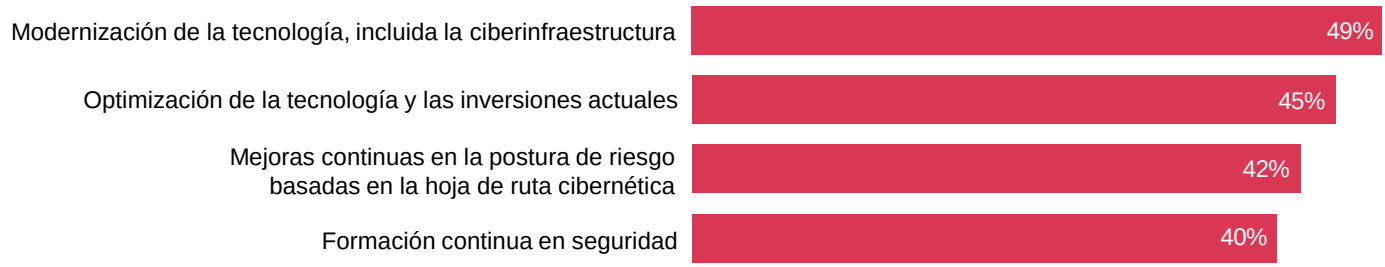
En la encuesta de 2024, el 44% afirma utilizar un conjunto integrado de soluciones de cibertecnología, y el 39% tiene previsto pasarse a uno en los próximos dos años. Casi una quinta parte (19%) afirma que tiene demasiadas soluciones cibernéticas y necesita consolidarlas.

El exceso de soluciones puntuales puede ser una de las razones por las que sólo el 5% de los encuestados de tecnología de la información (TI) afirman estar "muy satisfechos" con las capacidades tecnológicas de sus soluciones cibernéticas en las ocho áreas clave. El *software* que no funciona en conjunto puede obstaculizar el rendimiento, requerir más tiempo de gestión e impedir la visión de conjunto que es esencial para gestionar el riesgo cibernético.

Los que ya se han visto afectados lo saben. Los encuestados que han sufrido filtraciones de datos por valor de US$ 1 millón o más en los últimos tres años son más propensos a reconocer que tienen demasiadas soluciones de ciberseguridad y que necesitan integrarlas. Por otro lado, las organizaciones que utilizan conjuntos de soluciones cibernéticas cohesionadas suelen ser capaces de evitar las grandes y costosas filtraciones.

Los presupuestos de ciberseguridad para 2024 pretenden aprovechar al máximo las herramientas existentes

Líderes empresariales - Prioridades de inversión en ciberseguridad en los próximos 12 meses (clasificación de las tres principales)



P14b. ¿Cuál de las siguientes inversiones considera prioritarias a la hora de asignar el presupuesto cibernético de su organización en los próximos 12 meses? Base: Empresas encuestadas= 1.925
Fuente: PwC, 2024 Digital Trust Insights.

Aun así, los encuestados no están frenando el gasto. Más de tres cuartas partes (79%) afirman que aumentarán sus gastos cibernéticos en 2024 (frente al 64% del año pasado), especialmente las grandes organizaciones con ingresos de US$ 5.000 millones o más. Las que prevén aumentos presupuestarios superiores al 15% tienden a ser empresas con ingresos de US$ 50.000 millones o más, o de los sectores de tecnología, medios de comunicación y telecomunicaciones, o las que prevén un mayor crecimiento de los ingresos en el próximo año.

Las inversiones cibernéticas también están representando una mayor proporción del presupuesto total de TI, OT y automatización. Observamos un aumento medio global hasta el 14 % en 2024, frente al 11 % en 2023.

El reto de la C-suite no es la falta de herramientas o de inversión. Se trata más bien de averiguar cómo puede aprovechar su organización los beneficios de sus inversiones. ¿Es su arquitectura informática demasiado compleja para protegerla adecuadamente? ¿Está facilitando que los actores de amenazas encuentren lagunas en su defensa?

