pwc

Los líderes corporativos unidos para lograr la ciberseguridad

Conclusiones del Global Digital Trust Insights de 2023

Es un mundo nuevo y audaz en los negocios

Impulsados por eventos que nadie podría haber previsto, los líderes en los últimos años han empujado a sus empresas, y a ellos mismos, más allá de su zona de confort: fuera de la oficina en lugares de trabajo remotos, en la nube, a lo largo de cadenas de suministro que son casi completamente digitales. Por ende, con cada nuevo desafío han llegado nuevos riesgos de ciberseguridad.

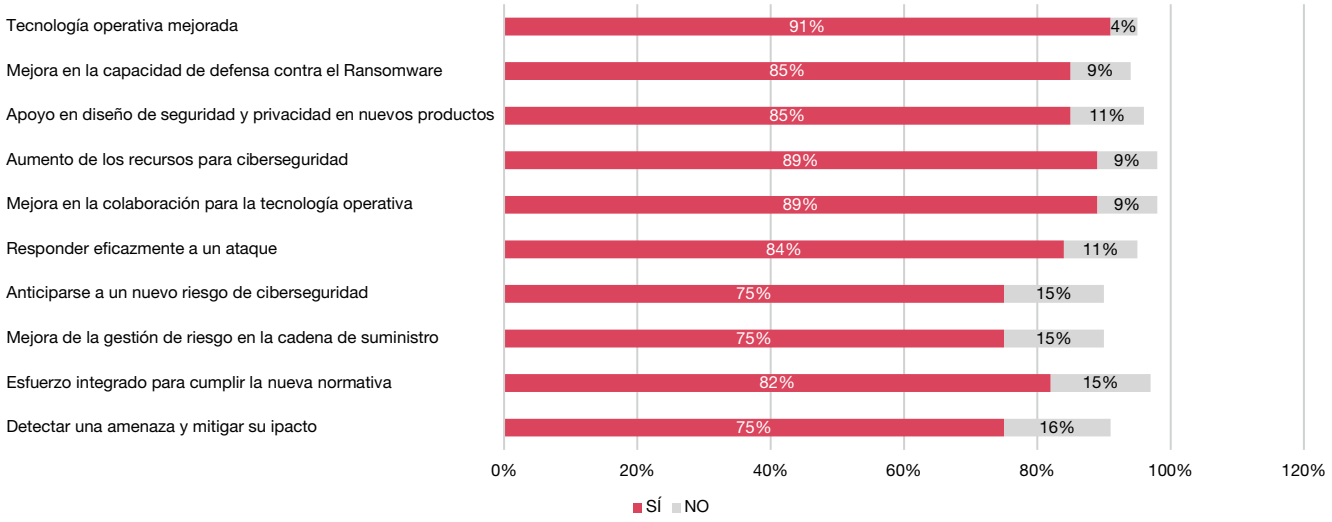
La buena noticia:

Los CISO (Chief Information Security Officer) y los equipos de ciberseguridad han aceptado el desafío, y varios ejecutivos del C-suite se han unido a ellos, al ser conscientes de que sus iniciativas han aumentado la exposición a riesgos de ciberseguridad en sus organizaciones.

Avances en ciberseguridad desde 2020

Más del 75% de los ejecutivos empresariales y de tecnología, encuestados en Colombia, identificaron mejoras en la ciberseguridad de sus empresas en el último año, gracias a las inversiones y a la colaboración con el C-suite. Más de una cuarta parte (26%) informó que han progresado en las 10 áreas que se identificaron como críticas para la madurez en ciberseguridad.

Gráfica 1: Acciones de mejora que han implementado las empresas en los últimos 12 meses para mejorar la ciberseguridad



Fuente: Digital Trust Insights 2023 - Capítulo Colombia
P7: Indique si el equipo de ciberseguridad de su organización ha realizado lo siguiente en los últimos 12 meses.
Nota: Los resultados no suman 100% porque solo se tomaron en cuenta las respuestas “Sí” y “no”.

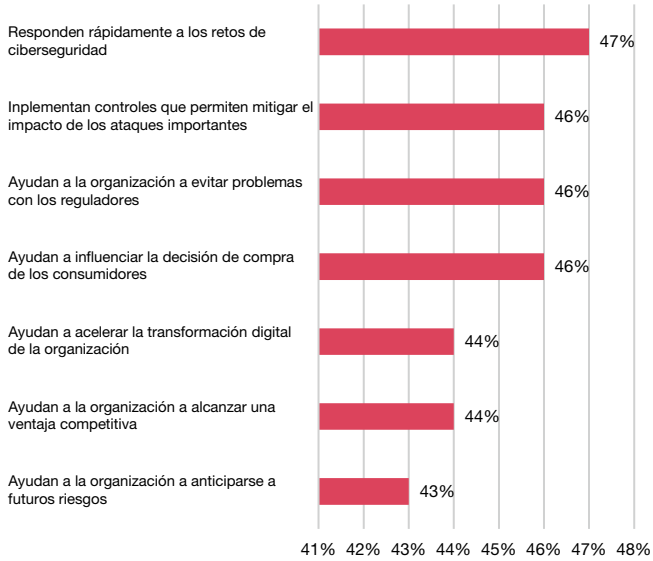
Entre quienes vieron mejoras en las 10 áreas clave:

- Los CEO (Chief Executive Officer) tienen 3 veces más probabilidades de decir que sus CISO están brindando resultados excepcionales en estrategias orientadas a responder más rápido a las amenazas y anticipar futuros riesgos cibernéticos. Casi el 8% mencionó que el CISO lo está haciendo en todas las áreas.
- Los CRO/COO (Chief Risk Officer/Chief Operations officer) tienen el doble de probabilidades de calificar como excepcionales sus programas de ciberseguridad y de privacidad.
- Los CMO/CDO/CPO (Chief Marketing Officer/Chief Data Officer/Chief Product Officer) tienen 2,5 veces más probabilidades de aceptar que sus programas de ciberseguridad y de privacidad son valiosos para la organización. Su mayor beneficio: capacidad de fomentar la confianza en el consumidor.

Gráfica 2: ¿Cómo los CISO están cumpliendo de forma excepcional con las expectativas del negocio?

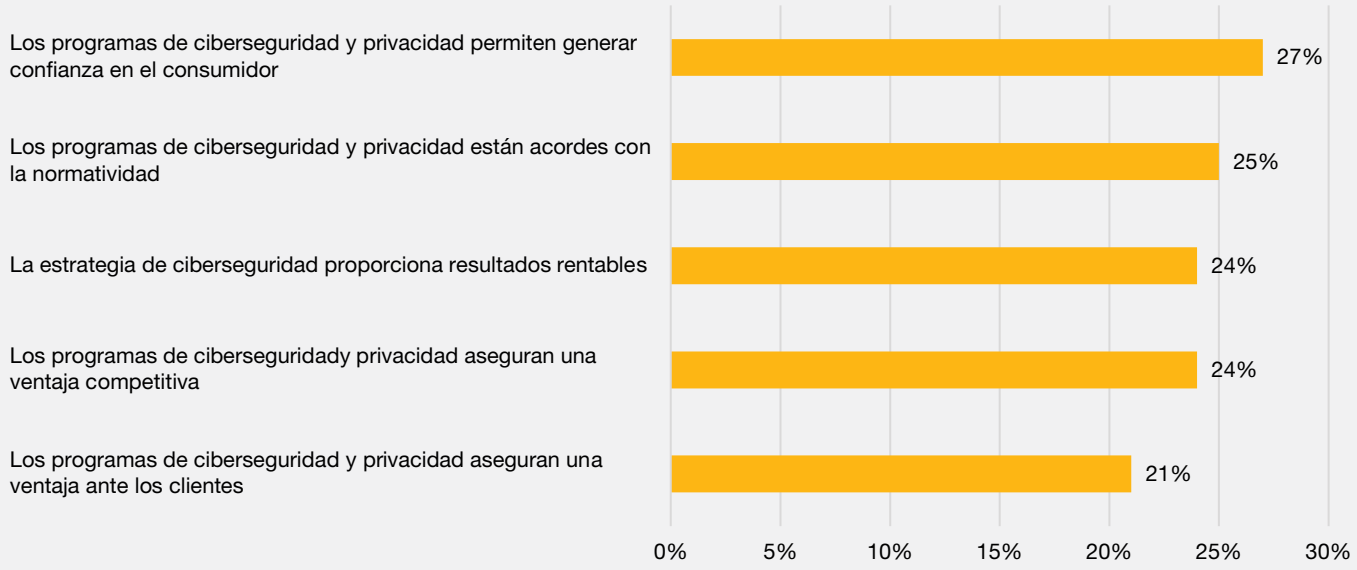
Fuente: Digital Trust Insights 2023

Gráfica 3: ¿Cómo los programas de ciberseguridad y privacidad están cumpliendo de forma excepcional con las expectativas del negocio?



Fuente: Digital Trust Insights 2023

Gráfica 4: ¿Qué tipo de valor están generando los programas y los equipos de ciberseguridad en las empresas?



