Global Digital Trust Insights de 2024 de PwC Colombia

Tendencias de la ciberseguridad en Colombia: Poniendo la seguridad en el centro de la innovación.

Contenidos

1. **Gestión de riesgos de ciberseguridad:** Preparados para la reinvención

2. **Simplificación de las herramientas cibernéticas:** La pesadilla de los ciberdelincuentes

3. **Seguridad en la nube:** Protegiendo el futuro de forma coordinada

4. **El uso de IA generativa para ciberdefensa** en la hoja de ruta de las organizaciones

5. **Regulaciones:** Garantizando un entorno seguro para el desarrollo y crecimiento

6. **Desafiando lo convencional en Ciberseguridad:** El manual de estrategia de la alta dirección para 2024

Aunque el entusiasmo por implementar programas de seguridad sólidos y de vanguardia va en aumento, y que esto se ve reflejado en el incremento de los presupuestos destinados a la ciberseguridad, la realidad es que el progreso para mejorarla es desafiante e incluso se encuentra estancado en muchos casos.

La encuesta Global Digital Trust Insights de 2024 de PwC se aplicó a 3876 ejecutivos de negocios y tecnología en las empresas más grandes del mundo. 30 % de ellos, que tiene ingresos de 10.000 millones de dólares o más, mostró que existe un margen considerable para mejorar la ciberseguridad.

Entre los principales hallazgos globales, así como los asociados a las encuestas en Colombia, encontramos los siguientes aspectos:

- Los costos de las brechas de seguridad y el número de brechas de alto valor siguen en aumento.
- Aunque los ataques a la nube son la principal preocupación cibernética, únicamente una cuarta parte de las organizaciones en Colombia cuenta con un plan estructurado de gestión de riesgos para abordar los desafíos de los proveedores de servicios en la nube.
- Solo la mitad de los encuestados está “muy satisfecho” con sus capacidades tecnológicas en áreas clave de ciberseguridad.
- Más del 30 % de las empresas no sigue sistemáticamente lo que deberían ser prácticas estándar de ciberdefensa.

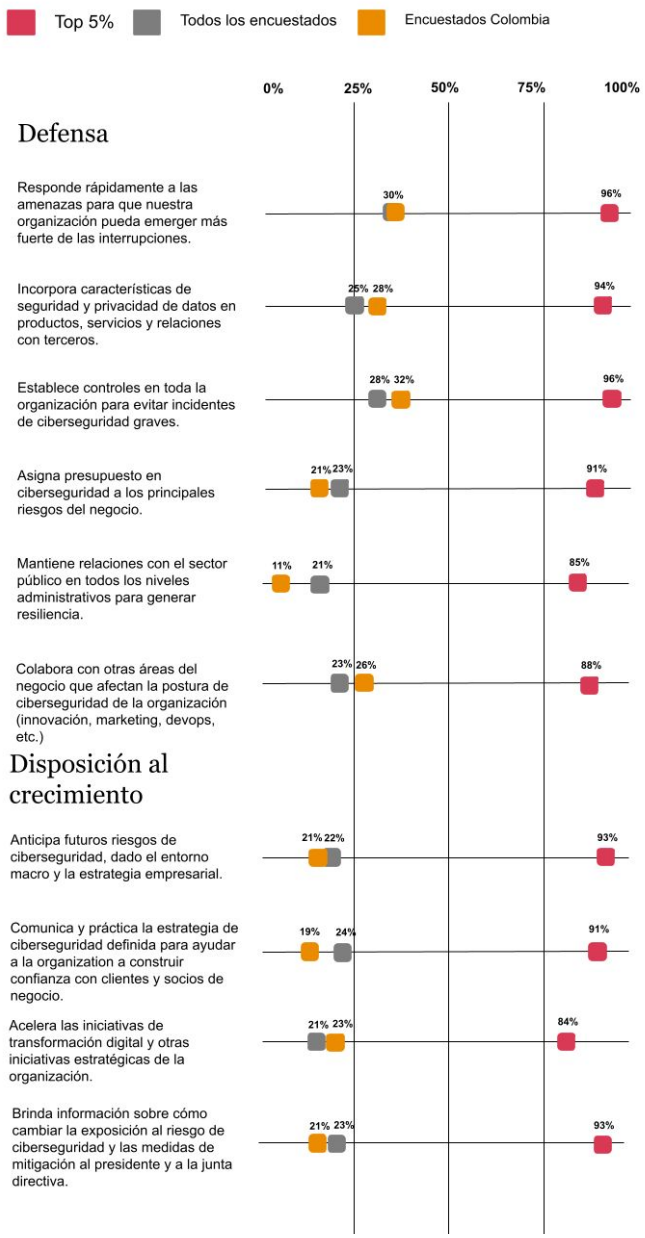
Actualmente, las empresas en Colombia y en el mundo, están apostando por la transformación y la innovación, conectando, cada vez más, las experiencias digitales gracias al uso de tecnologías disruptivas. Un contexto en el que la ciberseguridad debería situarse en el centro de la innovación.

Nuestro informe es una guía que recoge las iniciativas que, según la visión de los directivos encuestados, pueden apoyar la mejora de las capacidades de ciberseguridad de la organización.

Imagina un mundo donde la seguridad se sitúe en el centro de la innovación, un espacio donde broten ideas luminosas y ambiciones valientes. Visualiza al director de seguridad de la información (CISO, por sus siglas en inglés) en ese mismo lugar, esforzándose por proteger las grandes aspiraciones y los activos más valiosos de la organización.

Observamos que 179 encuestados parecen estar haciendo precisamente eso. Este 5 %, a quienes llamaremos *los guardianes de la confianza digital*, están obteniendo beneficios que otros están desaprovechando. Por ejemplo, están experimentando menos brechas y los ataques que los afectan no son tan costosos. Además, gestionan los riesgos de mejor manera porque optimizaron sus soluciones de seguridad y se han posicionado para tener una mayor productividad y un crecimiento más rápido, superando a la competencia mientras implementan nuevas tecnologías con la confianza de estar protegidos.

Imagen 1: Conoce a los guardianes de la confianza digital



Pregunta: Por favor Indica con qué frecuencia el equipo de ciberseguridad en tu organización realiza las siguientes acciones:

Fuente: Global Digital Trust Insights de 2024.

Imagen 2: 9 grados de diferencia. Los mejores frente al resto

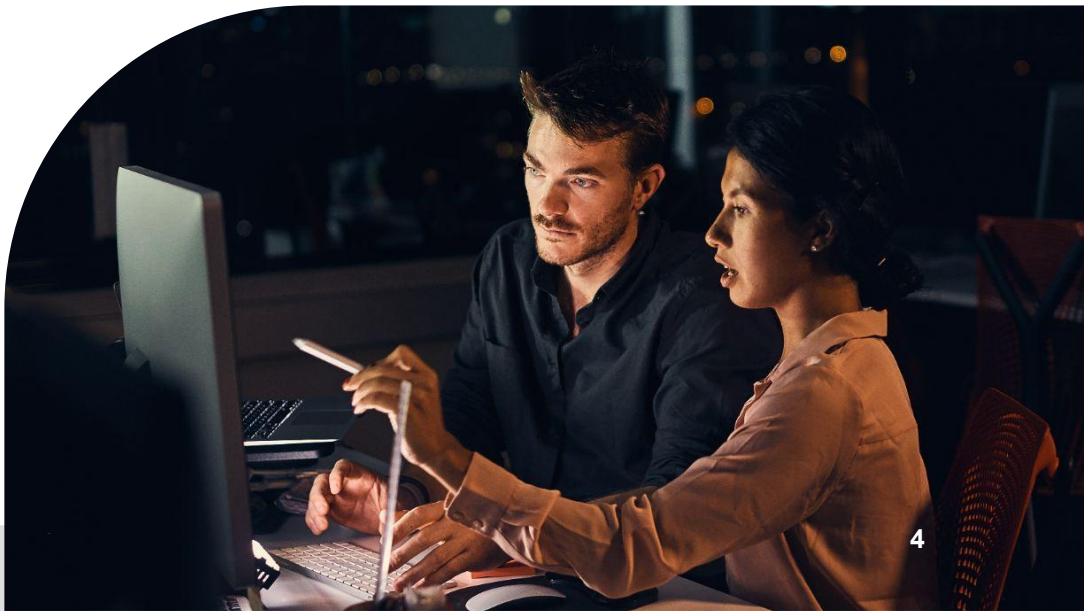
El top 5 % tienen:

- **6 veces más probabilidad** de haber implementado iniciativas transformadoras de ciberseguridad de las que están obteniendo beneficios.
- **5 veces más probabilidad** de estar muy satisfechos con sus capacidades actuales de tecnología en ciberseguridad.
- **4 veces más probabilidad** de actualizar continuamente su plan de gestión de riesgos para mitigar los riesgos en la nube.
- **9 veces más probabilidad** de ser maduros en sus prácticas de ciber-resiliencia.

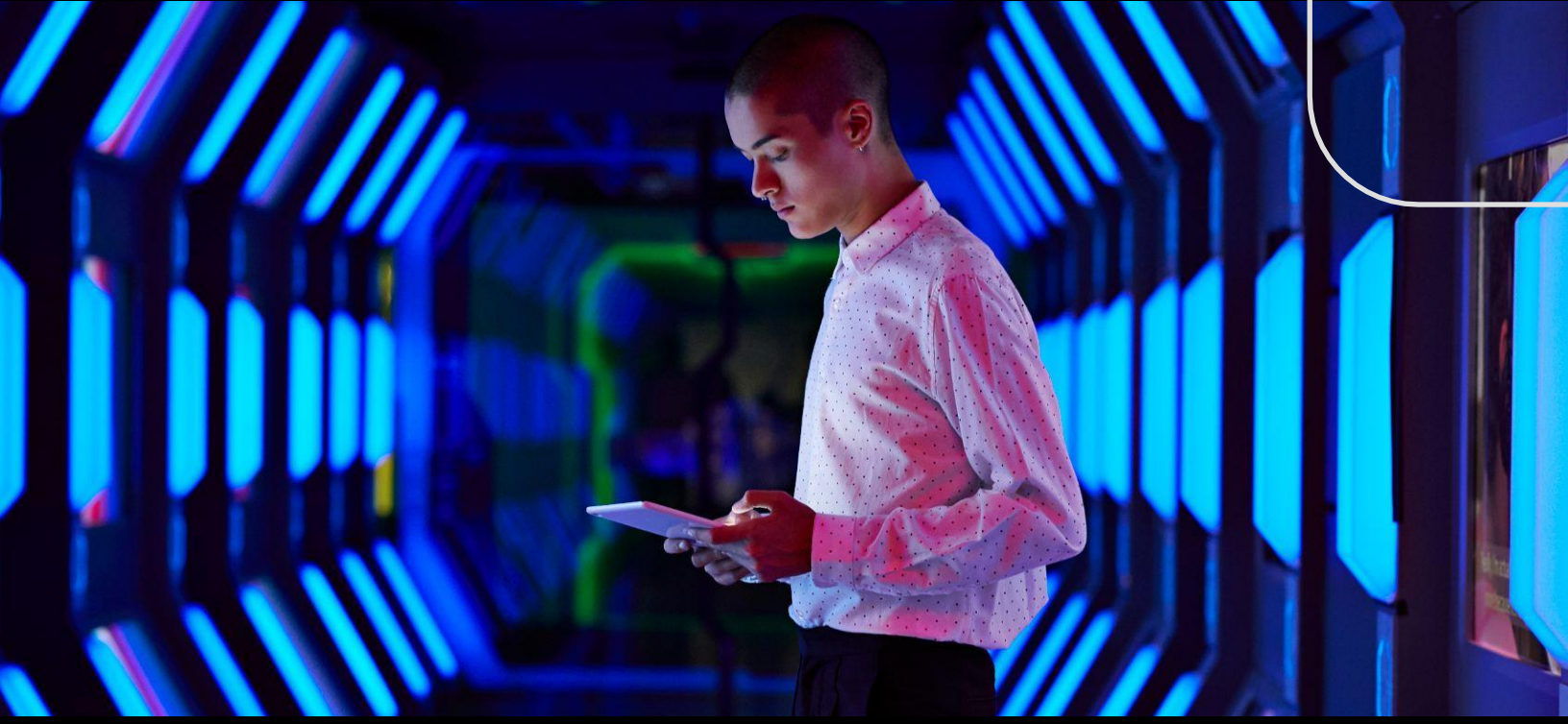
El top 5 % tiene más probabilidades de:

- Invertir más en el presupuesto de ciberseguridad: **el 85 % aumentará su presupuesto en 2024** (frente al 79 % en general).
- Dicen que el ciberataque más dañino en los últimos tres años **les costó menos de 100.000 dólares** (28 % frente a 19 % en general).
- Totalmente de acuerdo en que **su organización desarrollará nuevas líneas de negocio utilizando IA generativa** (49 % frente al 33 % en general).
- Planean implementar **herramientas de IA generativa para la ciberdefensa** (44 % frente a 27 %)
- **No están de acuerdo** en que la "IA generativa conducirá a un ciberataque catastrófico" (33 % frente a 22 % en general).