Sólo la mitad está satisfecha con sus capacidades cibertécnicas

Capacidades tecnológicas de la organización en áreas clave de ciberseguridad

Sólo el 5% de los encuestados sobre seguridad y TI están muy satisfechos en todas las áreas.

P23. ¿Cuál es su grado de satisfacción con las capacidades tecnológicas de su organización en las siguientes áreas? Base: Encuestados sobre seguridad e informática= 1.517
Fuente: PwC, 2024 Global Digital Trust Insights.

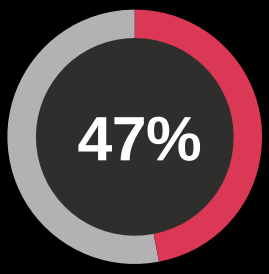
Seguridad en la nube: una atención concertada que llega con retraso

El uso de la nube siempre ha tenido que ver con la innovación empresarial y permitir que los desarrolladores colaboren en cualquier parte del mundo; adoptar formas de trabajo nuevas y más flexibles; inventar nuevos modelos de negocio; conectar tecnologías para mejorar el funcionamiento de la empresa; ofrecer un servicio superior a los clientes, etc.

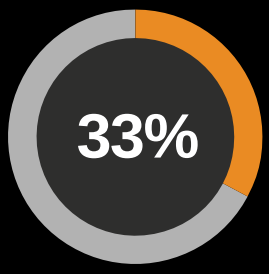
La seguridad en la nube es la principal preocupación en materia de ciberriesgos para casi la mitad (47%) de los encuestados. Las vías de entrada de los malos actores pueden parecer prácticamente ilimitadas.

La seguridad en la nube es la principal preocupación en materia de ciberriesgos para casi la mitad (47%) de los encuestados. Las vías de entrada de los malos actores pueden parecer prácticamente ilimitadas. Las organizaciones deben colocar controles en todas partes: en la identidad y el acceso, el movimiento lateral, las cuentas de correo electrónico, los portales de sitios web, las aplicaciones, la información propietaria, las interacciones con los clientes, los sistemas operativos, los dispositivos conectados, y la lista continúa.

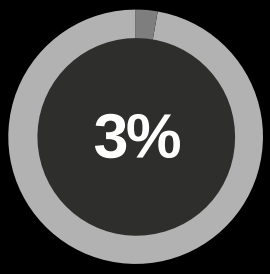
Seguridad en la nube: principal amenaza, principal inversión, pero mal gestionada