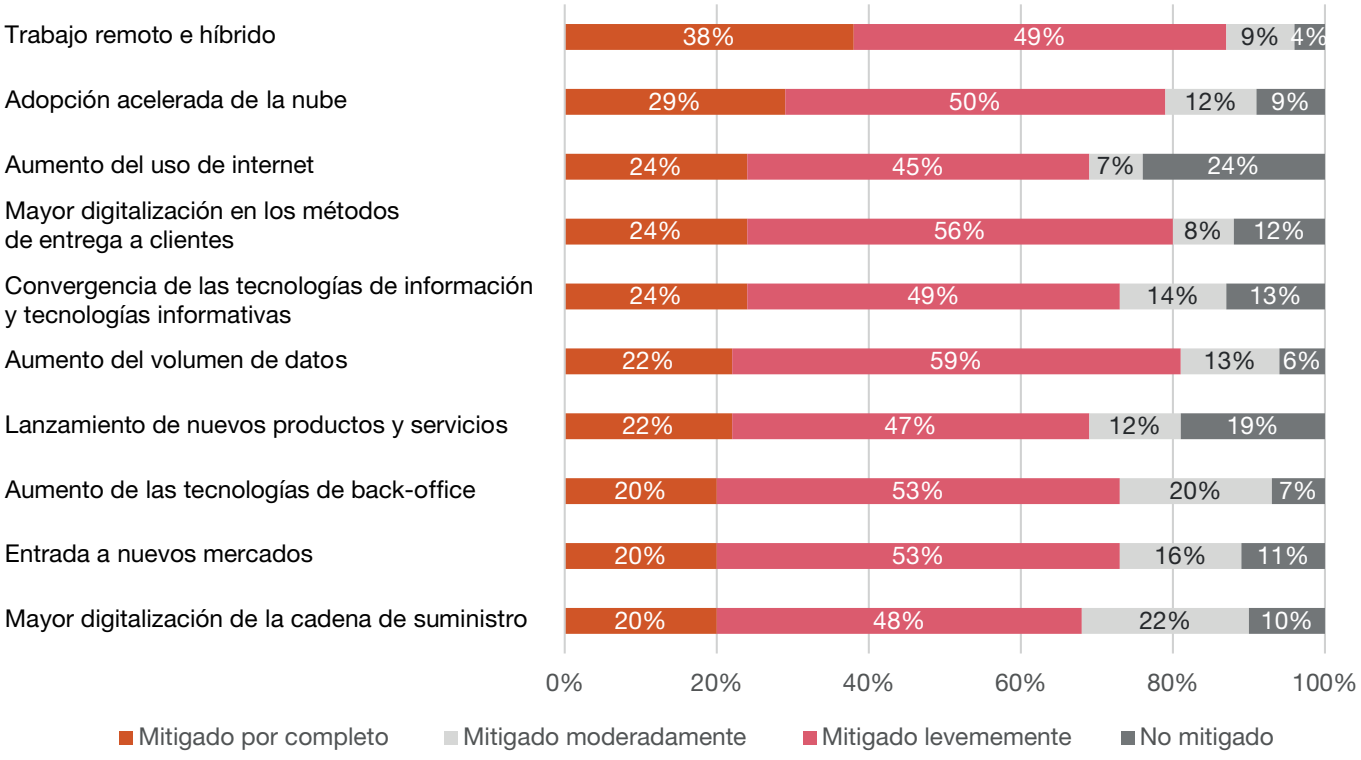
Fuente: Digital Trust Insights 2023

Los desafíos cambian rápidamente

La digitalización hace que la seguridad sea un asunto de todos. El futuro promete sistemas más conectados y con una cantidad de datos exponencialmente más alta, así como adversarios más organizados. Con los riesgos de ciberseguridad en constante expansión, los líderes empresariales tienen mucho más trabajo por hacer, en un entorno económico cada vez más difícil.

Menos del 40% de los encuestados en Colombia dice que han mitigado por completo los riesgos en los que incurren como producto de sus desafíos e iniciativas digitales. El trabajo remoto (38%) y el cambio a la nube (29%) han sido los riesgos que más atraen la atención. Es mucho más probable que las organizaciones más grandes hayan logrado mejores resultados.

Gráfica 5: ¿En qué medida las empresas han mitigado los 10 riesgos más importantes relacionados con ciberseguridad?

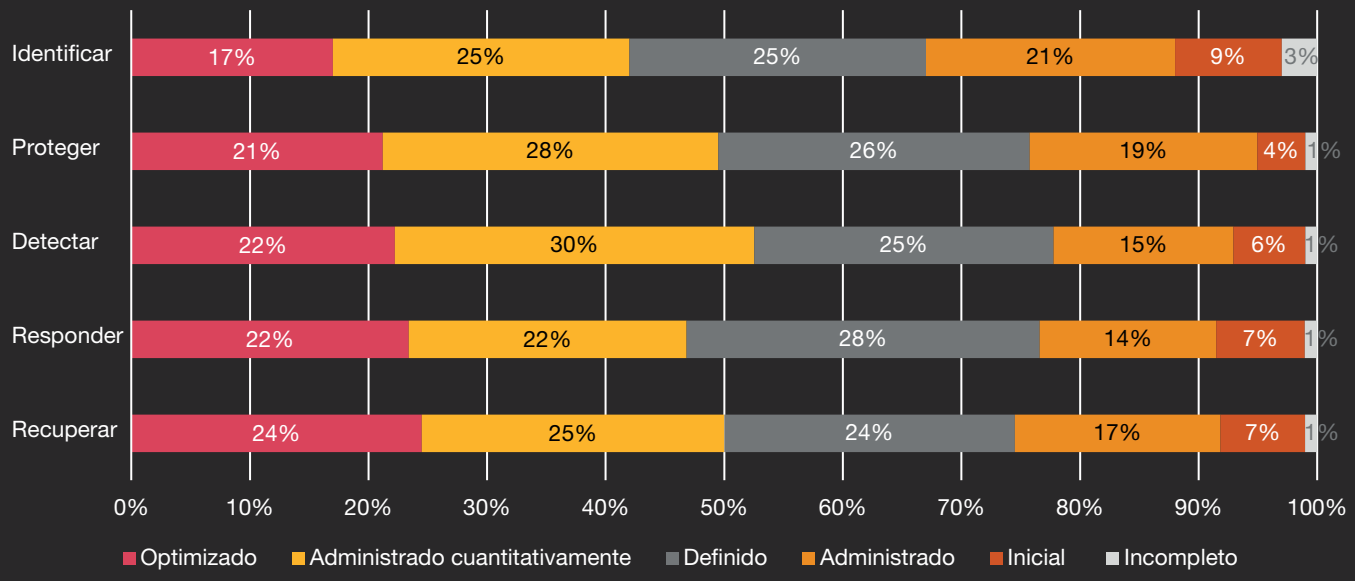


Fuente: Digital Trust Insights 2023 - Capítulo Colombia
P1b: En una escala del 1 al 10, ¿en qué medida su organización ha mitigado los riesgos de ciberseguridad asociados a cada uno de los siguientes aspectos en los últimos 12 meses?

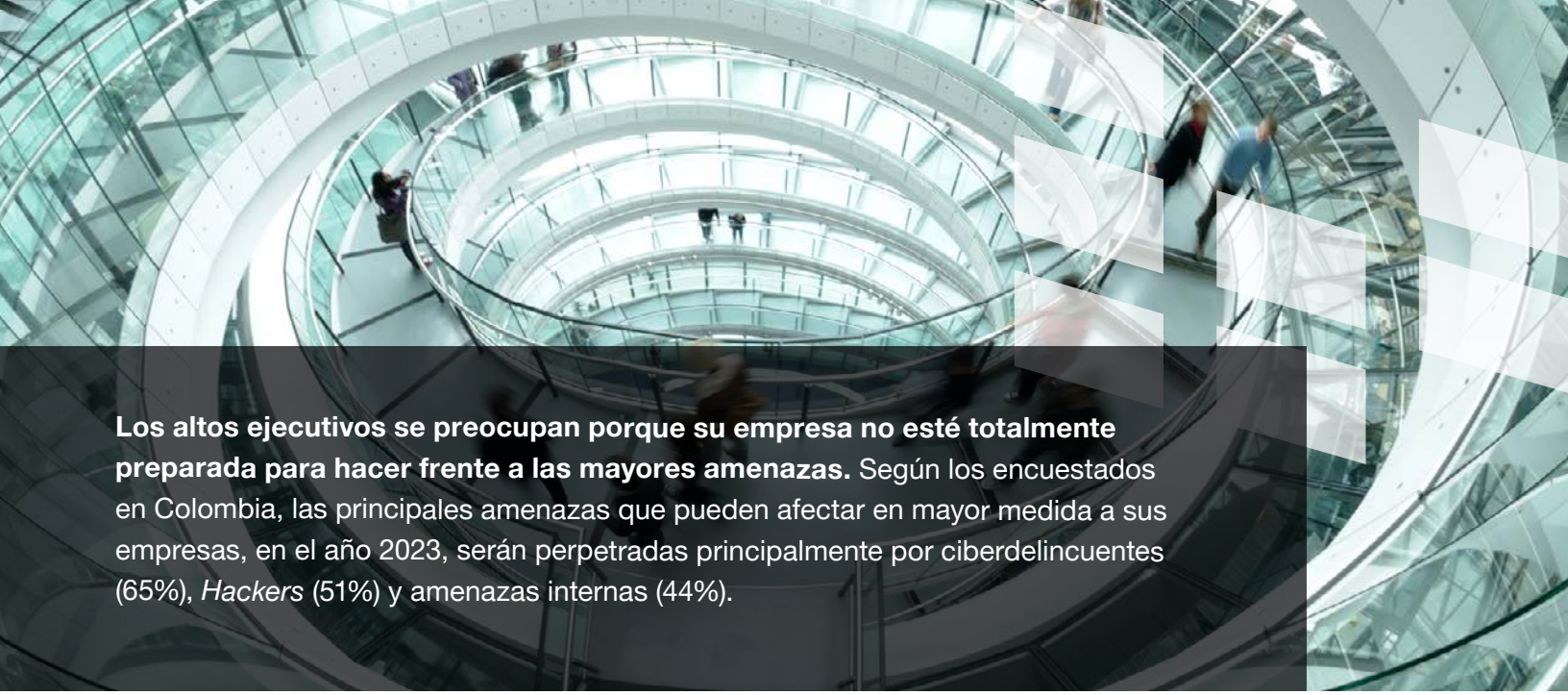
Según su propia evaluación, los CISO ven la necesidad de avanzar más en las 5 capacidades de ciberseguridad básicas descritas en el marco de seguridad cibernética del Instituto Nacional de Seguridad y Tecnología (NIST) de EE.UU.: Identificar, Proteger, Detectar, Responder y Recuperar. Solo el 3% respondió que cuentan con un nivel optimizado en todas las capacidades.

Es probable que las organizaciones más grandes, con ingresos superiores a mil millones de dólares, digan que están avanzando en la capacidad "Identificar" (21%). Aquellos que han visto aumentos en los ingresos y esperan que estos aumentos continúen, tienen más probabilidades de optimizar las 5 capacidades.