Fuente: Global Digital Trust Insights de 2024.



Gestión de riesgos de ciberseguridad: Preparados para la reinvención

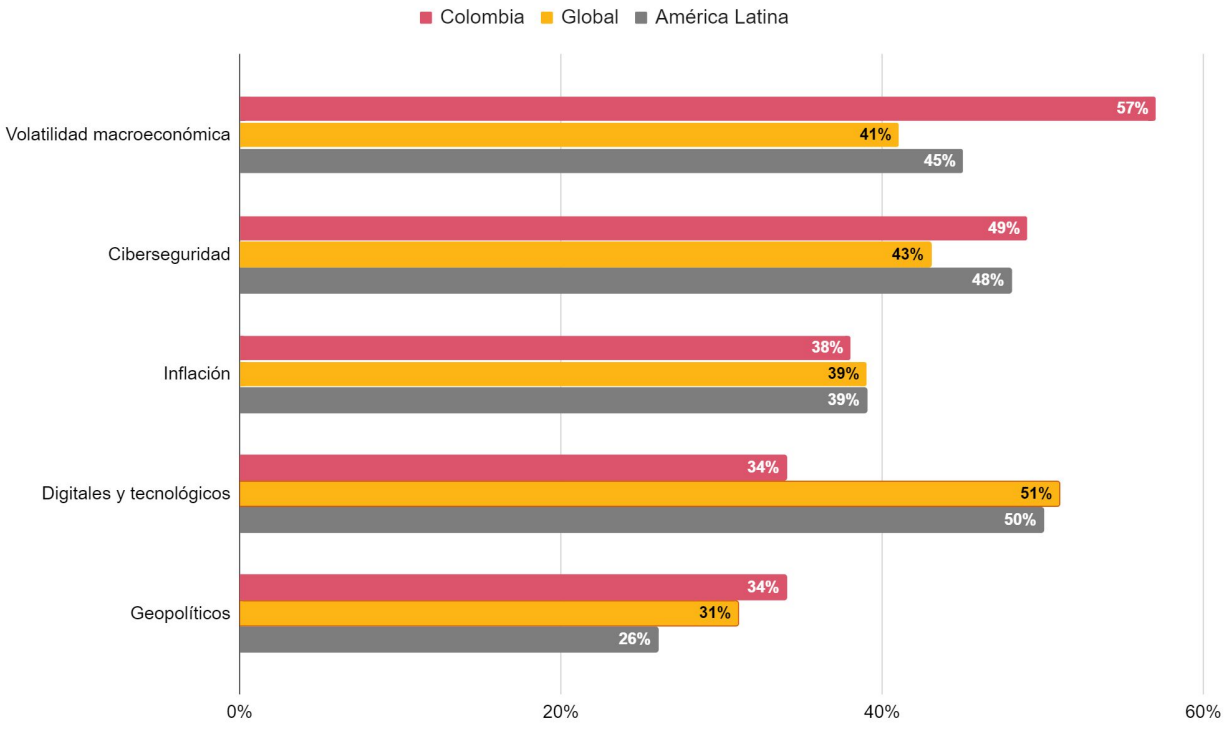


Innovar significa tomar medidas audaces y no hay nada más empoderador que saber que se ha hecho todo lo posible por mantener segura y protegida a la organización: se han evaluado y abordado los riesgos de ciberseguridad más importantes. La mitigación de los riesgos de ciberseguridad emerge como una de las prioridades cruciales para 2024, de acuerdo con la Encuesta Global Digital Trust Insights de 2024 de PwC.

En Colombia los riesgos de ciberseguridad se ubican detrás de los riesgos derivados de la volatilidad macroeconómica, mientras que a nivel global, el riesgo cibernético se ubica detrás de los riesgos digitales y tecnológicos. En la percepción de los líderes colombianos el foco está en hacer frente a los riesgos derivados de la situación económica actual, una condición que, sumada al contexto geopolítico del momento, puede potenciar los ciberataques. Por otro lado, en la percepción de los encuestados en el resto del mundo, los riesgos digitales y tecnológicos se entrelazan con los riesgos de ciberseguridad.

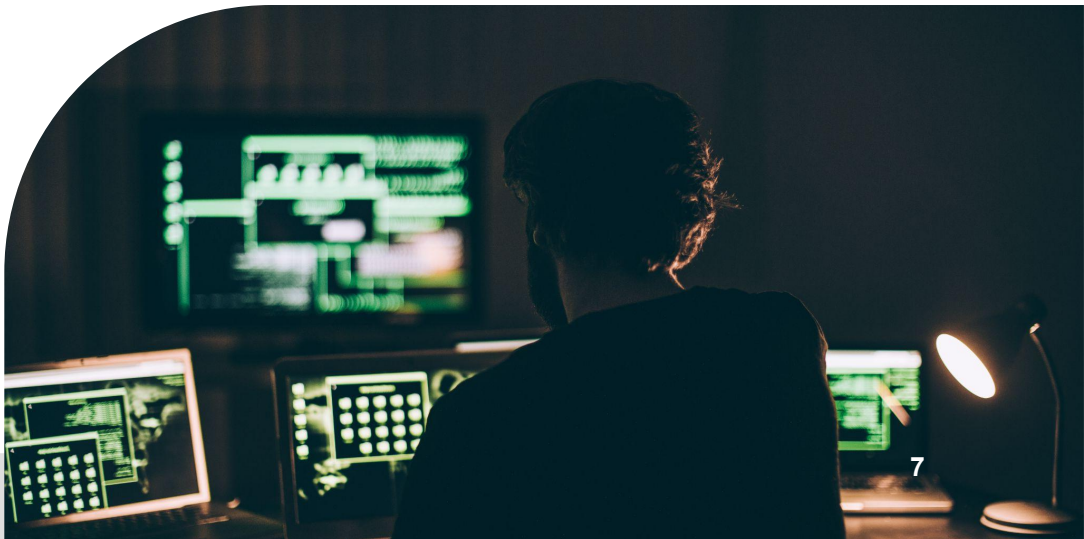
Gráfica 1: Riesgos priorizados para las empresas a corto plazo

Comparativo Colombia, Global y América Latina



Pregunta: ¿Qué riesgos está priorizando tu organización para su mitigación en los próximos 12 meses?

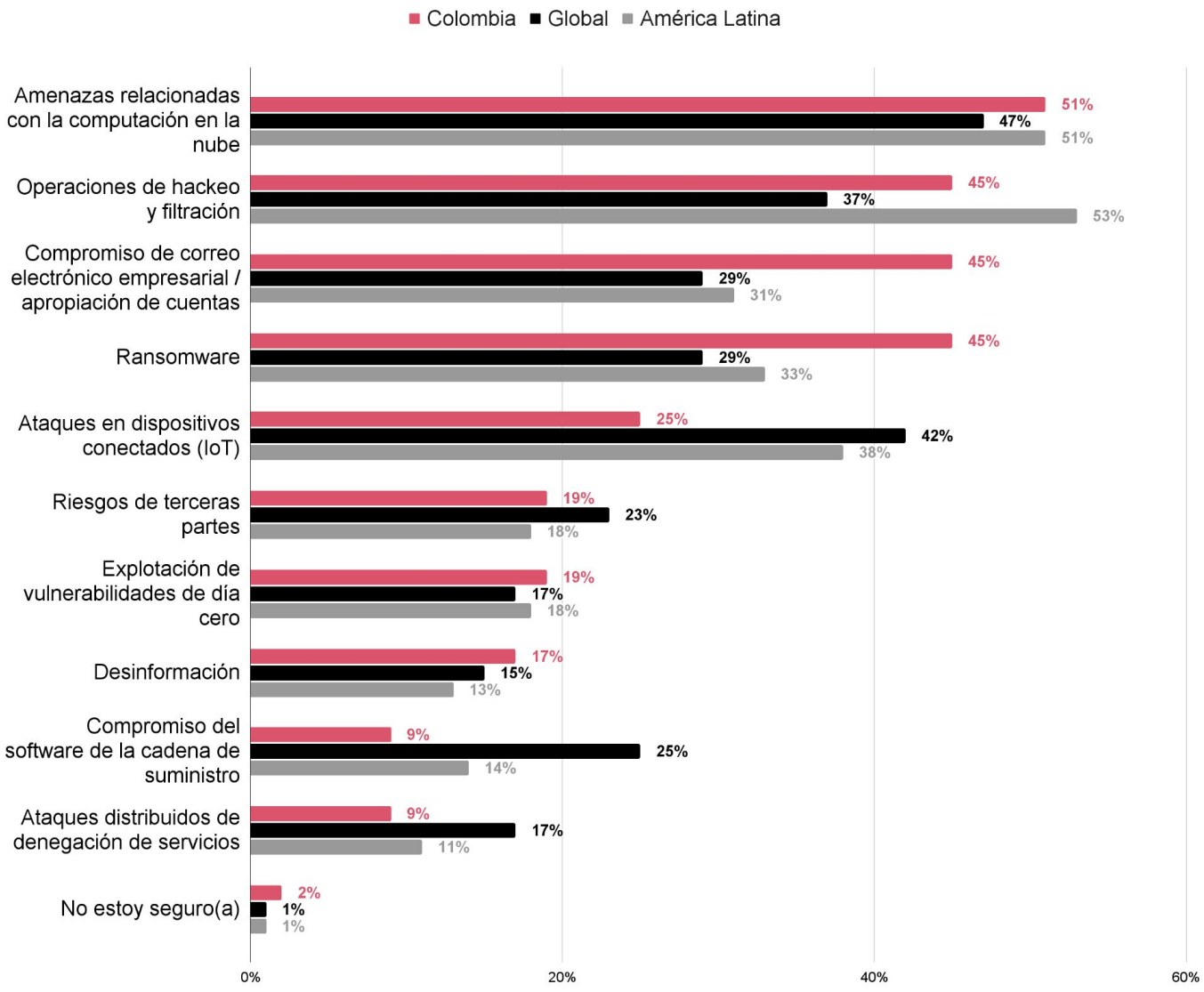
Fuente: Global Digital Trust Insights de 2024.