Principal amenaza



Principal ciberinversión



Plan de gestión de riesgos implementado y actualizado continuamente

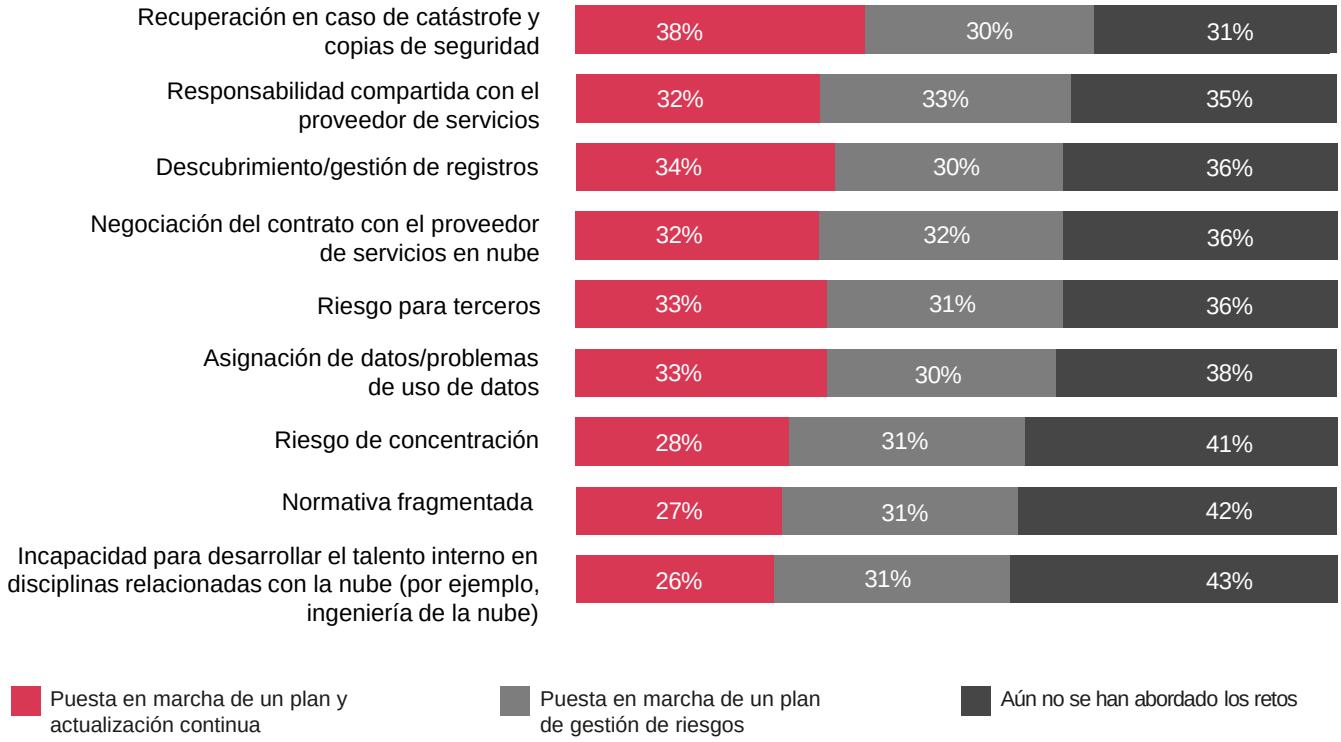
P3. En los próximos 12 meses, ¿cuál de las siguientes ciberamenazas preocupa más a su organización? (Clasificadas entre las tres primeras) Base: Todos los encuestados= 3.876
P14a. ¿Cuál de las siguientes inversiones está priorizando a la hora de asignar el presupuesto cibernético de su organización en los próximos 12 meses? (Clasificadas en los tres primeros puestos) Base: Encuestados de TI = 1.919
P19. ¿En qué medida ha abordado su organización los siguientes retos con su(s) proveedor(es) de servicios en la nube? Base: Usuarios de proveedores de servicios en la nube= 3.648
Fuente: PwC, 2024 Global Digital Trust Insights.

Muchos de nuestros encuestados (42%) utilizan más de una nube, y la preocupación por la seguridad en la nube aumenta entre los usuarios de nubes múltiples (híbridas). El 54% de estos encuestados citan la nube como su riesgo de ciberseguridad más apremiante. Los usuarios de nubes híbridas también son los más propensos a seleccionar la nube entre sus tres prioridades de inversión en seguridad para el próximo año (36% frente al 33% general).

Sin embargo, casi todas las organizaciones (97%) tienen lagunas en su plan de gestión de riesgos en la nube. Sólo el 3% mantiene planes actualizados que abordan las nueve áreas de seguridad de la nube. Por ejemplo, el 42% aún no ha abordado los riesgos que plantea la fragmentación de la normativa; el 41% no tiene un plan para hacer frente al riesgo de concentración; el 36% aún no ha abordado el riesgo de terceros en la nube.

Tantos riesgos en la nube y tan pocos planes para gestionarlos

Posición de la organización ante los retos de los proveedores de servicios en nube



P19. ¿En qué medida ha abordado su organización los siguientes retos con su(s) proveedor(es) de servicios en la nube?
Base: Usuarios de proveedores de servicios en la nube= 3648
Fuente: PwC, 2024 Global Digital Trust Insights.