Gráfica 6: Madurez en las habilidades de Ciberseguridad

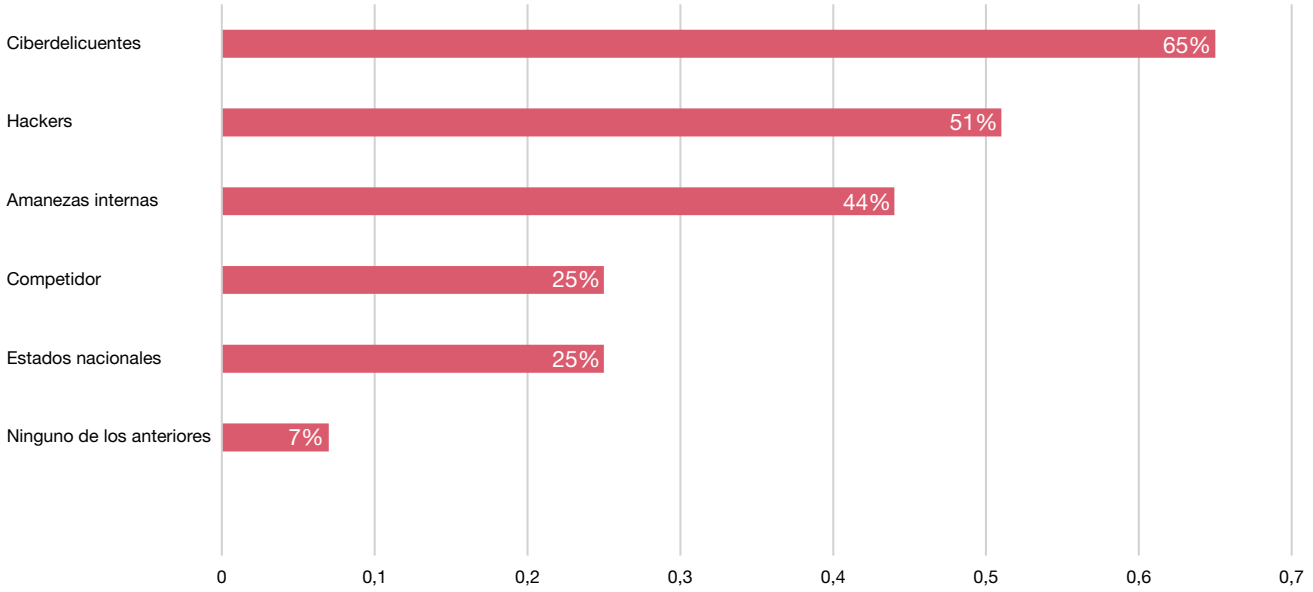


Fuente: Digital Trust Insights 2023



Los altos ejecutivos se preocupan porque su empresa no esté totalmente preparada para hacer frente a las mayores amenazas. Según los encuestados en Colombia, las principales amenazas que pueden afectar en mayor medida a sus empresas, en el año 2023, serán perpetradas principalmente por ciberdelincuentes (65%), *Hackers* (51%) y amenazas internas (44%).

Gráfica 7: Principales autores de ciberamenazas para las empresas en Colombia

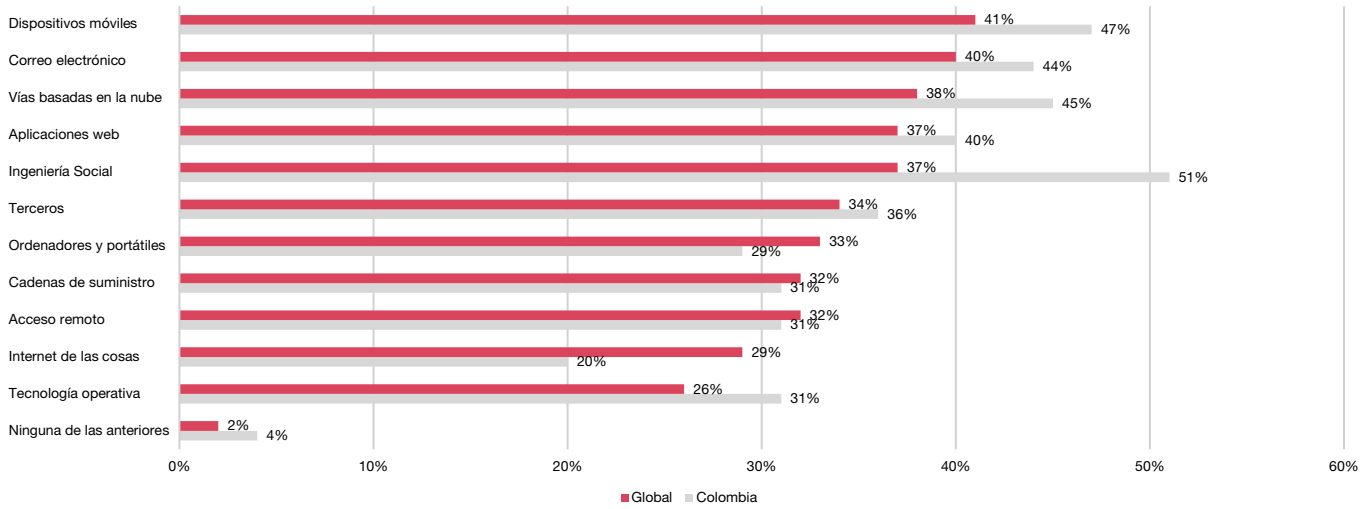


Fuente: Digital Trust Insights 2023 - Capítulo Colombia
P2a: Para cada uno de los actores de la amenaza que aparecen a continuación, ¿cuál espera que afecte significativamente a su organización en 2023 en comparación con 2022?

Los ciberataques son parte de la cotidianidad de operar en un ambiente digital. Las empresas pueden mantener sus defensas a través de una estrategia de ciberseguridad que brinde resiliencia y pueda reducir vulnerabilidades.

¿Cuáles son las vías principales de acceso para los adversarios a los sistemas de las compañías en Colombia? Los líderes del país mencionaron:

Gráfica 8: Principales vías a través de las cuales se vulnera la seguridad en las empresas en Colombia, en comparación con el resto del mundo



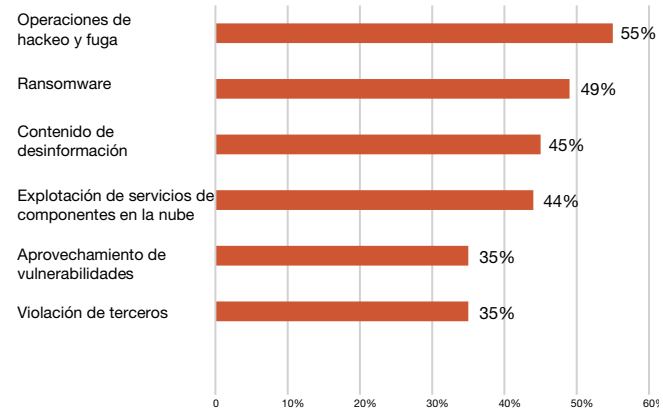
Fuente: Digital Trust Insights 2023
P2b: Para cada una de las vías (vectores de amenaza) por las que los adversarios pueden acceder a sus sistemas, marque las que espera que afecten significativamente a su organización en 2023 en comparación con 2022.

Las empresas están enfrentando ciberataques cada vez más complejos y sofisticados, los cuales se agudizaron por la necesidad de adoptar rápidamente tecnologías para operar en entornos virtuales, sin estar acompañados de la estrategia de ciberseguridad adecuada.

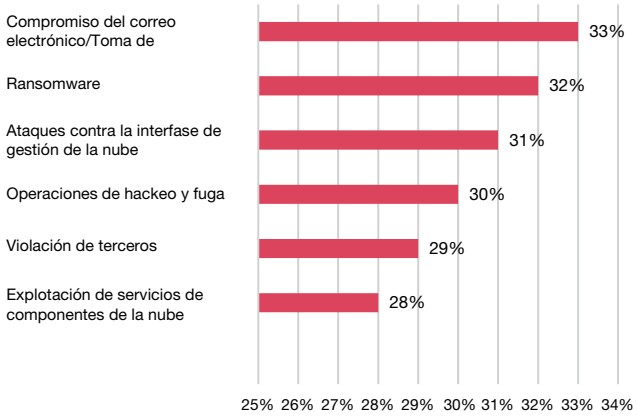
En línea con lo anterior, los encuestados en Colombia prevén que aumenten ciertos tipos de ataques cibernéticos en el año 2023, para los cuales las empresas deben no solo estar preparadas para afrontar, sino también deben, desde ya, fortalecer sus estrategias de prevención y mitigación. En primer lugar están los relacionados con acciones de hackeo y fuga de la información (55%), seguido de *Ransomware* (49%) y la explotación de servicios relacionados con la nube (44%). Las empresas colombianas deben dar mayor importancia a los ataques relacionados con el uso del correo electrónico y el robo o suplantación de cuentas corporativas. Otras empresas en el mundo ya los están considerando.

Gráficas 9 y 10: Tipos de ataques cibernéticos que pueden aumentar de forma significativa en las organizaciones colombianas y a nivel mundial, durante el 2023

Datos Colombia



Datos Global

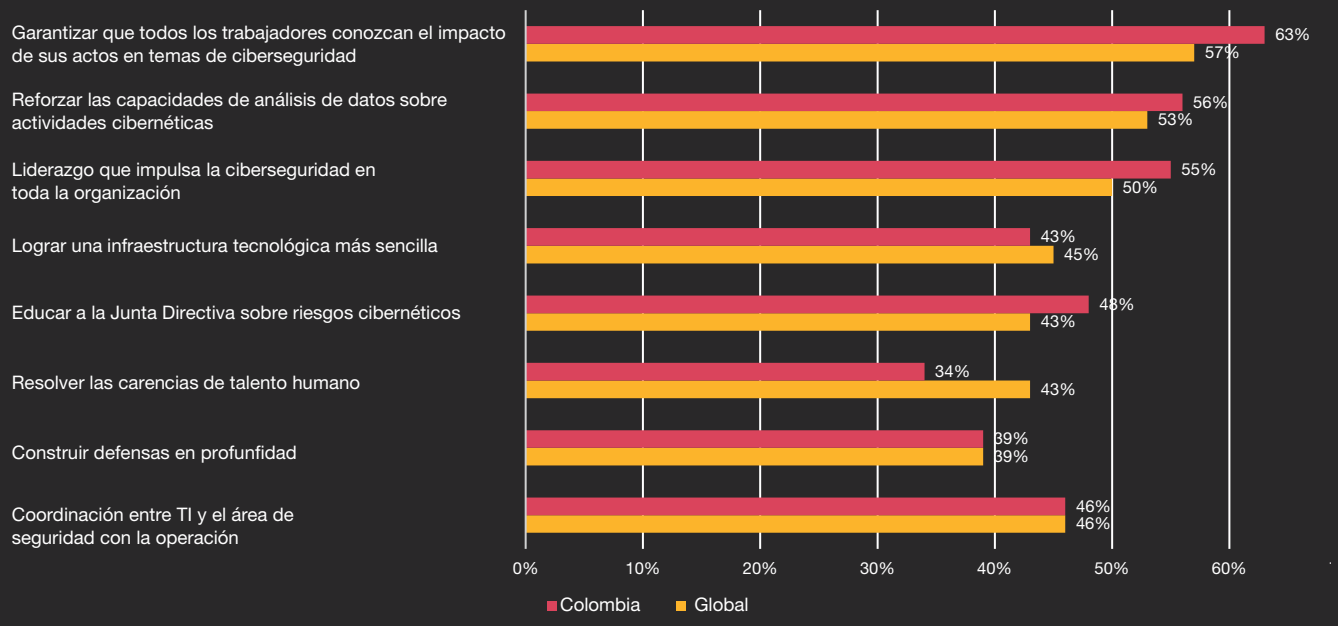


Fuente: Digital Trust Insights 2023
P2c: ¿Cuál de los siguientes ataques a su organización espera que aumente significativamente en 2023 en comparación con 2022?