En el entorno empresarial actual, simplemente no podemos hablar de transformación empresarial o de transformación digital sin mencionar a la ciberseguridad. De acuerdo con esta afirmación, los ataques a la infraestructura en la nube, los ataques de *phishing* y los ataques a dispositivos conectados (IoT) son algunas de las amenazas que más preocupan a nuestros encuestados: tecnologías que están en el centro de la transformación empresarial actual.

Gráfica 2: Todo está conectado, incluyendo los ciberataques

Top de riesgos de ciberseguridad en los próximos 12 meses
Comparativo Colombia, Global y América Latina



Pregunta: Durante los próximos 12 meses, ¿cuál de las siguientes amenazas cibernéticas preocupa más a tu organización?
Fuente: Global Digital Trust Insights de 2024.

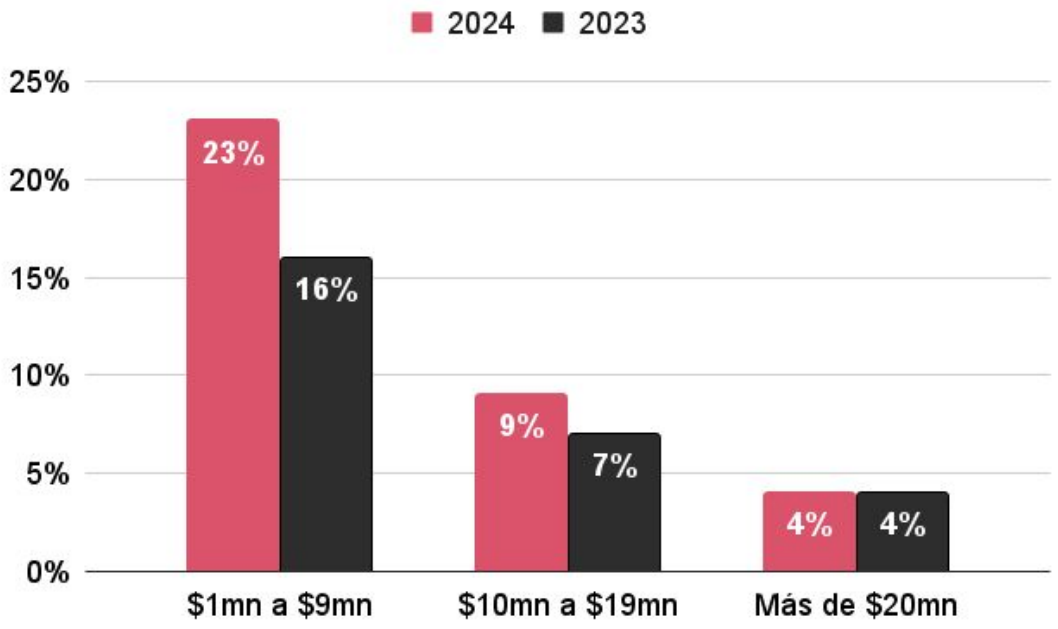
Estas amenazas de ciberseguridad en sí mismas están conectadas. Una vez que los actores maliciosos irrumpen en sistemas y redes, a menudo causan estragos en tantas formas como sea posible. Lo que puede comenzar como una vulneración de la infraestructura en la nube podría convertirse en una amenaza persistente avanzada, a medida que los delincuentes acechan dentro del sistema, recopilan datos y buscan otras formas de causar daño. Es posible que extraigan datos, luego lancen un ataque de *ransomware* y luego filtren los datos, incluso si la empresa paga el rescate.

Cualquiera de estos incidentes sería problemático por sí solo. En conjunto, pueden devastar las operaciones y la reputación de una empresa. Los incidentes de ciberseguridad de gran impacto están aumentando en número, escala y costo.

El porcentaje de quienes informaron costos de $1 millón de dólares o más por su peor incidente en los últimos tres años aumentó al 36 % (en América Latina fue de 18 % y en Colombia el 28 %), frente al 27 % del año pasado.

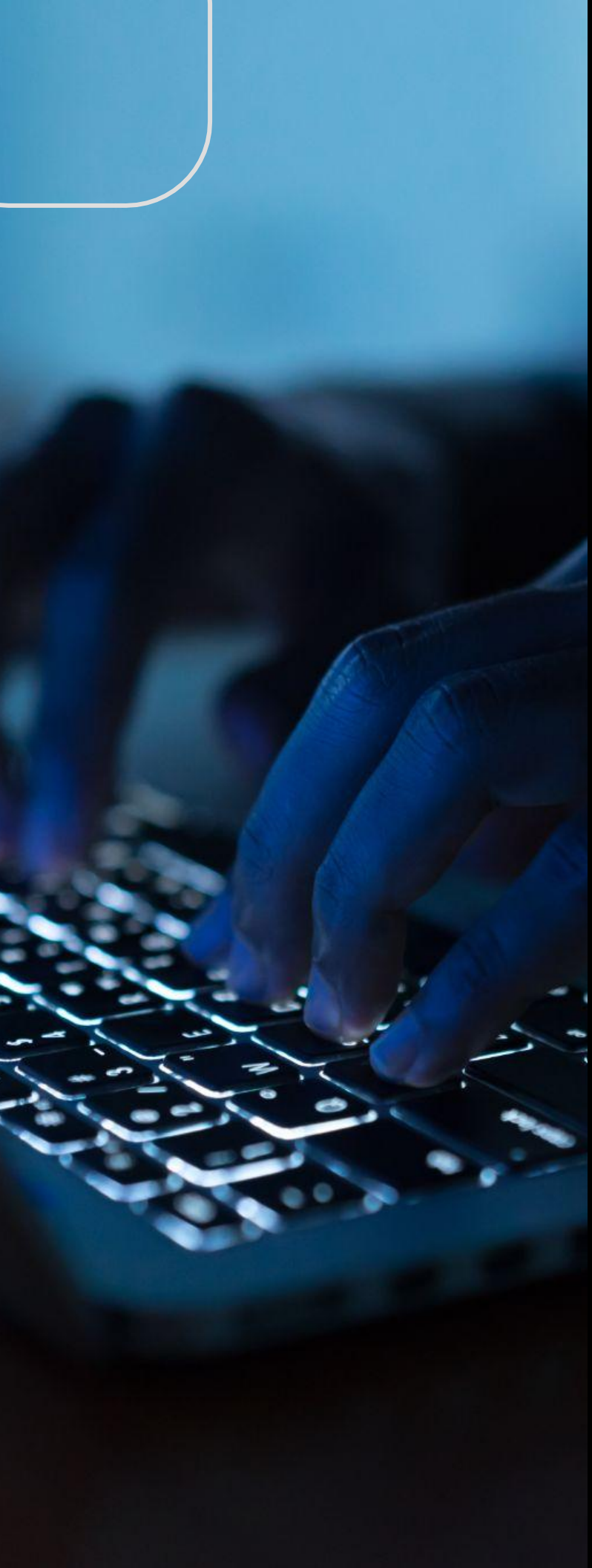
Gráfica 3: Los incidentes de ciberseguridad se vuelven más costosos

Costos estimados de las filtraciones de datos en los últimos tres años



Fuente: Global Digital Trust Insights de 2024.

Nota: Porcentaje que dice haber sufrido un incidente de más de un millón de dólares: total en 2024 = 36 %, total en 2023 = 27 %



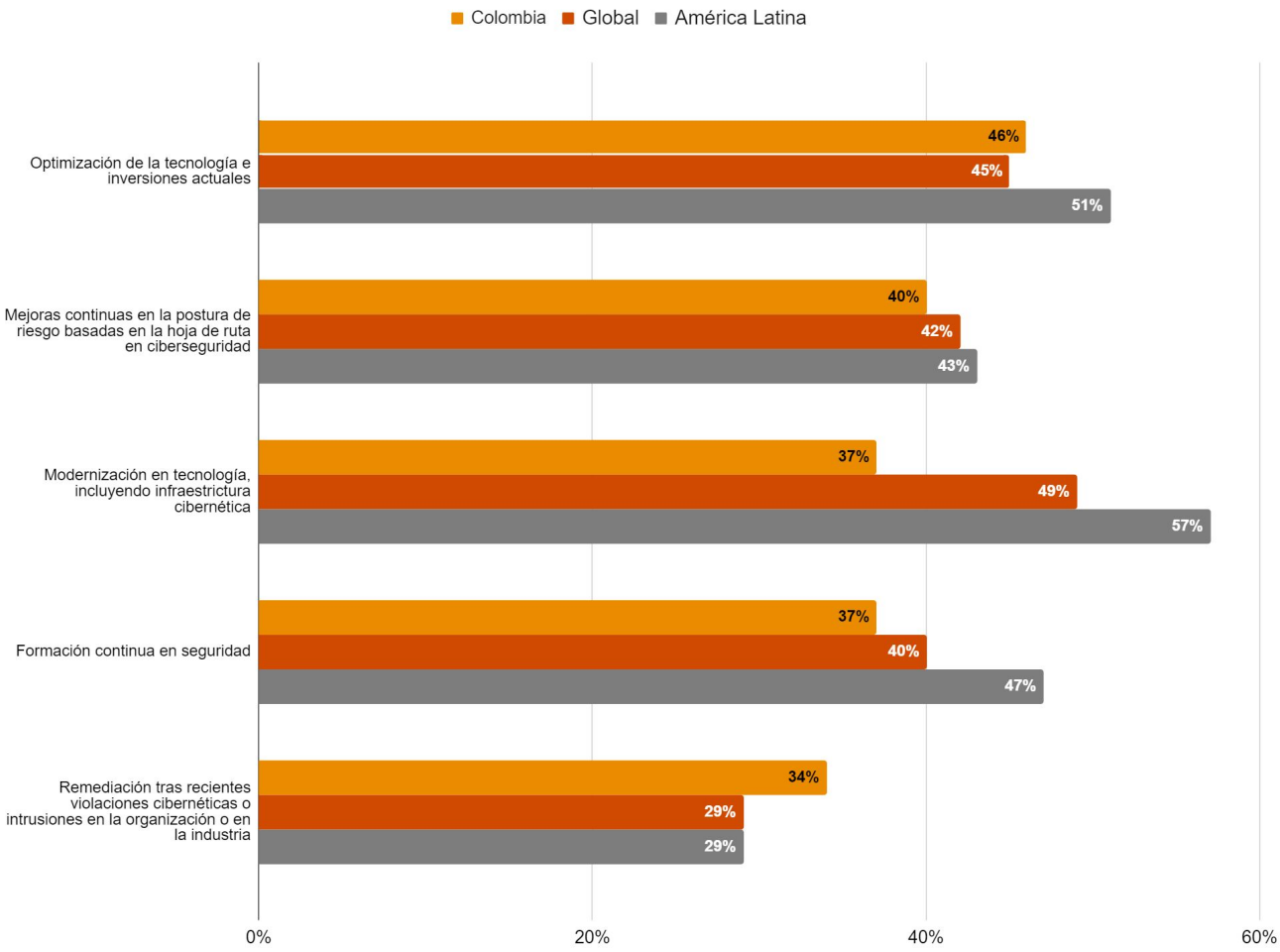
El ritmo de reinvención e innovación empresarial mediante la tecnología no muestra signos de desaceleración, especialmente, cuando el 30 % de los líderes de compañías en Colombia (40 % a nivel mundial) considera que sus empresas podrían dejar de ser económicamente viables dentro de una década, si continúan por el camino convencional.

El desafío para la alta dirección reside en lo siguiente: ¿Está la gestión de riesgos de ciberseguridad de la organización a la par de los cambios y transformación requeridos?