El 5% superior —nuestros "administradores de la confianza digital"— tienen cuatro veces más probabilidades de actualizar continuamente su plan de gestión de riesgos para mitigar los riesgos de la nube. El resto de nuestros encuestados, sin embargo, todavía tienen que hacer gran parte de este trabajo crítico.

El reto de la C-suite es el siguiente: ¿Cómo trabajar juntos y con sus proveedores de seguridad en la nube para avanzar en la defensa de los puntos de entrada más importantes a sus sistemas y activos a través de la nube?

El auge de la IA generativa para la ciberdefensa

Casi siete de 10 afirman que su organización utilizará IA generativa (GenAI, en inglés) para la ciberdefensa. Las herramientas GenAI pueden ayudar a reducir la desventaja de los equipos cibernéticos abrumados por el gran número y complejidad de los ciberataques dirigidos por humanos, ambos en continuo aumento.

GenAI para la ciberdefensa

69%

Más de dos tercios afirman que utilizarán GenAI para ciberdefensa en los próximos 12 meses.

47%

Casi la mitad ya está utilizando GenAI para la detección y mitigación de ciberriesgos.

21%

Una quinta parte ya está viendo los beneficios de GenAI en sus programas cibernéticos, apenas unos meses después de su debut.

P7. ¿En qué medida está de acuerdo o en desacuerdo con las siguientes afirmaciones sobre la IA Generativa?
P10. ¿En qué medida su organización aplica o tiene previsto aplicar las siguientes iniciativas de ciberseguridad? Base: Todos los encuestados= 3.876
Fuente: PwC, 2024 Global Digital Trust Insights.

Las plataformas están concediendo licencias de sus grandes modelos lingüísticos (LLM, su sigla en inglés) junto con sus soluciones de cibertecnología. Microsoft Security Copilot pretende ofrecer funciones de GenAI para la gestión de la postura de seguridad, la respuesta a incidentes y la elaboración de informes de seguridad. Google anunció Security AI Workbench para casos de uso similares.

Muchos proveedores están forzando los límites de la GenAI, probando lo que es posible. Podría pasar algún tiempo antes de que veamos un uso a gran escala de las GPT de defensa. Mientras tanto, he aquí las tres áreas más prometedoras para el uso de GenAI en ciberdefensa.

- **Detección y análisis de amenazas.** GenAI puede ser inestimable para detectar de forma proactiva las vulnerabilidades, evaluar rápidamente su alcance (qué está en riesgo, qué está ya comprometido y cuáles son los daños) y presentar opciones probadas de defensa y reparación. GenAI puede ayudar a identificar patrones, anomalías e indicadores de compromiso que eluden los sistemas tradicionales de detección basados en firmas.
- **Informes sobre ciberriesgos e incidentes.** GenAI también podría simplificar los informes sobre ciberriesgos e incidentes. Con la ayuda del procesamiento del lenguaje natural (PLN), GenAI puede convertir datos técnicos en contenidos concisos que puedan entender personas sin conocimientos técnicos. Puede ayudar a elaborar informes de respuesta a incidentes, inteligencia sobre amenazas, evaluaciones de riesgos, auditorías y cumplimiento de normativas. Y puede presentar sus recomendaciones en términos que cualquiera pueda entender, incluso traduciendo gráficos confusos a texto sencillo.
- **Controles adaptables.** Proteger la nube y la cadena de suministro de *software* requiere actualizaciones constantes de las políticas y controles de seguridad, una tarea de enormes proporciones en la actualidad. Los algoritmos de aprendizaje automático y las herramientas GenAI pronto podrían recomendar, validar y redactar políticas de seguridad y automatizar controles adaptados al perfil de amenazas, las tecnologías y los objetivos empresariales de una organización.

El reto de la C-suite es el siguiente: ¿Cómo utilizar las nuevas herramientas sin provocar nuevos riesgos en la organización y en la sociedad? ¿Qué hacer para utilizar GenAI de forma ética y responsable?