Nuevos retos para 2023

- Las empresas en Colombia y en el mundo deben lograr estar preparadas para cumplir con todos los requisitos de divulgación efectiva de las prácticas, la estrategia y los incidentes de ciberseguridad, incluso cuando aumenta la presión de los reguladores. Según este estudio, menos del 50% de las empresas cumplen con todas las habilidades requeridas para la divulgación externa de estos tópicos.
- Los altos ejecutivos en Colombia se preparan no solo para un ataque cibernético catastrófico (73%), sino también para una recesión global (41%), una nueva crisis de salud (45%), alta inflación (33%), un nuevo conflicto geopolítico (35%) y cuellos de botella en la cadena de suministro (37%). Sin embargo, solo el 7% de las empresas a nivel mundial, aborda la resiliencia de manera integrada.
- Los consumidores, los reguladores favorables al consumidor, los defensores de la privacidad y los activistas ESG están ganando terreno. La seguridad y la privacidad de los datos son el talón de Aquiles de muchas organizaciones. Menos del 5% de los altos ejecutivos dice que siempre implementan las 10 prácticas estándar que identificamos como críticas para la madurez de ciberseguridad, y que lideran prácticas para proteger y controlar los datos de los clientes.
- Para seguir avanzando en la mitigación de los riesgos relacionados con ciberseguridad, los ejecutivos encuestados aseguran que es fundamental garantizar que todos los colaboradores estén alineados con las consecuencias de sus acciones y así contribuir para combatir los riesgos desde sus puestos de trabajo. Los demás aspectos a considerar se muestran, a continuación:

Gráfica 11: Aspectos que marcarán la diferencia en la transformación de la seguridad en las empresas Colombianas y a nivel mundial, en los próximos 12 a 18 meses



Fuente: Digital Trust Insights 2023
P6A: En su opinión, ¿cuál de los siguientes aspectos marcará la mayor diferencia en la transformación de la ciberseguridad en su organización en los próximos 12 a 18 meses?

- Si bien, un gran número de compañías Colombianas ha logrado mejorar sus niveles de ciberseguridad, aún existen áreas de oportunidad que deben ser atendidas bajo un presupuesto basado en la cuantificación de riesgos. El reto más importante es poder lograr alinear el presupuesto de ciberseguridad con el presupuesto corporativo. Para esto se recomienda que el CISO, quien comprende la estrategia global de ciberseguridad, identifique los riesgos potenciales, construya un presupuesto de cuánto cuesta proteger a la empresa en cada uno de los niveles, después compartir con CFO los datos para incluirlo en el presupuesto destinado a respuesta de incidentes y socializar los datos con el CEO, quien además de aprobar, comprender la importancia de incluir la ciberseguridad en cada decisión de negocio y los riesgos asociados.
- Otro de los retos más importantes para las compañías es poder reducir las restricciones en la capacidad de uso de los datos para la toma de decisiones para lograr generar estrategias que permitan oportunidades de mejora, a partir del conocimiento de los clientes. Para los encuestados en Colombia, las áreas o actores que en mayor medida restringen el uso de los datos son: Seguridad y gobierno (55%), la accesibilidad (45%), la precisión de los mismos (38%) y la usabilidad (40%).

Playbook para el C-suite en ciberseguridad

La ciberseguridad se ha convertido en un campo dinámico, que se ajusta y cambia rápidamente para seguir el ritmo de los requerimientos e iniciativas de las organizaciones. La agilidad es un componente clave para responder a los difíciles desafíos que se avecinan.

¿Cómo puedes seguir marcando la diferencia? ¿Dónde deberían ejercer influencia los CISO y los equipos de ciberseguridad para obtener mejores resultados?

Los *playbook* para el C-suite en ciberseguridad, que se presenta en el último Global Digital Trust Insights, destacan lo que se ha hecho, lo que se está haciendo y lo que se debe hacer para enfrentar los desafíos de 2023, con un enfoque integrado para construir futuros preparados para los retos de la ciberseguridad.

Una nota:

Los equipos de gestión están organizados de manera diferente en todo el mundo, por lo que podemos referirnos a títulos del C-suite que podrían no existir en tu organización.

Considera los títulos como abreviaturas del ejecutivo encargado de la ciberseguridad en la organización (CISO), que trabaja con los ejecutivos responsables del negocio en general (CEO); la supervisión y el gobierno de la gestión (la Junta), la infraestructura tecnológica (CIO/CTO), las inversiones cibernéticas (CFO), operaciones y cadena de suministro (COO), gestión de riesgos (CRO), datos (CDO/CPO) y recursos humanos (CHRO).

Ciberseguridad para directivos

Frente a la dinámica organizacional y los desafíos presentes, los CISO tienen una oportunidad única de salir de su rol de especialista técnico y convertirse en aliado de los ejecutivos de la organización. Esta colaboración con el C-suite es fundamental en el contexto actual.

42% de los altos ejecutivos dice que los incidentes de ciberseguridad de sus sistemas han aumentado desde el año 2020. Los ejecutivos y los Comités directivos deben analizar y entender si puede existir alguna afectación o exposición relevante para el negocio.

Más de una cuarta parte de los ejecutivos ha visto comprometida la seguridad de sus datos en los últimos tres años con costos que superan el millón de dólares. Para alrededor del 10% el impacto alcanzó los $10 millones o más, informaron los CISO y CFO.

Para los directores financieros, las consecuencias adicionales que se generan frente a los incidentes asociados a la filtración y pérdida de datos involucran:

- Inactividad o interrupción de las operaciones.
- Afectación de la calidad del servicio y/o producto.
- Pérdida de contratos y oportunidades comerciales.

Para los ejecutivos de privacidad y datos que trabajan con el público, los efectos más críticos de estos incidentes son:

- Pérdida de clientes.
- Costos para lograr la recuperación de los datos.
- Datos de clientes perdidos
- Sanciones por parte de entidades regulatorias.

El potencial impacto negativo de estos escenarios puede servir como un llamado de atención frente a la importancia de la colaboración, generando conciencia del efecto devastador de un ataque, que puede impactar desde el nivel operativo hasta el nivel directivo, e invitando a todo el C-suite a actuar de una forma integrada.

Los altos ejecutivos del C-suite están comenzando a comprender la necesidad de trabajar de una forma coordinada frente a los retos de la ciberseguridad. En el centro está el CISO, autorizado por el CEO para abogar, colaborar y orquestar la estrategia de ciberseguridad. El 46% de los directores ejecutivos quieren otorgar al CISO más autoridad para impulsar la colaboración en materia de seguridad para este año.

Los CEO adoptan una postura más activa en materia de ciberseguridad este año

Más de la mitad de los directores ejecutivos dice que exigirán un plan de gestión de riesgos de ciberseguridad para cada cambio comercial u operativo importante. Y más de la mitad dice que encabezará iniciativas importantes, como la optimización de la cadena de suministro y la eliminación de productos que debilitan la postura cibernética de la empresa. Los CEO quieren más información que les ayude a realizar un mejor trabajo en la supervisión de los programas de ciberseguridad de sus organizaciones. Más del 35% prioriza tres áreas para una mejor presentación de informes:

- Evaluaciones y prácticas de riesgo cibernético.
- Planes de continuidad de negocio, contingencia y recuperación ante un ciber incidente.
- Un panel sobre riesgos ciberseguridad clave.

Los CISO están aprendiendo cómo brindar a la alta dirección la información correcta sobre su programa de ciberseguridad y los riesgos que enfrenta su organización.

Mensaje a la alta dirección

¿Dónde puede el CEO marcar la mayor diferencia en ciberseguridad? Los grandes cambios pueden ser la forma más efectiva de mejorar la postura de ciberseguridad y solo el CEO puede influirlos.

¿Estás tolerando complejidades evitables e innecesarias en tus operaciones y tecnologías? Si es así, es importante trabajar en ello.

A menudo, las investigaciones después de una brecha en ciberseguridad importante, revelan debilidades más sistémicas que tecnológicas, causadas por la falta de enfoque entre los líderes empresariales para abordar las debilidades que los equipos sabían previamente que existían. Tal vez una desconexión entre los altos ejecutivos o entre el negocio y las funciones cibernéticas está ralentizando los esfuerzos de crecimiento: una aplicación para uso del consumidor, una nueva línea de negocio que utiliza inteligencia artificial; expansión a un nuevo mercado, o el uso del Internet Industrial de las Cosas en las operaciones.

Llamado a la acción:

Habla sobre tu compromiso con la ciberseguridad. Usa tu influencia para inspirar cambios radicales y crear un frente unido contra los ataques. Reúne al equipo de líderes en torno a la idea de que la forma segura podría ser realmente la forma más fácil de lograr el éxito empresarial.

Los Comités directivos pueden promover las capacidades de ciberseguridad

Los directivos están más comprometidos con la ciberseguridad a medida que sus empresas enfrentan riesgos cada vez mayores. El 54% dice que su organización ha asumido más riesgos de ciberseguridad a medida que busca una mayor digitalización y el 44% informa un aumento en los incidentes de ciberseguridad en sus sistemas desde el año 2020.

Reconocen el desafío de mantenerse al día con la ciberseguridad. Hoy, menos de la mitad de los encuestados del Comité directivo dice que gobiernan la ciberseguridad de forma efectiva. Solo el 9% de los encuestados dice que el comité gobierna la ciberseguridad "muy efectivamente" en todas las áreas.