Simplificación de las herramientas cibernéticas: La pesadilla de los ciberdelincuentes

La modernización y la optimización encabezan las prioridades de inversión cibernética para 2024. Casi la mitad de los líderes empresariales en el mundo (49 % global y 37 % en Colombia) seleccionaron la modernización tecnológica, incluida la infraestructura cibernética, mientras que el 45 % a nivel global y el 46 % en Colombia optó por la optimización de las tecnologías e inversiones existentes.

Gráfica 4: El presupuesto para ciberseguridad en 2024 tiene como objetivo aprovechar al máximo las herramientas existentes



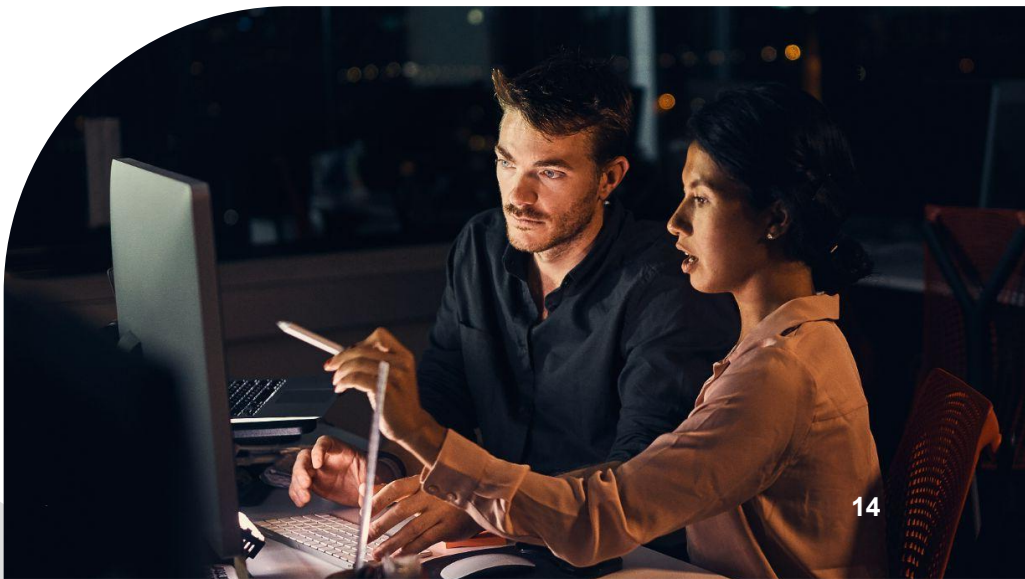
Fuente: Digital Pregunta: ¿Cuál de las siguientes inversiones prioriza tu organización al asignar el presupuesto para ciberseguridad durante los próximos 12 meses?
Fuente: Global Digital Trust Insights de 2024.

En nuestra encuesta de 2021, identificamos una preocupación pronunciada entre los altos ejecutivos, quienes, particularmente, sentían que sus organizaciones se habían tornado excesivamente complejas para ser protegidas adecuadamente. En ese contexto, el 32 % ya había consolidado proveedores de tecnología, en un esfuerzo por simplificar y reorientar su mezcla de servicios gestionados e internos.

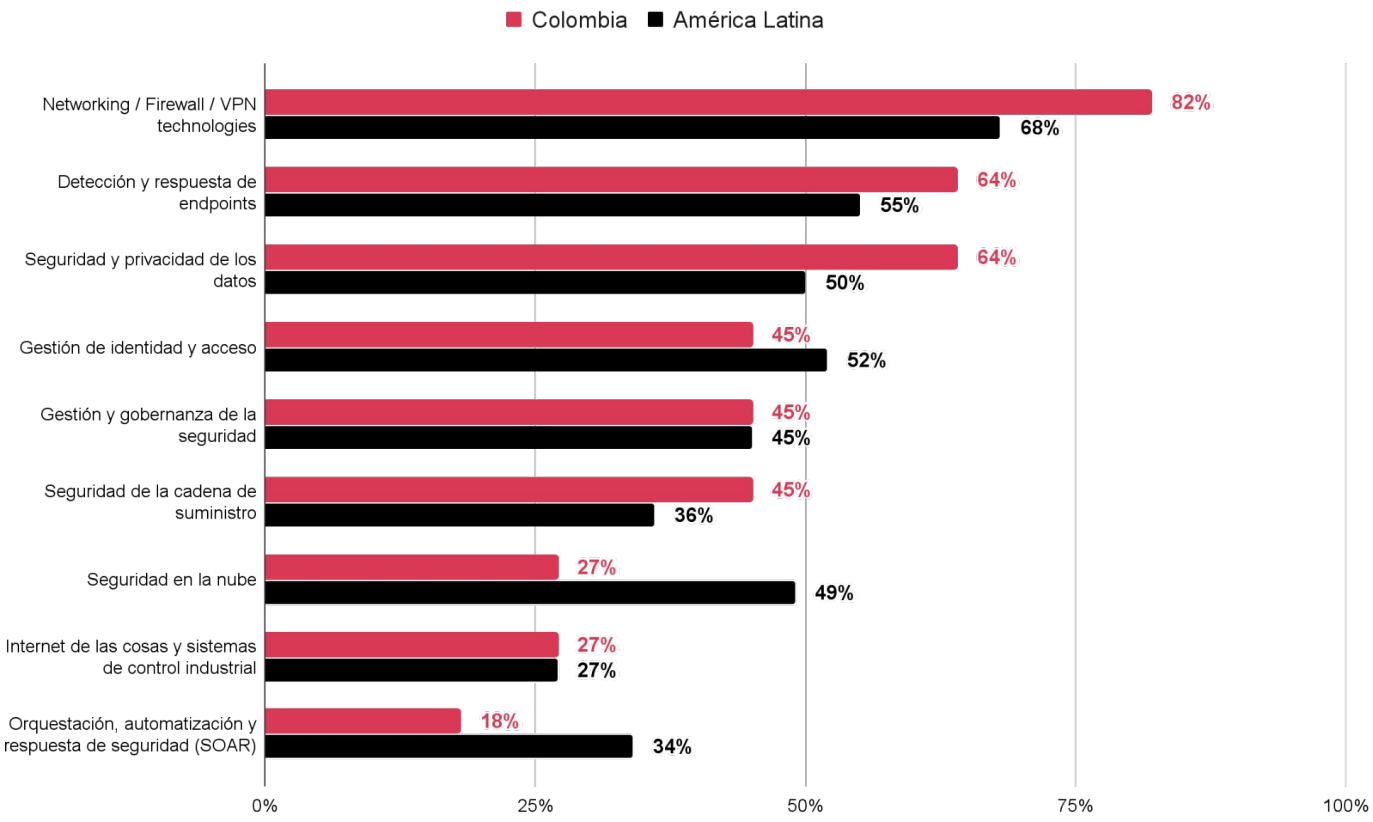
En los resultados de nuestra encuesta del 2024, el 44 % de los participantes a nivel global y el 28 % en Colombia informó que utiliza un conjunto integrado de soluciones de tecnología de ciberseguridad, mientras que el 39 % a nivel global y el 45 % en Colombia planea pasar a un conjunto en los próximos dos años. Esto quiere decir que casi una quinta parte dice que tiene demasiadas soluciones y necesita consolidarlas.

Una sobreabundancia de soluciones puntuales puede ser uno de los motivos por los que solo el 5 % de los encuestados de TI y tecnología dice estar "muy satisfecho" con las capacidades tecnológicas de sus soluciones de ciberseguridad en las ocho áreas clave. El software que no funciona en conjunto puede obstaculizar el rendimiento, requerir más tiempo para administrarlo e impedir la visión general que es esencial para gestionar el riesgo.

Los que ya han sido afectados lo saben. Los encuestados que han sufrido incidentes relacionados con pérdida de datos por valor de 1 millón de dólares o más en los últimos tres años tienen más probabilidades de reconocer que tienen demasiadas soluciones de ciberseguridad y necesitan integrarlas. Por otro lado, las organizaciones que utilizan conjuntos de soluciones cibernéticas integradas cuentan con mayores capacidades de evitar los grandes y costosos incidentes.

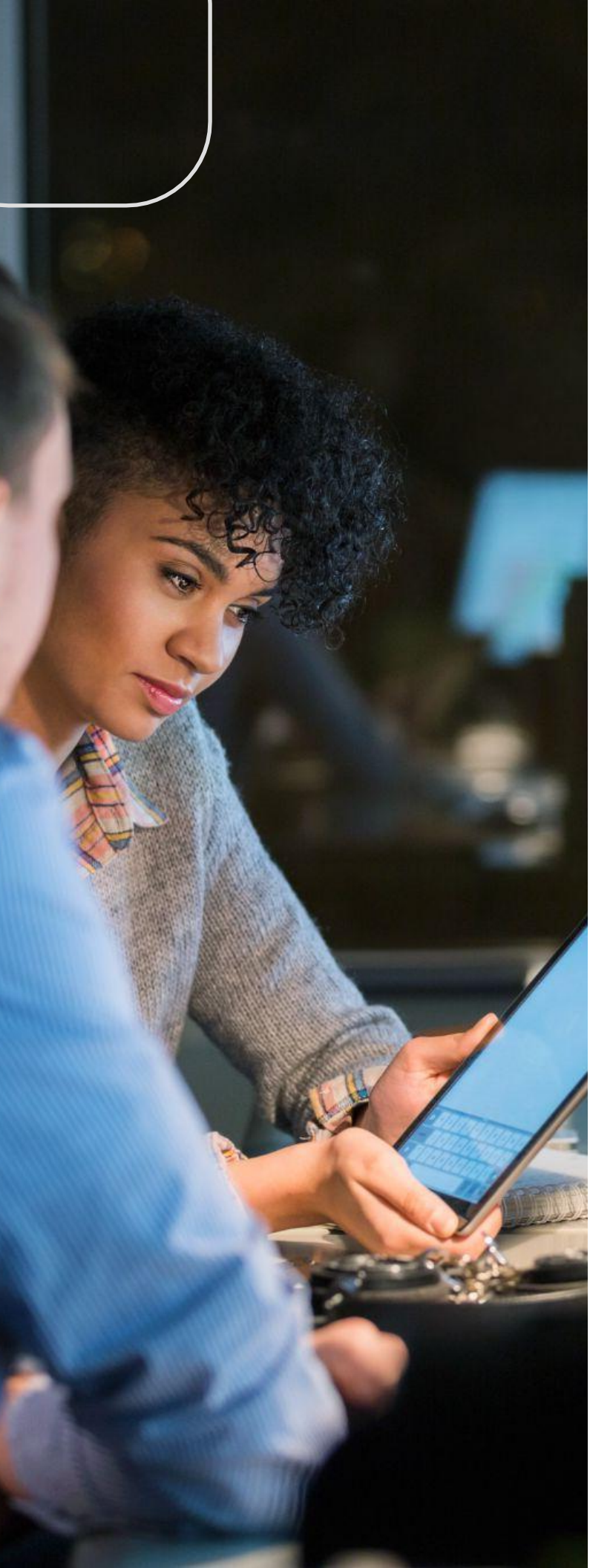


Gráfica 5: Baja satisfacción en capacidades de ciberseguridad clave en Colombia y América Latina



Pregunta: ¿Qué tan satisfecho estás con las capacidades de ciberseguridad de tu organización en las siguientes áreas?
Se muestran solo las respuesta “Muy satisfecho y satisfecho”
Fuente: Global Digital Trust Insights de 2024.

Sin embargo, existen retos importantes frente al control de los gastos. Más de la mitad de los encuestados (79 % a nivel global y 61 % en Colombia) dicen que aumentarán sus gastos de ciberseguridad en 2024, especialmente las grandes organizaciones. Quienes planean aumentos presupuestarios mayores (de más del 15 %) tienden a ser empresas con ingresos de 50 mil millones de dólares o más, o empresas que hacen parte de la industria de la tecnología, medios y telecomunicaciones o aquellas que proyectan un mayor crecimiento de ingresos en el próximo año.