Regulaciones: un lugar seguro para jugar y crecer

La opinión generalizada es que las nuevas normas y regulaciones obstaculizan los ingresos, pero ésta es la opinión de al menos un tercio de los encuestados: las barreras que ponen los reguladores pueden dar a las empresas más confianza para explorar, experimentar, inventar y competir. Cumplir los requisitos normativos puede convertirse en una ventaja competitiva para las empresas líderes.

Alrededor de un tercio de los encuestados de este año coinciden en que cuatro tipos de regulación serán los más importantes para garantizar el crecimiento futuro de su organización: la regulación de la IA (37%), la armonización de la cibernética y las leyes de protección de datos (36%), la notificación obligatoria de la gestión, estrategia y gobernanza de los ciberriesgos (35%) y los requisitos de resistencia operativa (32%).

La transparencia es el tamborileo normativo que se hará más fuerte en todo el mundo. Las nuevas normas de la SEC exigen la divulgación pública de las brechas de ciberseguridad que se considere que pueden tener un efecto material en los inversionistas. La Ley de Mercados Digitales y la Ley de Servicios Digitales requieren transparencia en las prácticas de datos y toma de decisiones algorítmicas. Y en el horizonte se vislumbran regulaciones que regularán la IA, como la Ley de Inteligencia Artificial de la UE y la normativa GenAI.

Regulaciones que podrían cambiar la ciberseguridad

Objetivos y principios regulatorios con mayor repercusión en el futuro crecimiento de los ingresos de la organización (los tres más importantes)

P24. ¿Cuáles de los siguientes objetivos y principios regulatorios propuestos tendrán un mayor impacto en la capacidad de su organización para garantizar el crecimiento futuro de sus ingresos? (Clasificados entre los tres primeros). Base: Todos los encuestados= 3.876
Fuente: PwC, 2024 Global Digital Trust Insights.

El lento avance de la ciberresiliencia

Grado de aplicación de las medidas clave de resiliencia en materia de ciberseguridad

P8. ¿En qué medida está aplicando o tiene previsto aplicar su organización las siguientes medidas de ciberresiliencia?
Base: Todos los encuestados= 3.876
Fuente: PwC, 2024 Global Digital Trust Insights.

La resistencia operativa es otro tema importante. Los reguladores saben que es un gran riesgo abordar el reto de los riesgos interrelacionados y complejos como todavía hacen habitualmente muchos equipos de dirección: como un ejercicio basado en silos que trata el perfil de riesgo de cada unidad de negocio por separado. Los nuevos requisitos, como la Ley de Resiliencia Operativa Digital, insistirán cada vez más en una resiliencia integrada con elementos básicos que hagan que una organización sea adaptable, flexible y con más fuerza después de cada acontecimiento perturbador.

Hasta tres cuartas partes esperan que el cumplimiento de estas normativas requiera importantes desembolsos de dinero y tiempo. Los elevados costes y el impacto en los ingresos pueden evitarse si las empresas se implican desde el principio y con frecuencia en los procesos normativos. Por ejemplo, reuniéndose con las fuerzas de orden, participando en comentarios públicos e incluso sentándose a la mesa con los reguladores para ayudar a elaborar o influir en las directivas propuestas.

El reto para la C-suite es el siguiente: en medio de la incertidumbre normativa, ¿puede dar a su organización el margen necesario para innovar, manteniendo al mismo tiempo la seguridad y la privacidad desde el diseño? ¿Cómo convertir este nuevo entorno normativo en una fuente de ventaja competitiva?