Gráfica 12: Eficacia en la gobernanza de la ciberseguridad por parte de los Comités directivos

Fuente: Digital Trust Insights 2023

Sin embargo, el futuro de la supervisión de la ciberseguridad podría ser diferente. Los directores corporativos están dispuestos a aprender más sobre ciberseguridad y dedicarle más tiempo. Dicen que esto les ayudará a hacer un mejor trabajo en la gestión de la ciberseguridad en 2023:

- Capacitación interna de los comités o juntas directivas por parte de la gerencia (47%)
- Mayor frecuencia de reuniones enfocadas en ciberseguridad (47%)
- Informes mejorados sobre incidentes de ciberseguridad, prácticas y oportunidades de mejora (44 %)
- Agregar un miembro al Comité o Junta directiva con experiencia en ciberseguridad (43%)

Los CISO y el C-suite pueden ayudar a los Comités o Juntas directivas a conocer mejor la ciberseguridad de su organización, especialmente en los siguientes aspectos clave que fortalecen sus informes de ciberseguridad:

- Un *dashboard* que ayude a comprender los riesgos de ciberseguridad clave para la organización, con métricas relevantes.
- La estrategia de ciberseguridad de la organización y cómo se alinea con la estrategia general.
- Los planes de continuidad de negocio, contingencia y recuperación que fortalezcan la resiliencia y permitan una mejor respuesta a incidentes de ciberseguridad.

Mensaje a los comités directivos

Llamado a la acción:

- Reconsidera la prioridad y el tiempo asignado al CISO y a los aspectos de ciberseguridad en tu agenda.
- No te conformes con informes sin profundidad que no te brinden confianza ni información precisa sobre cómo la organización está administrando los riesgos de ciberseguridad o asegurando las iniciativas estratégicas. La ciberseguridad es un proceso continuo, por lo que es importante validar el progreso frente a los objetivos de tu plan estratégico e iniciativas de seguridad, así como al desarrollo de capacidades de defensa frente a amenazas emergentes relevantes en el contexto del negocio. Es muy importante poder participar en ejercicios o simulaciones que te permitan comprender el estado actual de la resiliencia en ciberseguridad en tu organización.

La nueva era de la transparencia en la ciberseguridad

Las partes interesadas claman por más información sobre cómo las empresas gestionan su exposición al riesgo de ciberseguridad.

Los reguladores

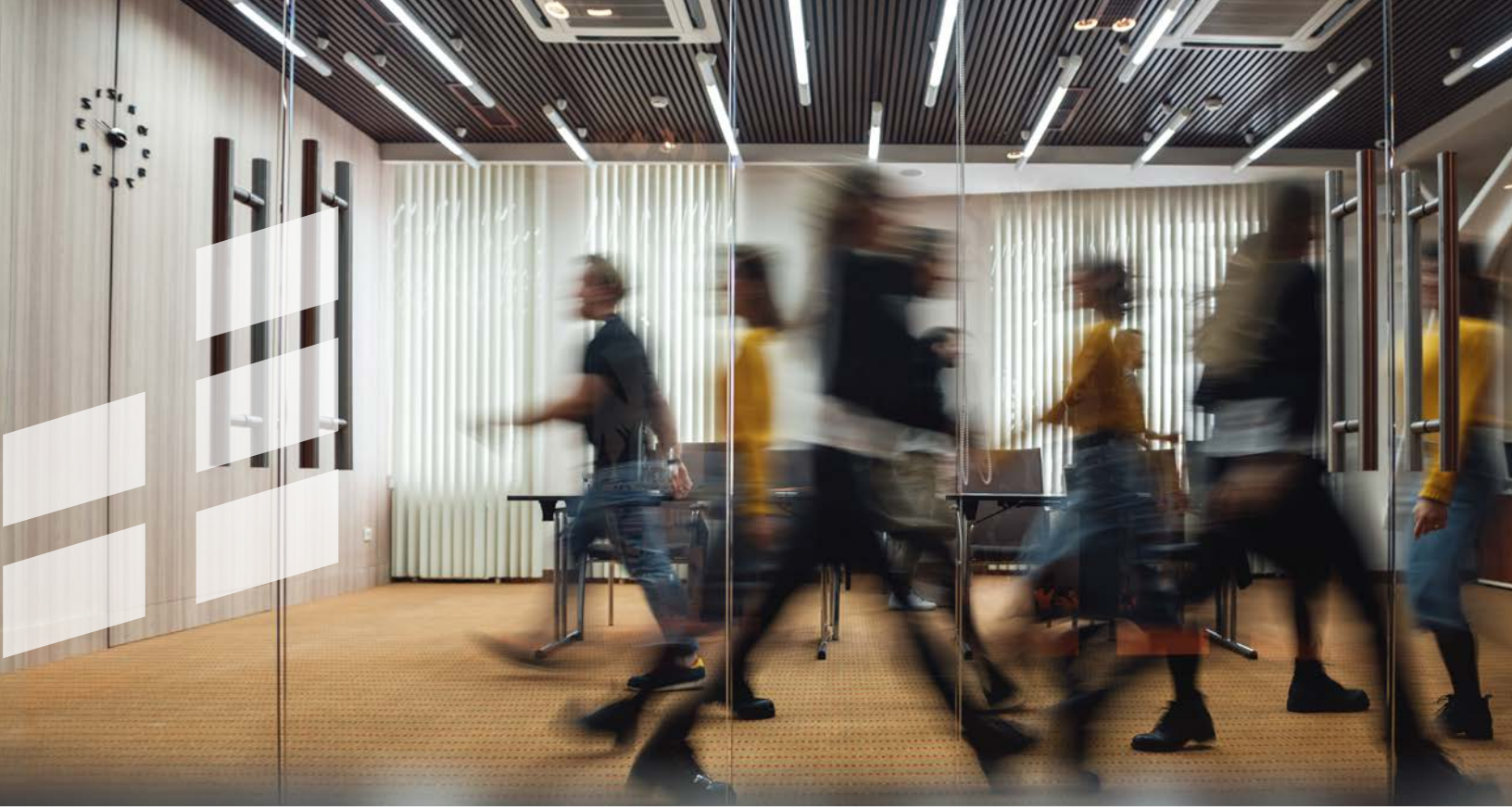
Quieren visibilidad acerca de las prácticas de ciberseguridad porque quieren proteger a los ciudadanos del fraude y la pérdida de privacidad; ayudar a los inversionistas a tomar mejores decisiones y evitar interrupciones en todo el sistema o en la industria. Varios países han publicado guías o protocolos sobre la respuesta y la gestión de incidentes de ciberseguridad. El Consejo de Información Financiera del Reino Unido ha emitido una guía sobre las divulgaciones de riesgos de seguridad digital después de descubrir que las divulgaciones actuales de algunas empresas del FTSE 350 no satisfacen las necesidades de los inversionistas y, a menudo, son repetitivas y demasiado estáticas. Además de las reglas pendientes con la Comisión de Bolsa y Valores (propuesta) y la Agencia de Seguridad de Infraestructura y Ciberseguridad (ley), el Departamento de Servicios Financieros del Estado de Nueva York está evaluando una propuesta que convierte las prácticas líderes en requisitos reglamentarios para las entidades reguladas.

Los inversionistas

Buscan divulgaciones coherentes y comparables para poder invertir su dinero en empresas que se ajusten a sus necesidades. Los incidentes de ciberseguridad pueden afectar el valor de las acciones, de manera temporal o permanente.

Las personas

saben que sus datos y su privacidad son vulnerables a los incidentes de ciberseguridad. **Los socios comerciales** quieren que sus datos y otros activos estén seguros. Estas partes interesadas quieren comprender cuánto pueden confiar en la capacidad de las empresas y de los sistemas para resistir las crecientes amenazas de ciberseguridad.



El C-suite ve una ventaja en la transparencia. Cuatro quintas partes de los altos ejecutivos en nuestra encuesta están de acuerdo en que la divulgación obligatoria de incidentes de ciberseguridad, con formatos comparables y consistentes, es necesaria para ganar la confianza de las partes interesadas. Sin embargo, menos del 10% confía en que su empresa pueda cumplir. Más de la mitad no está seguro de:

- Poder proporcionar la información requerida sobre un incidente importante dentro del período de tiempo requerido después del incidente (58%).
- Poder evaluar la materialización de un incidente de ciberseguridad con fines de notificación (58%).
- Poder describir la experiencia de ciberseguridad relevante en la Junta directiva para propósitos informativos (59%).
- Tener una política que establezca qué información puede o no divulgarse con respecto a incidentes de ciberseguridad (60%).
- Poder proporcionar información sobre la gestión de riesgos de terceros (63%).

Llamado a la acción:

Los CISO pueden posicionar a sus equipos para que trabajen con el CFO, la Junta directiva y otros altos ejecutivos, prepararse, traducir la estrategia y las prácticas en una narrativa precisa, cohesiva y convincente sobre las prácticas de gestión de riesgos de ciberseguridad de la empresa. La nueva era de transparencia en la ciberseguridad significa que los CISO deben volverse expertos en presentar información de una manera que la Junta directiva, la alta dirección y los inversionistas puedan entender y así, actuar en consecuencia. Requiere una estrategia de comunicación diferente a la jerga cotidiana de la ciberseguridad.

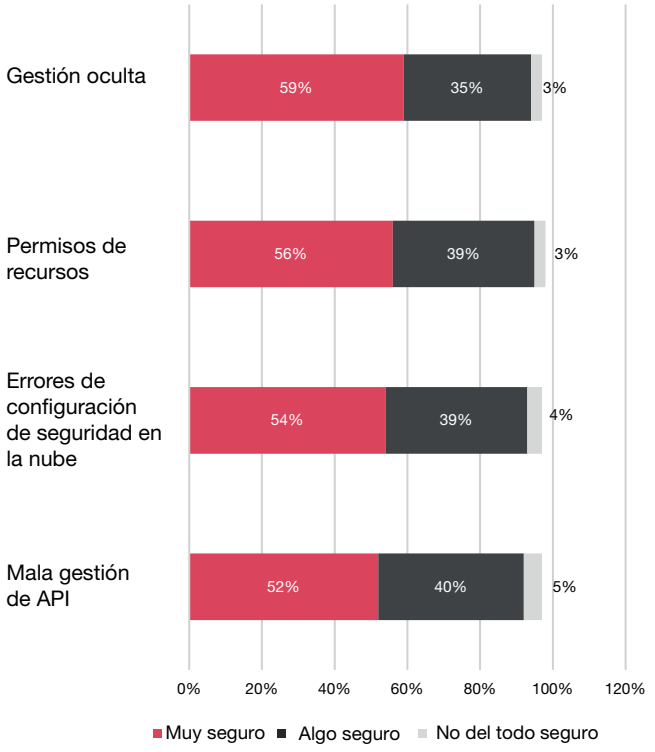
Los directivos de tecnología (CIO/CTO) enfrentan la seguridad en la nube en conjunto con el CISO

¿Es nuestro plan de seguridad en la nube tan ágil como nuestro propio negocio en la nube? Esa es la pregunta que los CIO y CISO deberían hacerse ahora.