Las empresas en Colombia planean aumentar su inversión en las siguientes áreas:

1. Servicios de seguridad gestionados (57 %).
2. Gestión de identidades y acceso (50 %).
3. Seguridad de aplicaciones, seguridad de *endpoints* y dispositivos móviles (29 %).

A nivel mundial, las inversiones en ciberseguridad representan una proporción mayor del total del presupuesto de TI, OT y automatización. Estamos viendo un aumento medio general al 14 % en 2024, frente al 11 % de 2023.

El desafío de la alta dirección no es la falta de herramientas o de inversión. Más bien, se trata de descubrir cómo su organización puede aprovechar en mayor medida los beneficios de sus inversiones: ¿Su arquitectura de TI es demasiado compleja para protegerla adecuadamente?, ¿está facilitando que los actores de amenazas encuentren brechas en su defensa?

Seguridad en la nube: Protegiendo el futuro de forma coordinada

El uso de la nube o red de servidores siempre ha tenido que ver con la innovación empresarial: permitir a los desarrolladores colaborar sin importar en qué parte del mundo se encuentren; adoptar formas de trabajo nuevas y más flexibles; inventar nuevos modelos de negocio; conectar tecnologías para ayudar a operar mejor el negocio; y brindar un servicio superior a clientes y aliados.

La rápida implementación de la nube ha resultado en la migración de información que solía residir en infraestructuras locales *(on premise)* hacia servicios de almacenamiento en la nube. Es así como un 21 % de los ejecutivos colombianos encuestados destacó que su empresa utiliza más de un proveedor en la nube. Los usuarios de la nube híbrida también son los más propensos, en un 36 %, a seleccionarla entre sus tres principales prioridades para las inversiones en seguridad durante el próximo año.

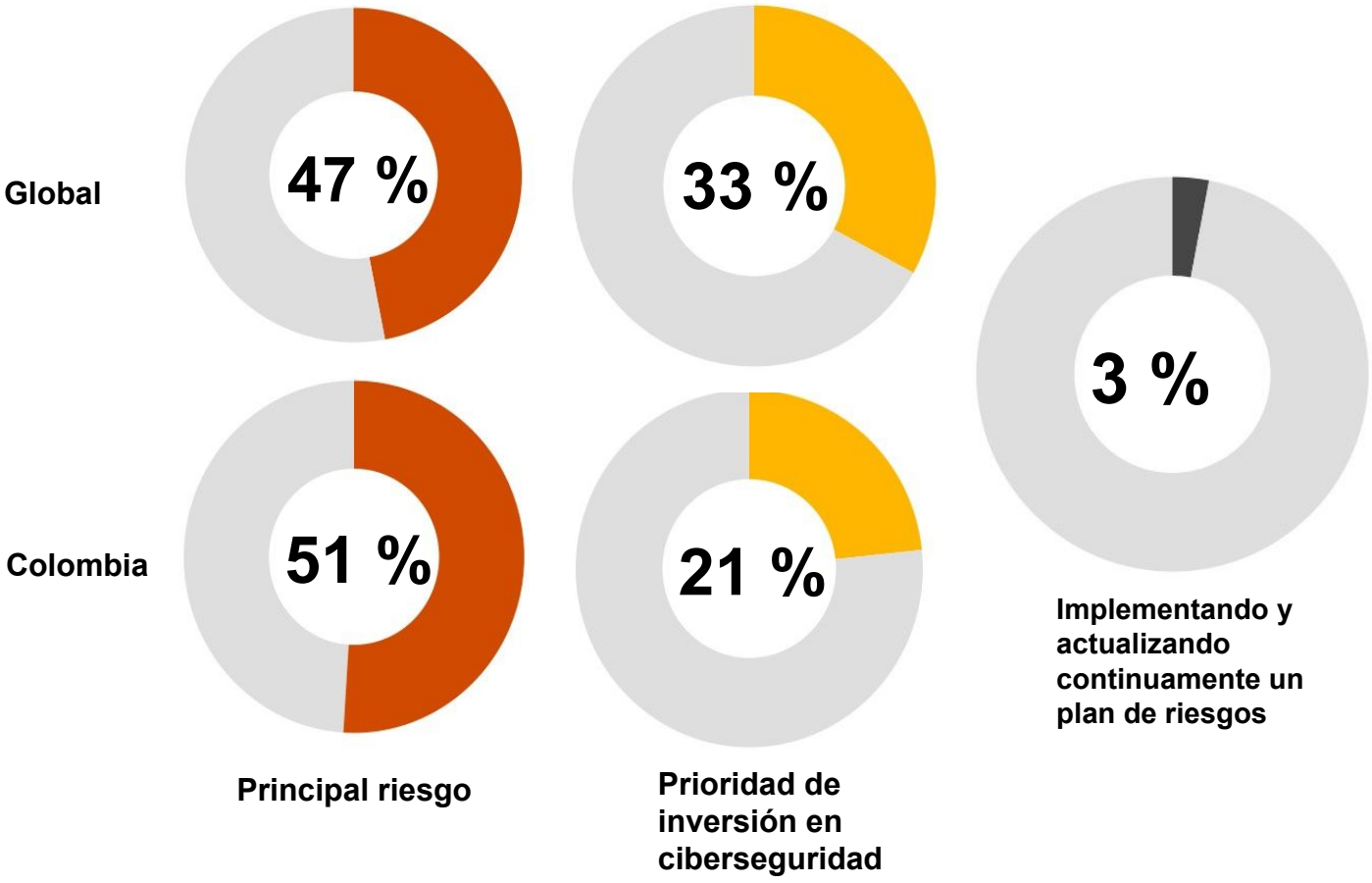
La seguridad en la nube es la preocupación número uno sobre riesgos de ciberseguridad para más de la mitad de los encuestados en Colombia (51 %). Las vías por las cuales los actores malintencionados podrían infiltrarse parecen ser prácticamente ilimitadas. Las organizaciones deben implementar controles exhaustivos: en identidad y acceso, movimiento lateral, cuentas de correo electrónico, portales web, aplicaciones, información patentada, interacciones con clientes, sistemas operativos, dispositivos conectados, y la lista sigue.

Pero casi todas las organizaciones (97 %) tienen brechas en su plan de gestión de riesgos en la nube. Solo el 3 % de las empresas a nivel mundial mantiene planes actualizados que abordan las nueve áreas de seguridad de esta red de servidores. De esta forma, los riesgos asociados a deficiencias regulatorias aún no han sido abordados en un 42 %; el 41 % no tiene planes para afrontar riesgos asociados a la resiliencia de las operaciones; o el 36 % aún no ha abordado el riesgo de terceras partes en la nube.

La situación en Colombia es aún más preocupante: casi el 70 % de las empresas encuestadas no han abordado el riesgo de terceros; más del 60 % no ha creado un plan para mitigar los riesgos de inventario y uso de datos; y casi la mitad de las empresas (51 %) no cuenta con un plan de respaldo y recuperación ante desastres probado frente a las amenazas actuales.

Gráfica 6: Seguridad en la nube

Principal amenaza y mayor inversión, pero brechas en gestión de riesgos



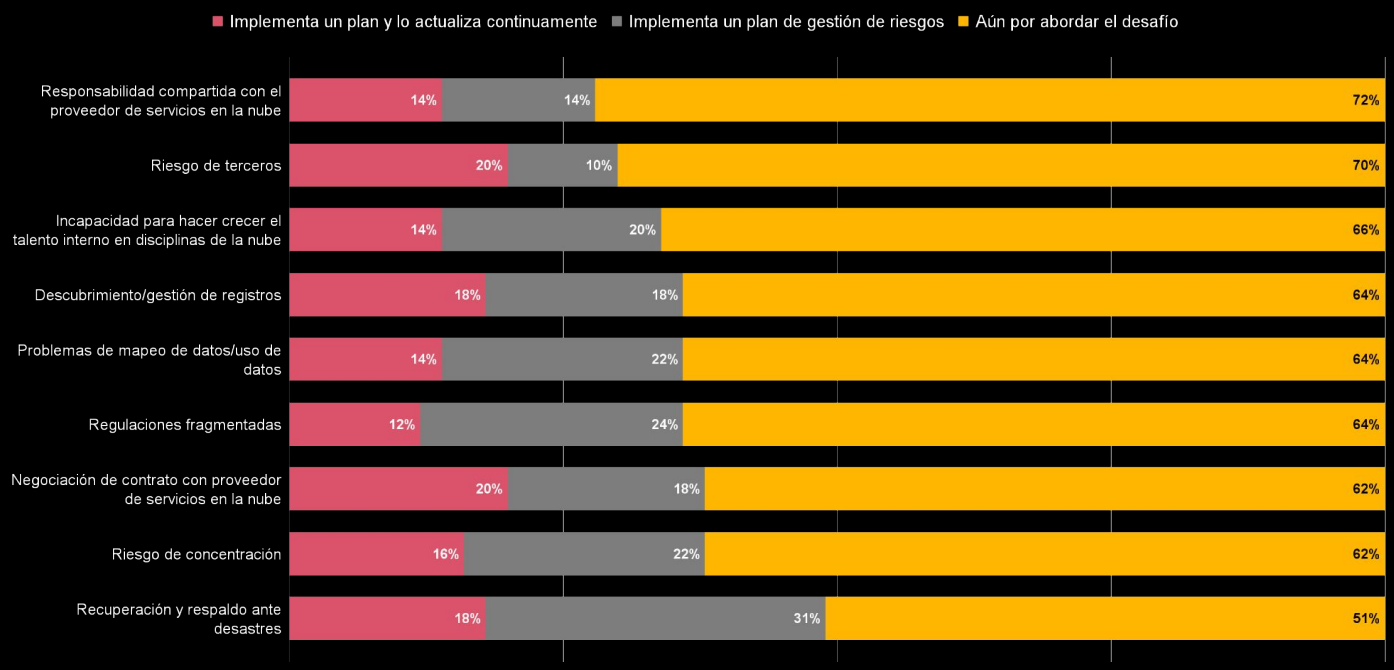
Pregunta: Durante los próximos 12 meses: ¿Cuál de las siguientes amenazas cibernéticas preocupa más a tu organización? ¿Cuál de las siguientes inversiones se prioriza en tu empresa al asignar el presupuesto de ciberseguridad?

Fuente: Global Digital Trust Insights de 2024.

Nota: El texto en 3 % es: Implementado y continuamente actualizando el plan de gestión de riesgos

Gráfica 7: Seguridad en la nube en Colombia

Muchos riesgos de la nube, pocos planes para gestionarlos



Pregunta: ¿En qué medida tu organización ha abordado los siguientes desafíos con su(s) proveedor(es) de servicios en la nube?

Fuente: Global Digital Trust Insights de 2024.

Es importante resaltar que *los guardianes de la confianza digital* son cuatro veces más propensos a actualizar de manera continua sus planes de gestión de riesgos para mitigar los riesgos en la nube. Sin embargo, la mayoría de nuestros encuestados todavía tiene que realizar gran parte de este trabajo crucial para las organizaciones.

El desafío para la alta dirección radica en cómo trabajar en conjunto con sus equipos y proveedores de seguridad en la nube para avanzar en la defensa de los puntos de entrada más importantes a sus sistemas y activos que se encuentran en la red de servidores.

El uso de IA generativa para ciberdefensa en la hoja de ruta de las organizaciones

La IA generativa está creando nuevas oportunidades para las organizaciones y para sus estrategias de ciberseguridad, que ya están analizando los más de 3800 ejecutivos que participaron en nuestra encuesta este año. Sin embargo, la adopción de IA debe ir acompañada de gobierno, responsabilidad y gestión del riesgo.