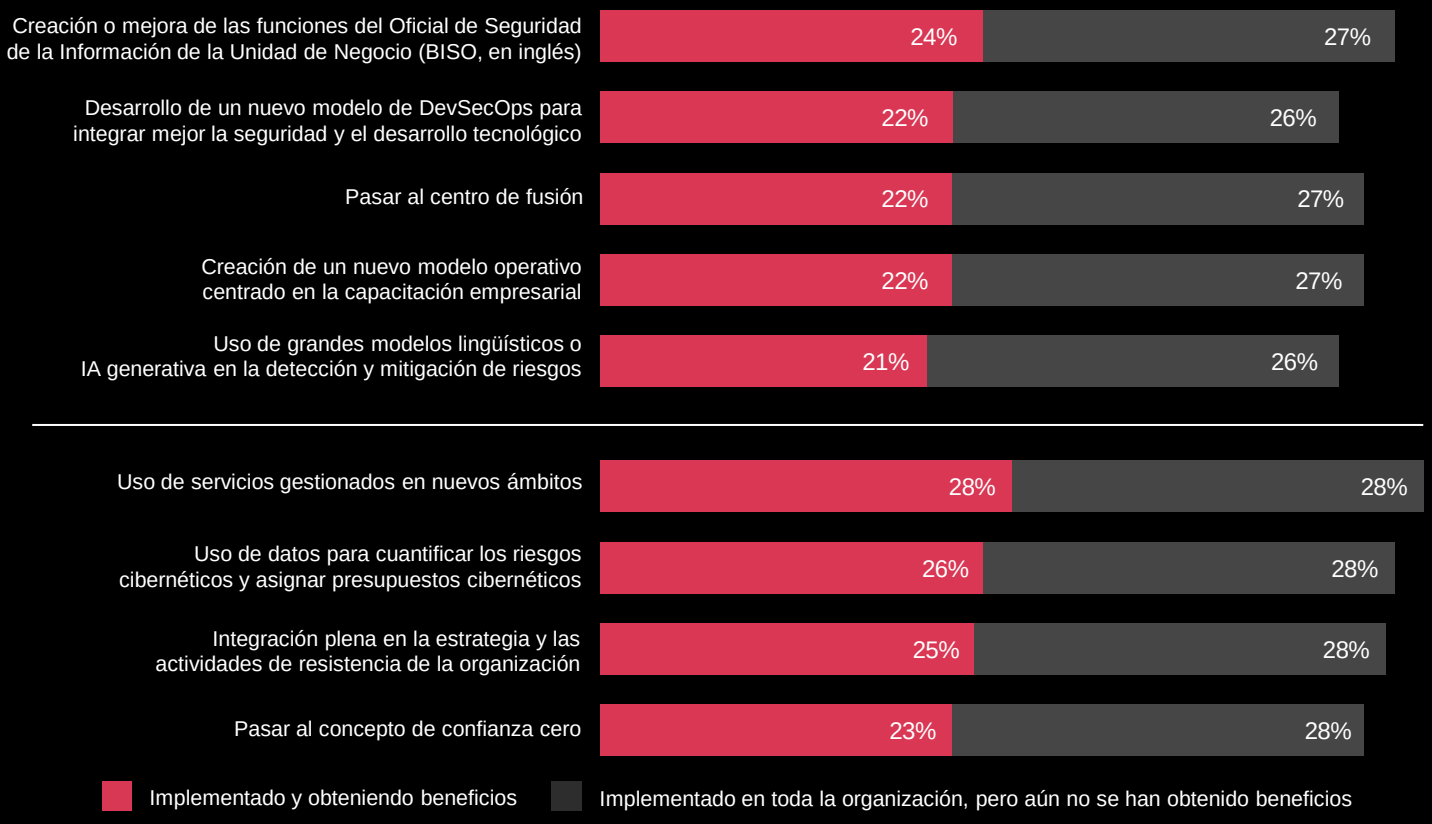
Atrévase a romper con lo cibernético habitual: el libro de jugadas para la C-suite 2024

Ya no es el "negocio de siempre" en su organización. Pero la mayoría de las empresas siguen atrapadas en la ciberseguridad de siempre, como muestra la encuesta Global Digital Trust Insights 2024. Iniciativas fragmentadas. Un abanico de complejidades tecnológicas en constante expansión. Un programa de gestión de riesgos que, con sus lagunas, es arriesgado en sí mismo.