Las amenazas basadas en la nube están aumentando en casi el 40% de las organizaciones. Mientras tanto, casi dos tercios de los altos ejecutivos dicen que no han mitigado por completo los riesgos de la adopción de la nube.

Las noticias no son todas negativas. La mitad de los CISO, CIO y CTO dice que han logrado avances en la implementación del gobierno, la gestión de identidades, la concesión de permisos de recursos, las configuraciones de seguridad en la nube y la gestión de API (Application Programming Interfaces), pero solo el 19% está “muy seguro” de que su organización ha gestionado adecuadamente todas las amenazas de ciberseguridad en este entorno.

Gráfica 13: Confianza en que la organización está protegida frente a las siguientes acciones que representan violaciones a la seguridad en la nube



El CIO o CTO y su equipo de DevOps (Development Operations) pueden sentirse ansiosos o presionados, por aprovechar la agilidad, la velocidad y la colaboración que ofrece el trabajo en la nube.

Estos equipos pueden eludir al CISO para evitar priorizar el análisis o la implementación de controles de seguridad que el CISO seguramente recomendaría. En el vertiginoso mundo digital, las iniciativas de negocio son conscientes que la velocidad es un factor crítico para el logro de sus objetivos. Cuando la agilidad y la velocidad son los objetivos, ¿quién necesita frenos?

Sin embargo, el gobierno y la seguridad asociada a las iniciativas de transformación en la nube es clave, especialmente en un entorno de múltiples nubes donde cada proveedor de servicios tiene diferentes capacidades y requisitos de seguridad. Los lanzamientos de nuevas funciones y actualizaciones generan cambios permanentes y nuevos vectores para posibles ataques.

En 2023, es hora de diseñar una arquitectura de seguridad general que incluya todas las plataformas en la nube que utiliza tu empresa.

Reúne todos los controles de seguridad de tu empresa para que puedas protegerlos desde una ubicación y con la mayor automatización posible. Crea herramientas de infraestructura como código (IaC) y DevSecOps (Development Security Operations) para establecer automáticamente las comprobaciones de seguridad adecuadas en todas sus plataformas en la nube.

Los CISO pueden proporcionar a los desarrolladores servicios de seguridad en la nube que sean fáciles de usar y se ajusten a las políticas de seguridad de la organización. La creación de una API de cifrado para uso de los desarrolladores, por ejemplo, puede ayudar a acelerar el tiempo de comercialización de una aplicación, así como a confirmar que el cifrado utiliza protocolos aprobados por la empresa.

Mensaje a los CIO y CTO

- Forma alianzas con tu equipo de seguridad y DevSecOps.
- Adopta un enfoque donde los lineamientos y mecanismos de seguridad en la nube sean definidos e implementados antes que comience el uso de la nube. El desarrollo ágil, los controles y servicios de la arquitectura de seguridad pueden ir de la mano. Las empresas líderes diseñan y administran controles con un enfoque preventivo, a la velocidad y agilidad del DevOps.
- El desarrollo rápido y los controles sólidos pueden ir de la mano. Las empresas líderes diseñan y administran controles que no funcionan al ritmo lento que a menudo se asocia con la supervisión, sino a la velocidad rápida y ágil del DevOps. En estas organizaciones, todos ganan.

Llamado a la acción:

Logra el aseguramiento de las tecnologías de *back-end, front-end, IoT* y operacionales trabajando en conjunto con el CISO para generar entornos digitales en la nube confiables.

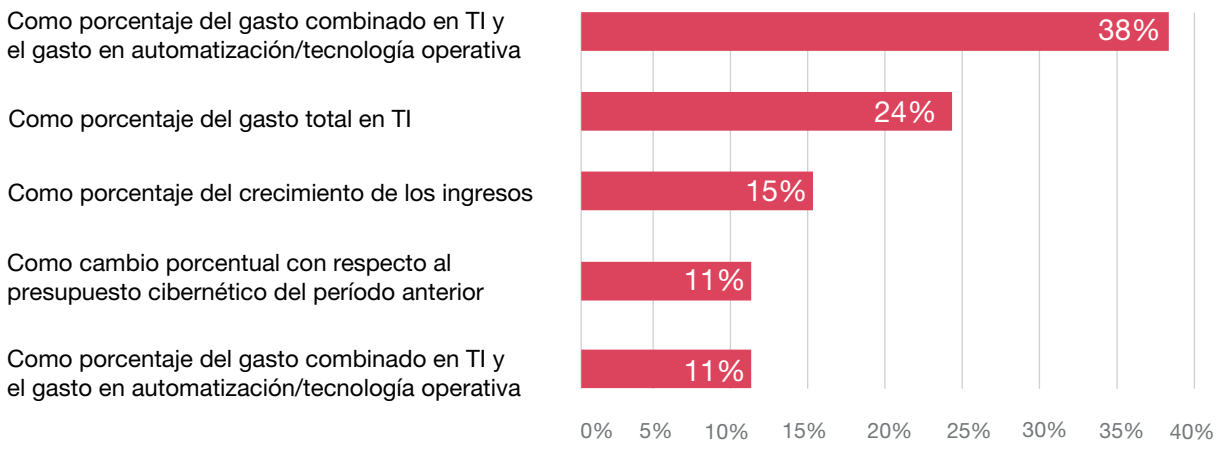
Los CFO y los CISO toman en serio el retorno de beneficios frente a la inversión en ciberseguridad

Las empresas siguen aumentando su inversión en ciberseguridad. El 65% de los altos ejecutivos dice que esperan un aumento en 2023, en comparación con el 69% en 2022, pero no están aumentando los presupuestos cibernéticos tanto como lo hicieron para 2022. Si bien más de una cuarta parte de las empresas esperaban que los desembolsos para ciberseguridad en 2022 aumentaran más del 10%, menos de una quinta parte espera que esa tasa aumente el próximo año.

El presupuesto para ciberseguridad está cambiando

Cuando se habla de presupuesto para la ciberseguridad, las empresas adoptan un enfoque más expansivo. Casi 4 de cada 10 CEO, CFO y CISO dicen que sus empresas ahora financian la ciberseguridad como un porcentaje de todo el gasto en tecnología, incluidos OT y automatización. Otro 15% dice que asigna el presupuesto de ciberseguridad como un porcentaje de los ingresos.

Gráfico 14: ¿Cómo establecen las empresas los presupuestos para ciberseguridad?



Fuente: Digital Trust Insights 2023

Muchos también han comenzado a cambiar su estrategia de inversión en ciberseguridad. Más de la mitad dice que está eligiendo “en gran medida” cómo gastar en ciberseguridad de acuerdo con siete parámetros clave , que incluyen:

- En línea con la estrategia comercial general (55%)
- Reflejando las prioridades de ciberseguridad (55%)
- Agregando valor a la organización (52%)
- Equilibrando las necesidades inmediatas y a largo plazo (51%)
- Informado por cuantificación de riesgo (51%)
- Considerando la tolerancia de riesgo de la organización (51%)
- Asignado de acuerdo a los riesgos que enfrenta la organización (51%)

Modernización de la tecnología

Las soluciones tecnológicas de ciberseguridad encabezan la lista de áreas que los CFO consideran clave para mejorar la postura de ciberseguridad de su organización.

De hecho, la modernización, especialmente de la tecnología operativa, sigue siendo un problema en muchas organizaciones. La tecnología obsoleta y la gestión de sus vulnerabilidades son las principales barreras para mejorar la seguridad de la tecnología operativa, dicen los CISO, CIO y CTO.

La complejidad también sigue siendo una gran preocupación. Simplificar y consolidar la cartera de soluciones de ciberseguridad es una de las principales prioridades para 2023 entre los encuestados que han tenido un incidente de ciberseguridad en los últimos tres años. El informe *Global Digital Trust Insights* de 2022 anticipó esta tendencia: el 75% informó que sus datos, tecnología y otras operaciones eran demasiado complejas, lo que generaba preocupaciones sobre los riesgos de ciberseguridad.

Gráfica 15: Áreas donde las empresas consideran aumentar la inversión en ciberseguridad