- Según nuestro estudio, siete de cada diez altos directivos (69 %) afirman que su compañía tiene previsto utilizar la IA generativa para sus estrategias de ciberseguridad en los próximos 12 meses.

- Es más que probable que el uso de la IA generativa provoque otro repunte de las ciberamenazas y facilite ataques a gran escala. Los CISO y los director de tecnologías de la información (CIO, por sus siglas en inglés) no deben perder de vista esta opinión: el 52 % de los entrevistados en el estudio prevé que el uso de la IA generativa provoque ciberataques de alto impacto en los próximos 12 meses.

- Las compañías necesitan diseñar un gobierno de inteligencia artificial sólido y adelantarse a los riesgos que podrían derivarse del uso de la IA generativa. En este sentido, tan solo el 19 % de los directivos encuestados manifiesta no sentirse cómodo con el uso de herramientas de IA generativa, antes de haber establecido las políticas de gobierno y control correspondientes.

Casi siete de cada diez encuestados afirman que su compañía utilizará la IA generativa para su ciberdefensa. Algunas plataformas están ofreciendo licencias para sus modelos grandes de lenguaje (LLM, por sus siglas en inglés) junto con sus herramientas de ciberseguridad para la gestión de la seguridad, la respuesta a incidentes y la generación de informes en este ámbito. Incluso sin recurrir a las herramientas de sus proveedores, algunas compañías han estado utilizando IA generativa para identificar y gestionar intentos de *phishing*.

Imagen 3: IA generativa para la ciberdefensa

IA generativa para la ciberdefensa, oportunidad para Colombia

Pregunta: ¿En qué medida estás de acuerdo o en desacuerdo con las siguientes afirmaciones sobre la IA generativa?
Fuente: Global Digital Trust Insights de 2024.

Las plataformas están otorgando licencias para sus modelos grandes de lenguaje (LLM) junto con sus soluciones de tecnología cibernética. Microsoft Security Copilot tiene la intención de proporcionar funciones de IA generativa para la gestión de seguridad, la respuesta a incidentes y la generación de informes de seguridad. Por su parte, Google anunció Security AI Workbench para casos de uso similares.

Actualmente, estas son las áreas más prometedoras para el uso de IA generativa en ciberseguridad y defensa:

Detección y análisis de amenazas: La IA generativa puede ser invaluable para detectar proactivamente vulnerabilidades, evaluar rápidamente su alcance (qué está en riesgo, qué está comprometido y cuáles son los daños), y luego presentar opciones probadas y verdaderas para la defensa y remediación. Por otro lado, puede también identificar patrones, anomalías e indicadores de compromiso que eluden los sistemas tradicionales de detección basados en firmas.

Reporte de incidentes y riesgos de ciberseguridad: La IA generativa también podría simplificar mucho la notificación de incidentes y riesgos de ciberseguridad. Con la ayuda del procesamiento del lenguaje natural (NLP), puede convertir datos técnicos en contenido conciso que las personas sin conocimientos técnicos puedan entender. Puede ayudar con informes de respuesta a incidentes, inteligencia sobre amenazas, evaluaciones de riesgos, auditorías y cumplimiento normativo. Además, puede presentar sus recomendaciones en términos que cualquiera pueda entender, incluso traduciendo gráficos confusos en texto simple.

Respuesta y mitigación de amenazas avanzadas: Las capacidades de automatización de la IA van más allá de la detección, facilitando respuestas automáticas a diversas amenazas. Al extraer grandes cantidades de datos de seguridad y correlacionar información, la IA genera de forma autónoma respuestas informadas contra amenazas cibernéticas alineadas con registros técnicos, patrones de tráfico de red e inteligencia de amenazas.

Inteligencia sobre amenazas y análisis predictivo: La inteligencia artificial permite combinar información de los activos críticos con las evaluaciones de exposición a amenazas para predecir las áreas más vulnerables y de mayor exposición. Esta conciencia situacional soporta una mayor precisión en la evaluación de riesgos, la búsqueda proactiva de amenazas y la respuesta oportuna a incidentes, fortaleciendo las capacidades de ciberseguridad de la organización.

Controles adaptativos: Proteger la nube y la cadena de suministro de software requiere actualizaciones constantes en las políticas y controles de seguridad, una tarea de enormes proporciones en la actualidad. Los algoritmos de aprendizaje automático y las herramientas de la IA generativa pronto podrían recomendar, validar y redactar políticas de seguridad y automatizar controles que se adapten al perfil de amenazas, las tecnologías y los objetivos comerciales de una organización.

El desafío de la alta dirección es cómo aprovechar las capacidades de la inteligencia artificial sin generar nuevos riesgos y hacerlo de forma ética y responsable.

Regulaciones: Garantizando un entorno seguro para el desarrollo y crecimiento

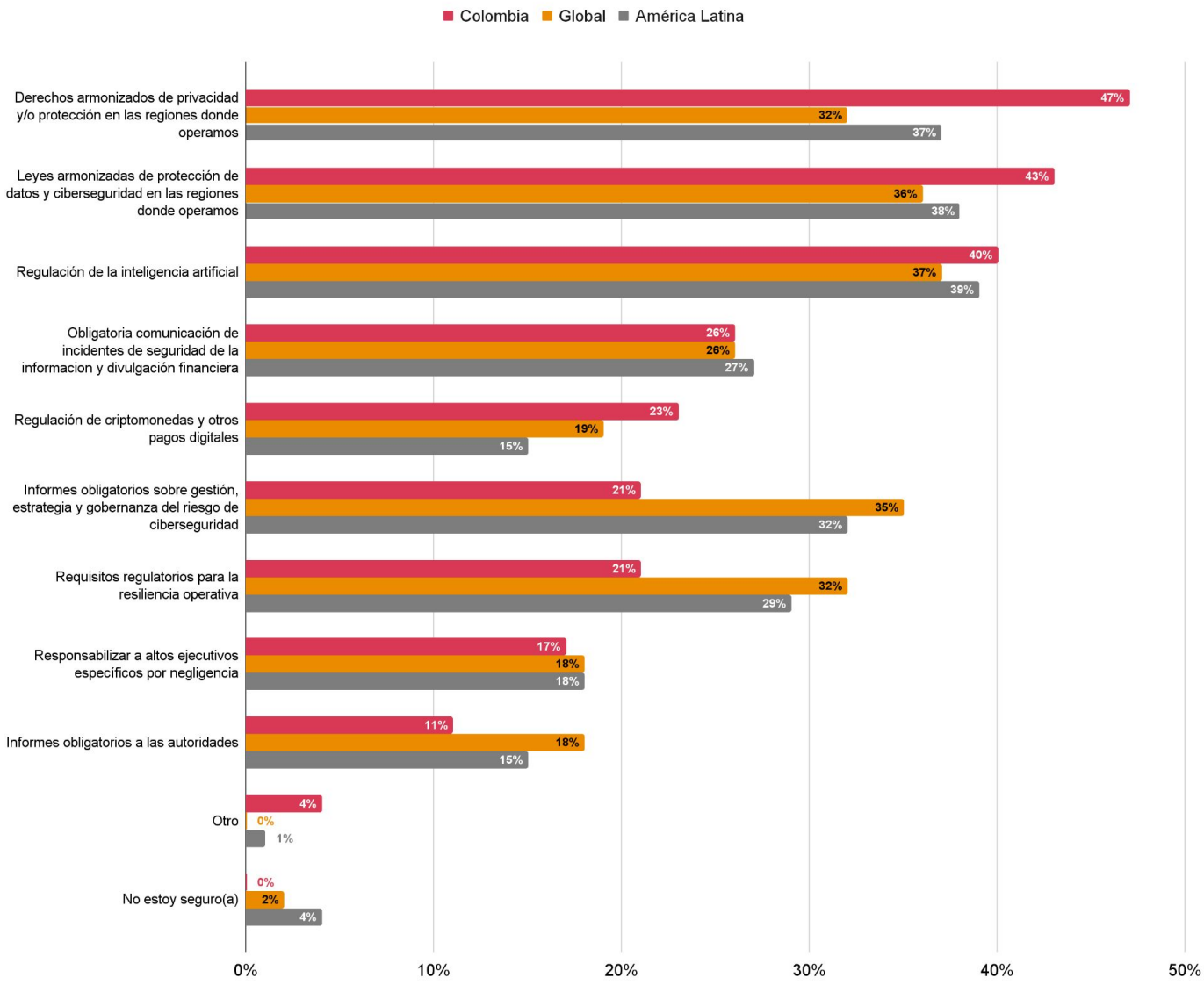
Una opinión común es que las nuevas reglas y regulaciones obstaculizan los ingresos, pero para un tercio de nuestros encuestados su visión es diferente: los controles que definen los reguladores pueden dar a las empresas mayor confianza para explorar, experimentar, inventar y competir. Navegar por los requisitos regulatorios puede convertirse en una ventaja competitiva para las empresas líderes.

Alrededor de un tercio de los encuestados de este año coincide en que cuatro tipos de regulación serán los más importantes para asegurar el crecimiento futuro de su organización: regulación de la IA (37 %), armonización de las leyes de ciberseguridad y de protección de datos (36 %), informes obligatorios de ciberseguridad, gestión de riesgos, estrategia y gobernanza (35 %), y requisitos de resiliencia operativa (32 %).

La transparencia es el tono regulatorio que se hará más fuerte en todo el mundo. Las nuevas reglas de la SEC exigen la divulgación pública de los incidentes de ciberseguridad que se considere que tienen un efecto material potencial en los inversionistas. La Ley de Mercados Digitales y la Ley de Servicios Digitales exigen transparencia en las prácticas de datos y la toma de decisiones algorítmicas. Además, se vislumbran regulaciones que rigen la IA, incluida una ley de IA de la Unión Europea (UE) en proceso y una regulación de IA generativa.