Transformaciones y proyectos que no producen los resultados deseados. Estos y otros escollos siguen obstaculizando el camino hacia una ciberseguridad que sea realmente digna de confianza. En el libro de jugadas 2023, identificamos los retos críticos que los ejecutivos de la C-suite deben abordar juntos, como socios. Estos retos siguen siendo relevantes.

Regulaciones que podrían cambiar la ciberseguridad

Las iniciativas en la parte superior del gráfico están centradas en la cibernética; las de la parte inferior, en la empresa.



P10. ¿En qué medida su organización está aplicando o tiene previsto aplicar las siguientes iniciativas de ciberseguridad?
Base: Todos los encuestados= 3.876. La técnica de análisis utilizada es el análisis factorial.
Fuente: PwC, 2024 Global Digital Trust Insights.

En 2024, planteamos el reto:

¿Se atreve, como líder de la alta dirección, a salir de la inmovilidad y dar uno o dos pasos audaces que sean importantes para su organización?

¿O a dar ese salto imaginativo que podría despejar por fin los obstáculos que impiden a su empresa alcanzar sus objetivos?

Vemos que algunas empresas ya están eligiendo sus mejores apuestas. El abanico de opciones es amplio.

¿Cuál es la más adecuada para su organización?

Hable un nuevo idioma.

CISO CFO GC

Situarse en el epicentro de la innovación significa ir al encuentro de sus equipos de liderazgo donde ellos se encuentren y ayudarles a superar la intimidación que puedan sentir con respecto a lo que usted hace. Utilizar términos de iniciados como "ciberpaisaje", "superficie de ataque" e incluso "confianza cero" sólo puede desconcertar aún más a los ajenos a su profesión.

Atrévase a hablar de cibernética en lenguaje empresarial, tecnológico, financiero o cotidiano. Hable a sus clientes, inversionistas y socios comerciales en los informes anuales de seguridad de forma que informen y atraigan. Usar vocabularios comunes puede ayudar a los ejecutivos a lidiar con las compensaciones, las tensiones y el caos que inevitablemente se producen en el epicentro de la innovación.

Pruebe nuevas y audaces formas de gestionar el ciberriesgo.

CISO CRO IA CCO COO

Utilice enfoques más sofisticados para la modelización del riesgo cibernético, como la búsqueda de amenazas mediante fórmulas específicas para el sector, la visión y la estrategia de su empresa. Cree un incentivo de rendimiento vinculado al riesgo para cada empleado de la empresa con derecho a bonificación, a fin de crear una cultura del riesgo.

Invente nuevas formas de encontrar y reforzar sus puntos débiles, quizás con un moderno programa de recompensas por fallos que incentive la investigación independiente en materia de seguridad. Por último, adquiera y empiece a utilizar una solución de identidad gestionada centralmente que dé prioridad a la nube para garantizar sus objetivos de expansión empresarial.

Dar forma a los guardarraíles.

CISO CIO GC RA

Hable el lenguaje de la confianza, no sólo el del cumplimiento normativo. Involúcrese desde el principio y con frecuencia para tener más posibilidades de influir en las nuevas normas y garantizar que impulsen, y no obstaculicen, el éxito empresarial. La IA, el metaverso, las criptomonedas, la privacidad... estos temas normativos candentes podrían beneficiarse de su experiencia y conocimientos. Recuerde que los reguladores pueden sentirse tan desconcertados como cualquiera por el funcionamiento de la cibernética y la tecnología.

Libere a sus equipos para el pensamiento creativo (automatización, GenAI, servicios gestionados).

CISO CIO CTO CRO COO

Una de las ventajas de la automatización, GenAI y los servicios gestionados es que le permiten estar atento las 24 horas del día. Realizar tareas mundanas para que sus equipos no tengan que hacerlo es otra.