Fuente: Digital Trust Insights 2023

Mensaje a los directores financieros

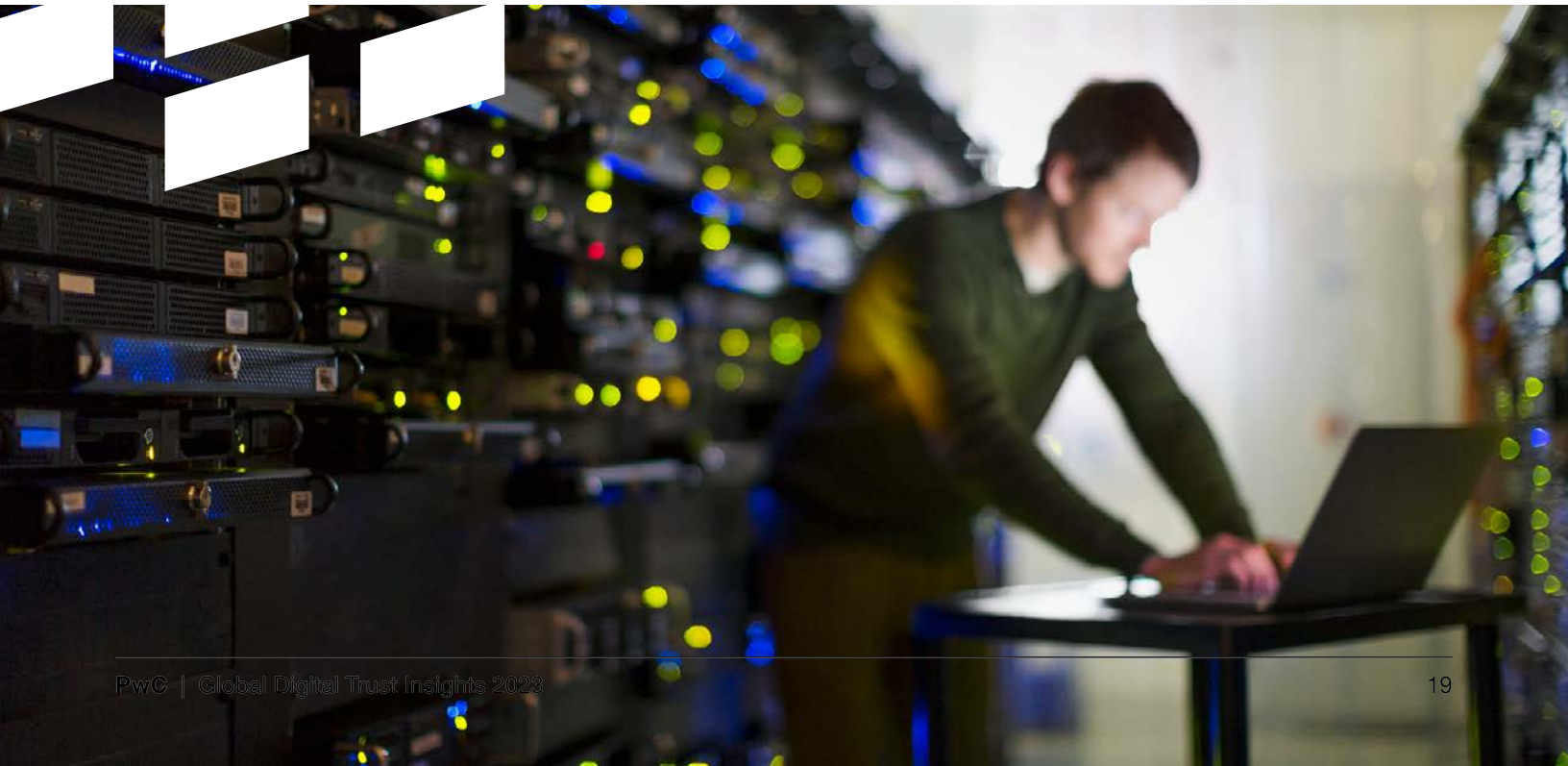
Tener claridad frente a las siguientes preguntas es fundamental para la gestión de las iniciativas de seguridad: ¿Estamos gastando lo suficiente y en las áreas correctas? Y ¿estamos reduciendo el riesgo de ciberseguridad en la proporción correcta, de acuerdo a nuestras inversiones?

A medida que proliferan las soluciones y servicios en seguridad, los directivos deberán trabajar con el CISO desarrollando un plan que proteja su organización en múltiples niveles y, al mismo tiempo, simplificar y optimizar los controles y servicios de ciberseguridad.

La naturaleza abierta de la nube y de las plataformas tecnológicas requiere ajustar sus parámetros de confianza, involucrando arquitecturas de confianza cero. El 36% de los CISO dice que han comenzado a implementar componentes de confianza cero y otro 25% comenzará en los próximos dos años.

Llamado a la acción:

a medida que modernices y simplifiques tu arquitectura de seguridad, pregúntate cómo cada cantidad que gastas puede reducir una mayor parte del riesgo de ciberseguridad. Las empresas que conocen los impactos económicos del riesgo entienden la importancia de asegurar desde la planeación y esto les permite ahorrar frente a enfoques correctivos.



Los directivos responsables de las operaciones de negocio (COO) coordinan planes de defensa en conjunto con el CISO para hacer frente a los crecientes ataques a la cadena de suministro y a la infraestructura OT

La cadena de suministro es un punto focal para las amenazas de ciberseguridad y de otro tipo, las presiones macroeconómicas, competitivas, y las preocupaciones de ESG.

Más de la mitad (56%) de los CRO y COO dice que están **extremadamente o muy preocupados** por su capacidad para resistir los ataques a la cadena de suministro.

Solo alrededor de una cuarta parte está totalmente de acuerdo en que su fuerza laboral de operaciones tiene las habilidades digitales necesarias o que han invertido lo suficiente, para evitar que los ataques de ciberseguridad interrumpan su cadena de suministro.

De igual manera, les preocupa que su capacidad para controlar estas amenazas esté en parte, en manos de terceros que no tengan la capacidad para protegerlas. Solo una quinta parte está totalmente de acuerdo en que sus socios y proveedores externos han invertido o están haciendo lo suficiente para evitar interrupciones en la cadena de suministro por ataques de ciberseguridad, 13% está en desacuerdo.

Tecnologías operativas (OT): se necesitan más y mejores soluciones

Solo alrededor de un tercio de todos los encuestados dice que han mitigado por completo los riesgos asociados con la convergencia de OT y TI o los riesgos asociados al mayor uso del Internet de las cosas.

Esta es otra área de preocupación para los COO y CRO: la seguridad de la tecnología operativa (OT). A medida que las tecnologías y soluciones de OT se vuelven más sofisticadas, por ejemplo, mediante el uso de inteligencia artificial y aprendizaje automático para aumentar la automatización en las plantas de fabricación, las organizaciones luchan por mantenerse al día y mantener sus operaciones seguras.

No solo los CRO y los COO ven estos desafíos. Los CISO y los CIO también los conocen. Sin embargo, entre ellos existen diferencias en lo que cada uno considera como el mayor obstáculo para las operaciones modernas y totalmente seguras:

- Ambos grupos dicen que tener soluciones tecnológicas inadecuadas es un gran obstáculo para mejorar OT.
- Para los CISO/CIO, el obstáculo número uno proviene del uso de software y herramientas de gestión de vulnerabilidades obsoletos.
- Al mismo tiempo, los CRO/COO creen que se necesita un enfoque más amplio para el riesgo cibernético de OT, uno que considere no sólo los riesgos comerciales y financieros, sino también los riesgos de salud, seguridad y ambientales. Para ellos, que estas preocupaciones no reciban la misma consideración juega un papel principal para obstaculizar las mejoras de OT.
- También quieren soluciones que aborden específicamente la seguridad de OT.

Si bien son conscientes de estas deficiencias, los CISO y los CIO también señalan que sus organizaciones carecen de un inventario de activos completo y preciso de datos, personas, sistemas e instalaciones de OT, lo que es fundamental para la resiliencia operativa.

Mensaje a los directores de operaciones

A medida que las operaciones de la empresa son cada vez más digitales, la importancia de asegurar las operaciones en conjunto con los equipos de ciberseguridad es fundamental, en especial frente a las posibles deficiencias de aliados y proveedores externos.

Es posible que sus equipos de riesgo, auditoría interna y cumplimiento ya estén trabajando con los equipos de ciberseguridad. La mitad de los CRO/COO encuestados dice que estos equipos están monitoreando y priorizando los riesgos de manera consistente. Otro tercio lo hace a veces.

Este trabajo en equipo está dando sus frutos. Casi el 79% de los encuestados dice que su equipo de ciberseguridad ha progresado en la protección de su infraestructura OT en el último año. Casi tres cuartas partes dice que han visto una mejor colaboración entre los equipos de ciberseguridad y de OT.

Pero los ataques a la cadena de suministro y OT no han llegado a la parte superior de la lista en términos de amenazas probables, lo que puede crear una falsa sensación de seguridad. No bajar la guardia. Ya se ha identificado lo que puede suceder cuando las empresas bajan la guardia con respecto a la cadena de suministro de software y los ataques OT, que van en aumento. Los actores de amenazas de ciberseguridad que buscan una forma de atacar sus sistemas, a menudo, identifican como objetivo el punto de menor resistencia, así que no permitas que tu dominio sea ese punto.

Llamado a la acción:

Trabaja activamente con tu CISO para que sus equipos colaboren en la seguridad de la infraestructura OT y la cadena de suministro, considerando desde el monitoreo y pruebas de seguridad, hasta el gobierno y la arquitectura. Analiza cómo mejorar la resiliencia y cómo prevenir o responder ataques específicos.

Directivos de riesgo (CRO) y CISO respondiendo al riesgo con resiliencia

"Riesgo" es la palabra de hoy. Cada vez más, los equipos de ciberseguridad trabajan junto con los de riesgo, auditoría interna y cumplimiento, una señal de que la ciberseguridad está ocupando un lugar importante, como una prioridad de gestión de riesgos empresariales.

Un número creciente de CRO, CAE y directores de cumplimiento reconocen que ciberseguridad significa negocio. La mitad de los encuestados dice que los equipos de ciberseguridad están monitoreando y priorizando los riesgos "consistentemente" junto con estas otras funciones. Aproximadamente otro tercio lo hace parte del tiempo.

- Monitoreo de riesgos (50%).
- Priorización de riesgos (50%).
- Tener una comprensión común de cómo encajan los riesgos de ciberseguridad en la gestión de riesgos empresariales (49%).
- Reportar a la alta dirección (49%).
- Responder juntos a ciberataques e incidentes (48%).
- Aplicar un modelo común de gobierno de datos (45%).
- Desarrollar una visión común de los riesgos y amenazas en todo el ecosistema (44%)
- Cuantificar los riesgos (44%).
- Proporcionar a los líderes de las unidades de negocio (los propietarios de riesgos) las herramientas para gestionar mejor los riesgos en las operaciones (43%).
- Aplicar un modelo común de gobernanza digital (41%).
- Seguir un modelo operativo para la división de responsabilidades entre funciones de riesgo y ciberseguridad (40%).

Es mucho más probable que aquellas empresas con un incidente de ciberseguridad en su historial respondan de manera consistente a las intrusiones: el 50% en comparación con el 38% de las empresas sin incidentes.

Sin embargo, el enfoque de "todos para uno, uno para todos" del riesgo de ciberseguridad no ocurre tan a menudo como podría parecer a primera vista. Solo el 7% afirma que los equipos de ciberseguridad trabajan de manera consistente con otras funciones en todas las actividades relacionadas con el riesgo. Los CRO/COO tienen trabajo que hacer en esta área.