Gráfica 8: Regulaciones que podrían cambiar la ciberseguridad

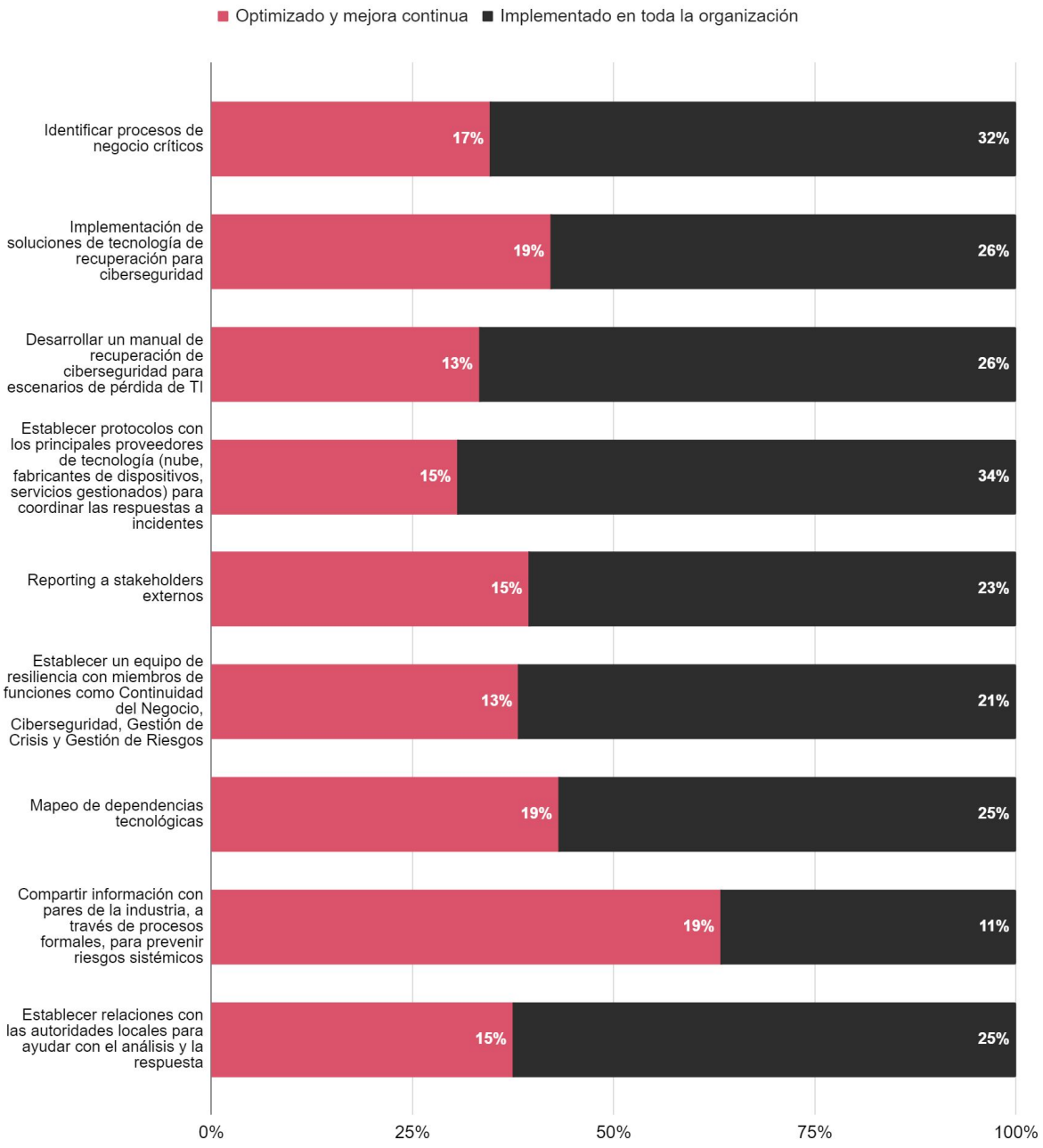
Objetivo y principios regulatorios con mayor impacto en el crecimiento futuro de los ingresos de la organización



Pregunta: ¿Cuál de los siguientes objetivos y principios regulatorios tendrá el mayor impacto en la capacidad de tu organización para asegurar el crecimiento futuro de los ingresos?
Fuente: Global Digital Trust Insights de 2024.

La resiliencia operativa es otro tema importante. Los reguladores saben que es un gran desafío abordar los riesgos complejos e interrelacionados, de la manera en que lo hacen muchos equipos de alto nivel: 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 Operacional Digital, insistirán cada vez más en la resiliencia integrada con elementos centrales que hagan que una organización sea adaptable, flexible y más fuerte después de cada evento disruptivo.

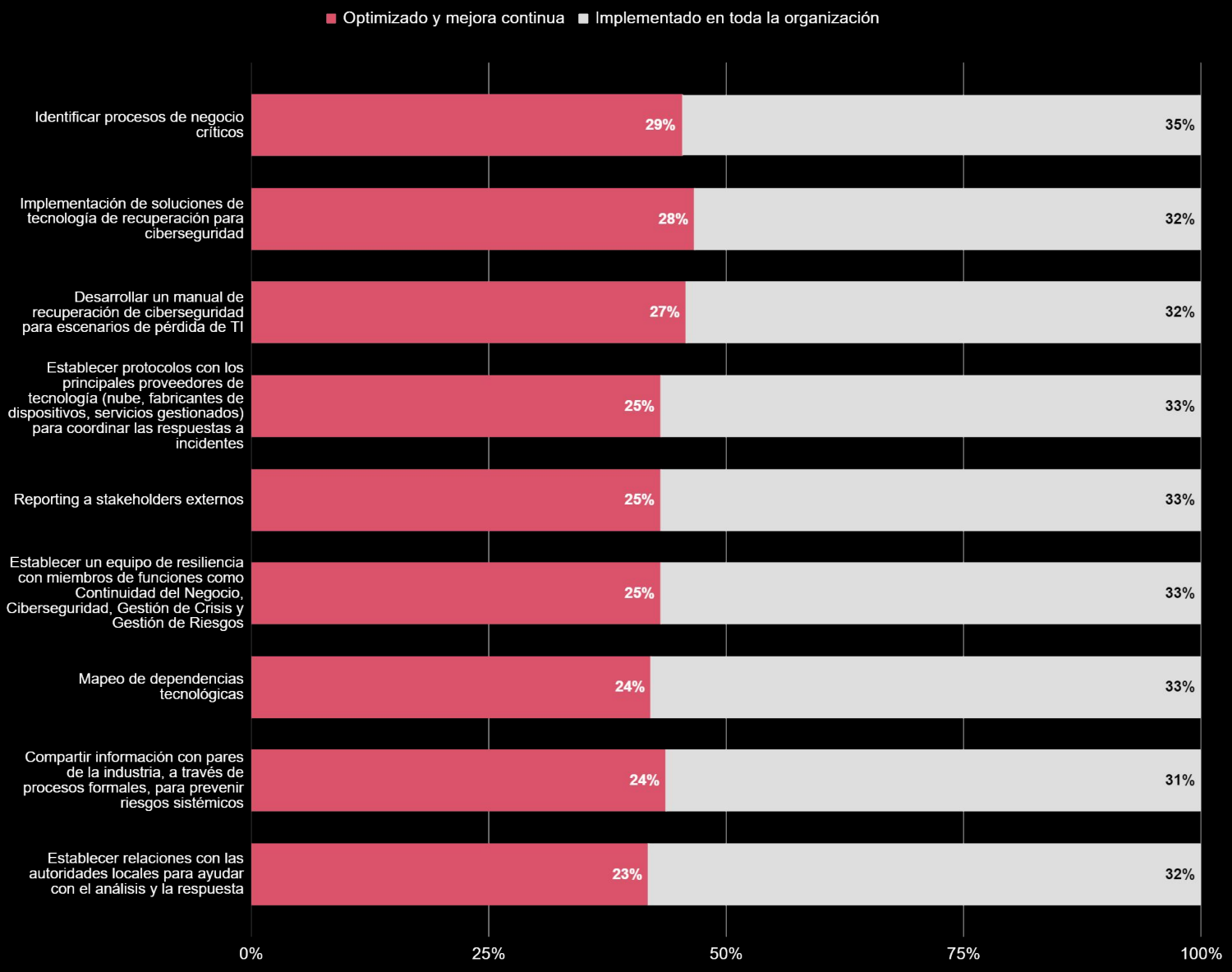
Gráfica 9: El lento avance en la ciber resiliencia en Colombia



Pregunta: ¿En qué medida tu organización está implementando o planea implementar las siguientes acciones de ciber resiliencia?

Fuente: Global Digital Trust Insights de 2024.

Gráfica 10: El lento avance en la ciber resiliencia a nivel global



Pregunta: ¿En qué medida tu organización está implementando o planea implementar las siguientes acciones de ciber resiliencia?
Fuente: Global Digital Trust Insights de 2024.

Hasta tres cuartas partes esperan que el cumplimiento de estas regulaciones requiera importantes desembolsos de dinero y tiempo. Incurrir en altos costos e impactos en los ingresos puede ser evitable si las empresas se involucran desde el principio y con frecuencia en los procesos regulatorios, reuniéndose con las autoridades, por ejemplo, participando en comentarios públicos e incluso, sentándose en la mesa con los reguladores para ayudar a elaborar o influir en las directivas propuestas.

El desafío de la alta dirección es este: En medio de la incertidumbre regulatoria, ¿puede darle a su organización el espacio para innovar, manteniendo al mismo tiempo la ciberseguridad y la privacidad desde el diseño? ¿Cómo se puede convertir este nuevo entorno regulatorio en una fuente de ventaja competitiva?

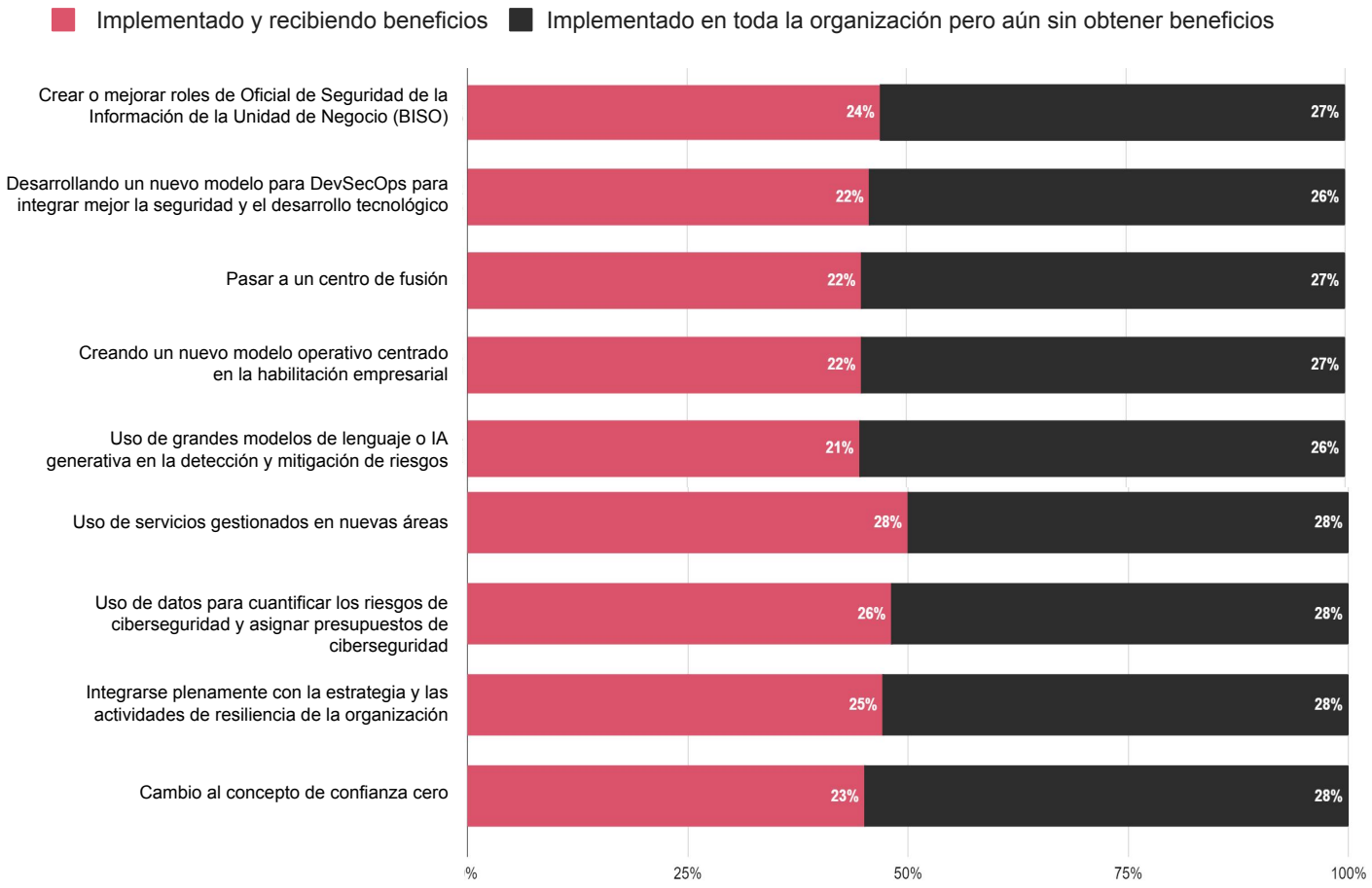
Desafiando lo convencional en Ciberseguridad: El manual de estrategia de la alta dirección para 2024

Iniciativas fragmentadas, una gama cada vez mayor de complejidades tecnológicas, un programa de gestión de riesgos que, con sus lagunas, es arriesgado en sí mismo; y transformaciones y proyectos que no producen los resultados esperados. Estos son algunos de los obstáculos que impiden que la ciberseguridad genere la confianza que las organizaciones necesitan.