Liberados de la tiranía de las tareas tediosas, su personal puede encontrar tiempo y espacio para reflexionar sobre las nuevas amenazas cibernéticas y crear nuevas formas de frustrar las amenazas en evolución.

Dé la bienvenida a la cibernética en la sala de juntas.

CISO B CEO

La cibernética encabeza el registro de riesgos en la mayoría de las empresas y en muchas encuestas a ejecutivos. Pero ¿es un tema básico en la sala de juntas? ¿Obtiene información de calidad no sólo sobre los riesgos y controles cibernéticos, sino también sobre cómo las principales iniciativas estratégicas están impulsando el crecimiento del negocio y los ingresos? La seguridad es la base de todo lo que hace la organización: finanzas, desarrollo, personal, tecnología y otras áreas de la empresa de las que probablemente hable cada vez que se reúna.

Mirar de frente a su programa cibernético puede ser un paso atrevido.

Piense como el dueño de la empresa.

CISO CEO

La transformación empresarial es una cosa. La cibertransformación no es otra. Son lo mismo. El CISO y el CEO necesitan adoptar ahora la cibernética como un esfuerzo de toda la empresa, poniéndose en el lugar del propietario de la empresa. ¿No querrían que todos los aspectos —registros financieros, investigación patentada, desarrollo de aplicaciones, datos de clientes y similares— estuvieran protegidos de la visualización o el uso no autorizados? ¿No querrían salvaguardar su marca? ¿No podría la ciberseguridad estimular innovaciones que ahorren dinero y ayuden a la empresa a crecer? Esta es la *raison d'etre* de la ciberseguridad.

Acerca de la encuesta

Global Digital Trust Insights 2024 es una encuesta realizada a 3.876 ejecutivos de empresas, tecnología y seguridad (CEOs, directores corporativos, CFOs, CISOs, CIOs y oficiales C-Suite) entre mayo y julio de 2023.

Cuatro de cada 10 ejecutivos pertenecen a grandes empresas con ingresos de US$ 5.000 millones o más. Y lo que es más importante, el 30% pertenece a empresas con ingresos de US$ 10.000 millones o más.

Los encuestados operan en una amplia gama de industrias, incluyendo la fabricación industrial (20%), servicios financieros (20%), tecnología, medios de comunicación, telecomunicaciones (19%), mercados minoristas y de consumo (17%), energía, servicios públicos y recursos (11%), salud (9%) y gobierno y servicios públicos (3%).

Los encuestados proceden de 71 países. El desglose regional es Europa Occidental (32%), Norteamérica (28%), Asia Pacífico (18%), Latinoamérica (10%), Europa del Este (5%), África (4%) y Oriente Medio (3%).

La encuesta Global Digital Trust Insights se conocía hasta ahora como Global State of Information Security Survey (GSISS). En su 26º año, es la encuesta anual más antigua sobre tendencias de ciberseguridad. También es la mayor encuesta del sector de la ciberseguridad y la única que cuenta con la participación de altos ejecutivos de empresas, no sólo de seguridad y tecnología.

PwC Research, el Centro de Excelencia global de PwC para la investigación de mercado y el conocimiento, llevó a cabo esta encuesta.

Contáctenos

Federico Morello
Socio Líder de Consultoría
PwC Chile
rfederico.morello@pwc.com

+56 9 8159 5402

Pablo de Uría
Socio de Technology
PwC Chile
pablo.de.uria@pwc.com

+56 9 6405 9516

Gabriela Diez
Socia de Technology
PwC Chile
gabriela.diez@pwc.com

+56 9 9549 3092

® PwC. Todos los derechos reservados. PwC se refiere a la red de firmas miembro de PricewaterhouseCoopers International Limited y/o a firmas individuales dentro de la red de PwC o a varias o todas ellas colectivamente, cada una de las cuales es una entidad legal separada e independiente. PricewaterhouseCoopers Consultores, Auditores Compañía Limitada es una sociedad chilena, miembro de dicha red de firmas.