En nuestros resultados del 2023 identificamos los desafíos críticos que los ejecutivos de alto nivel deben abordar juntos de forma coordinada para responder a las amenazas de ciberseguridad. Estos siguen siendo vigentes y relevantes.

Gráfica 11: Retos de la ciberseguridad, panorama global

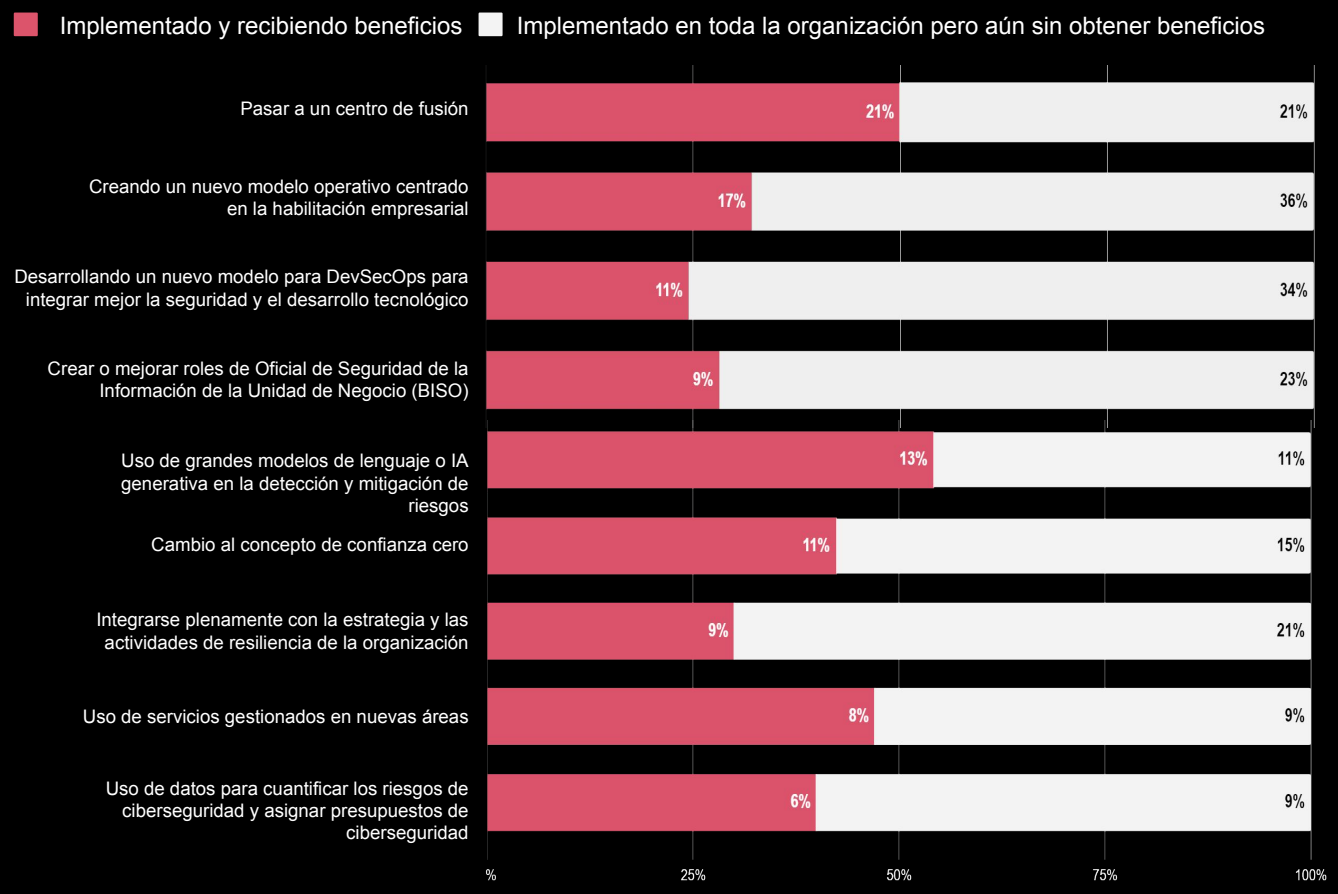
Desafíos críticos que los ejecutivos de la C-suite deben abordar juntos, como socios



Pregunta: ¿En qué medida tu organización está implementando o planea implementar las siguientes iniciativas de ciberseguridad?
Fuente: Global Digital Trust Insights de 2024.
Nota: Estado de la implementación de iniciativas de ciberseguridad.

Gráfica 12: Retos de la ciberseguridad en Colombia

Desafíos críticos que los ejecutivos de la C-suite deben abordar juntos, como socios



Pregunta: ¿En qué medida tu organización está implementando o planea implementar las siguientes iniciativas de ciberseguridad?
Fuente: Global Digital Trust Insights de 2024.
Nota: Estado de la implementación de iniciativas de ciberseguridad

En 2024 estamos elevando el desafío: ¿Estás preparado como líder de la alta dirección para romper con lo convencional y apoyar los movimientos estratégicos que necesita tu organización? ¿O dar ese salto que finalmente podría eliminar los obstáculos que impiden que tu empresa alcance los objetivos? Vemos que algunas empresas ya eligen sus mejores apuestas. El abanico de opciones es amplio ¿Qué es lo correcto para tu organización?

Habla un nuevo idioma

CISO, CFO y Asesor general.

Ponerte en el centro de la innovación significa reunirte con tus equipos de liderazgo y ayudarlos a superar la intimidación que pueden sentir con respecto a lo que haces. El uso de términos especializados como indicadores de compromiso, superficie de ataque e incluso confianza cero puede desconcertar a quienes no pertenecen a la profesión.

Atrévete a hablar de ciberseguridad en un lenguaje empresarial, tecnológico, financiero y cotidiano. Habla con tus clientes, inversionistas y socios comerciales a través de informes de seguridad anuales, de manera que estos generen confianza, informen y atraigan. El uso de un lenguaje común puede ayudar a los ejecutivos a lidiar con las tensiones y el caos que inevitablemente ocurren en el centro de la innovación.

Prueba nuevas formas de gestionar el riesgo de ciberseguridad

CISO, CRO, IA, CCO y COO.

Utiliza enfoques más precisos para el modelado de riesgos de ciberseguridad, considerando las amenazas específicas de tu sector, y la visión y estrategia de tu empresa. Crea incentivos de desempeño vinculados a la gestión de riesgos para cada trabajador de la empresa para construir una cultura de riesgo. Crea nuevas formas de identificar y superar las debilidades, utilizando, por ejemplo, programas de recompensas para identificación de vulnerabilidades que incentiven la investigación y la conciencia frente a la seguridad de forma individual. Finalmente, adquiere y comienza a utilizar una solución de gestión de identidades que integre tus iniciativas en la nube para asegurar tus objetivos de expansión empresarial.

Lenguaje de confianza

CISO, CIO y GC.

Habla el lenguaje de la confianza, no solo el del cumplimiento normativo. Involúcrate con frecuencia para tener la mejor oportunidad de influir en el nuevo gobierno y garantizar que las medidas que se adopten impulsen, no obstaculicen, el éxito del negocio.

La inteligencia artificial (IA), el metaverso, las criptomonedas, la privacidad: estos temas regulatorios podrían beneficiarse de tu experiencia y conocimientos. Recuerda, los reguladores pueden sentirse tan desconcertados como cualquiera por el funcionamiento de la ciberseguridad y la tecnología.

Libera a tus equipos para el pensamiento creativo (automatización, GenAI y servicios gestionados)
CISO, CIO, CTO, CRO y COO.

Hacer seguimiento las 24 horas del día es uno de los beneficios de la automatización, la IA generativa y los servicios gestionados. Realizar tareas operativas para que tus equipos no tengan que hacerlo es otro de ellos. Liberados de las tareas tediosas, tu equipo puede encontrar tiempo y espacio para reflexionar sobre nuevas amenazas cibernéticas y crear nuevas formas de frustrar las amenazas en evolución.

Bienvenida la ciberseguridad a la sala de juntas
CISO, Junta directiva y CEO.

La ciberseguridad encabeza la identificación de riesgos en la mayoría de empresas y encuestas dirigidas a altos ejecutivos ¿Pero es este un tema recurrente en la sala de juntas de tu organización? ¿Estás obteniendo información de calidad no solamente sobre riesgos y controles cibernéticos, sino también sobre cómo las principales iniciativas estratégicas de ciberseguridad están impulsando el crecimiento del negocio y de los ingresos? La seguridad proporciona la base para todo lo que hace la organización: finanzas, desarrollo, personal, tecnología y otras áreas del negocio que probablemente estén en el orden del día cada vez que te reúnes.

Piensa como el dueño del negocio
CISO y CEO.

La transformación empresarial y la transformación en ciberseguridad son igualmente críticas para la organización. El CISO y el CEO juntos ahora deben adoptar la ciberseguridad como un esfuerzo de toda la empresa, poniéndose en el lugar del propietario de la misma ¿No querrían que todos los aspectos (registros financieros, investigaciones patentadas, desarrollo de aplicaciones y datos de clientes) estuvieran protegidos contra accesos o usos no autorizados? ¿No querrían salvaguardar su marca? ¿No debería la ciberseguridad estimular innovaciones que ahorren dinero y ayuden a crecer el negocio? Esta es la razón de ser de la ciberseguridad.

Acerca de la encuesta

Global Digital Trust Insights de 2024 es una encuesta aplicada a 3876 ejecutivos de negocios, tecnología y ciberseguridad (CEO, Directores corporativos, CFO, CISO, CIO y funcionarios de C-Suite), realizada entre mayo y julio de 2023.

Cuatro de cada 10 ejecutivos están en grandes empresas con ingresos de 5 mil millones de dólares o más. Es importante destacar que el 30 % pertenece a empresas con ingresos de 10.000 millones de dólares o más.

Los encuestados operan en una variedad de industrias, incluida Productos industriales (20 %), Servicios financieros (20 %), Tecnología, Medios, Telecomunicaciones (19 %), Retail y consumo (17 %), Energía, Servicios públicos y Recursos (11 %), Salud (9 %) y Gobierno y servicios públicos (3%).

Los encuestados se encuentran en 71 países. El desglose regional es Europa Occidental (32 %), América del Norte (28 %), Asia Pacífico (18 %), América Latina (10 %), Europa del Este (5 %), África (4 %) y Medio Oriente (3 %).

La Encuesta Global Digital Trust Insights se conocía como encuesta sobre el estado global de la seguridad de la información (GSISS). En su vigésimo sexto año, es la encuesta anual de mayor duración sobre tendencias de ciberseguridad, también es la encuesta más grande en la industria de la ciberseguridad y la única que atrae la participación de altos ejecutivos de negocios, no solo ejecutivos de ciberseguridad y tecnología.

Contactos

Mauricio Arias
Socio de Consultoría en Tecnología, PwC Colombia.

Mauricio Sanchez
Gerente de Ciberseguridad y Privacidad, PwC Colombia.

Carol Sthefanny Hernández
Gerente de Ciberseguridad y Privacidad, PwC Colombia.

pwc

www.pwc.com/co