Estos ejecutivos tienden a aplaudir el desempeño de los equipos de ciberseguridad y de privacidad de sus organizaciones. Casi la mitad dice que estos equipos están logrando objetivos importantes "excepcionalmente bien", incluida la implementación de controles para evitar incidentes de continuidad, algo importante para la resiliencia empresarial. Sin embargo, solo el 5% de los CRO/COO cree que la ciberseguridad y la privacidad cumple todas las expectativas "excepcionalmente".

Pruebas de resiliencia en 2023

"La vida es eso que pasa mientras haces otros planes", dice el refrán. También es cierto en los negocios.

La resiliencia significa poder mantener sus operaciones incluso cuando surgen problemas inesperados: un ataque de ciberseguridad, una recesión mundial, una nueva crisis sanitaria, aumento de la inflación o escasez de materias primas.

Estas son las principales preocupaciones de nuestros encuestados para los próximos 12 a 24 meses, pero pocos parecen estar listos para manejarlos adecuadamente.

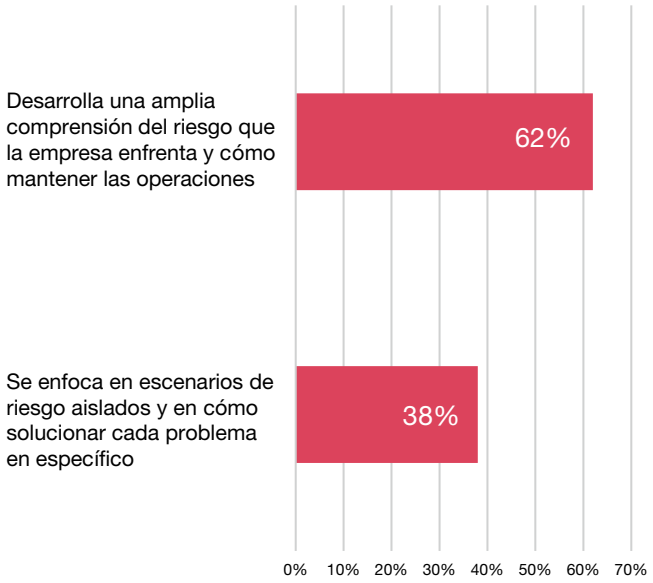
Adoptar un enfoque que considere los distintos escenarios de crisis en el contexto actual, identificando las fuentes de interrupción y los protocolos de escalamiento, es fundamental. Sin embargo, solo el 7% de los altos ejecutivos dice que están adoptando enfoques verdaderamente integrados y holísticos para las 5 capacidades básicas de la ciberseguridad que fortalecen la resiliencia.

La buena noticia para los CRO/COO es que el 62% maneja el riesgo de manera integral, pero en todas las demás áreas (respuesta a incidentes, continuidad del negocio, recuperación ante desastres), aproximadamente la mitad de las organizaciones parece tratar cada incidente como único en lugar de integrar las lecciones aprendidas de las diversas competencias básicas de resiliencia.

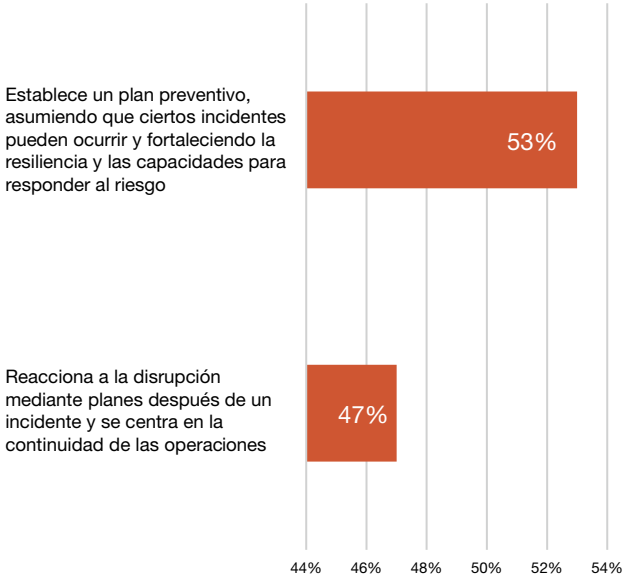
Los CRO/COO se están dando cuenta de que este modelo a corto plazo es similar a tapar fugas en el dique a medida que ocurren, en lugar de construir una presa fuerte y resistente desde el inicio, que es un enfoque mucho más efectivo.

Gráficas: 16 al 20 Enfoque y capacidad actual de resiliencia cibernética en las organizaciones - diferentes enfoques

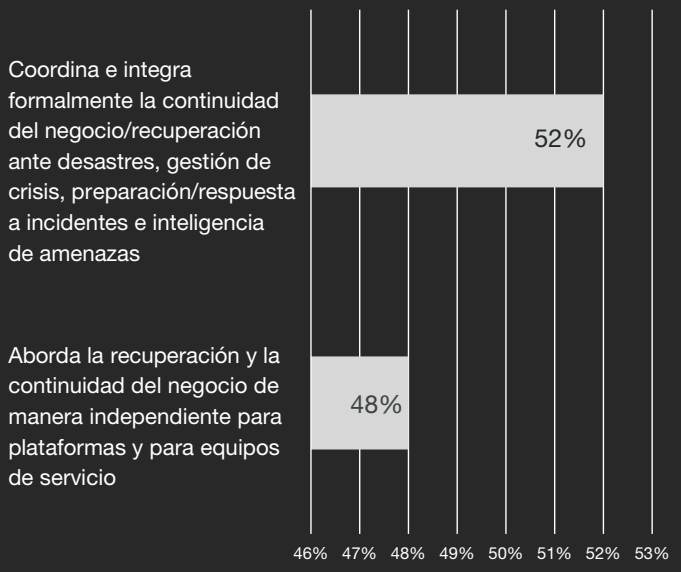
Gráfica 16: Riesgo



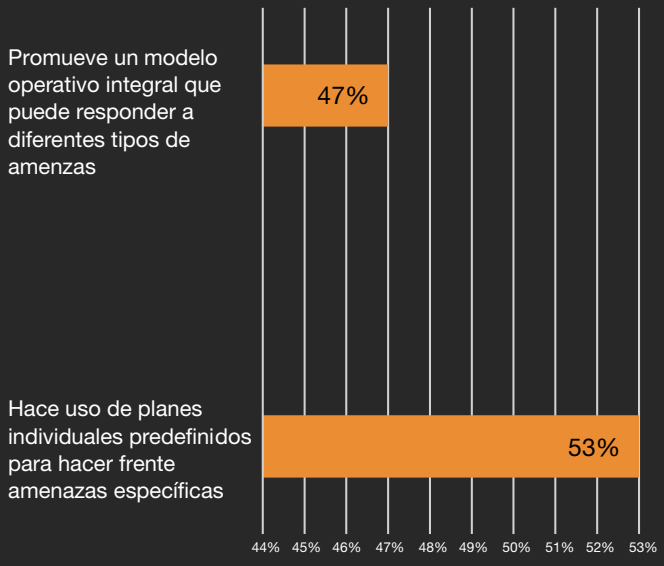
Gráfica 17: Respuesta



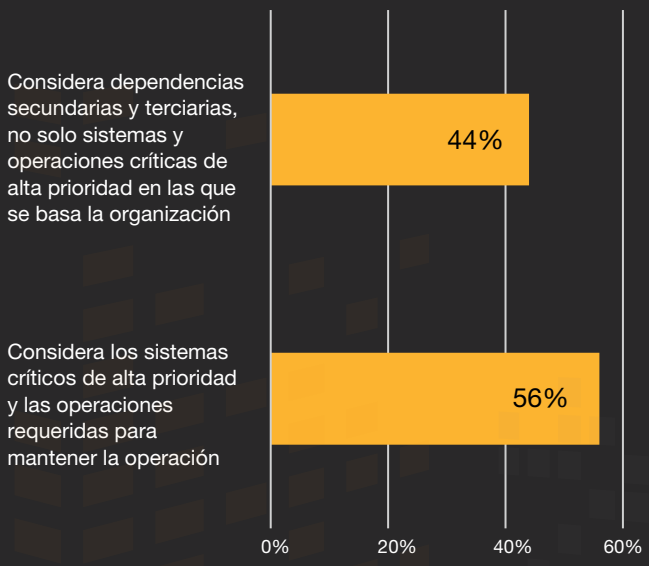
Gráfica 18: Continuidad de negocio



Gráfica 19: Preparar



Gráfica 20: Sistemas



Fuente: Digital Trust Insights 2023
Pregunta: ¿Cuál de las siguientes declaraciones describe mejor el enfoque y la capacidad actual de resiliencia cibernética de su organización?

Mensaje a los CRO

Los escenarios de 2023 requieren que el C-suite y la alta dirección trabajen juntos.

Los incidentes, se dice, son inevitables. Una respuesta acertada, una que limite severamente el impacto que pueden causar los cibercriminales, es en gran medida una función del trabajo preliminar que se ha realizado para establecer una base de ciberseguridad sólida y resistente.

Cada vez más, las autoridades financieras de todo el mundo colaboran para probar la resiliencia de las instituciones financieras. La coordinación y el cumplimiento regulatorio están comenzando a extenderse más allá de los servicios financieros.

En asociación con los CISO, se debe presentar un caso al CEO y a la alta dirección: la verdadera resiliencia organizacional requiere mucha coordinación entre todo el C-suite y ellos deben liderar el camino.

Los directores ejecutivos pueden necesitar un empujón ocasional para salir de su zona de confort, especialmente si se encuentran en un estado de inercia. Pueden pensar que no necesitan actuar porque la empresa ya tiene planes de gestión de crisis, continuidad del negocio o recuperación ante desastres. Pero, ¿qué tan coordinados son estos planes? ¿La organización los ha probado? ¿Puede la organización recuperarse dentro de los objetivos de tiempo que se ha fijado?

Llamado a la acción:

Revisa tu tolerancia al riesgo para conocer tus límites de resiliencia: el significado específico de la resiliencia depende en parte de la tolerancia y de la adaptación al riesgo de la organización. Valida los planes de crisis, continuidad del negocio y recuperación de desastres en un plan de resiliencia empresarial integral. Debes estar en sintonía con los altos ejecutivos para establecer un enfoque coordinado que te permita desarrollar capacidades de respuesta en el caso de que surjan problemas.

La colaboración en la seguridad y la protección de la privacidad de los datos es urgente

Las empresas se están volviendo expertas en el uso de datos para comprender mejor lo que los clientes quieren y de ésta manera dárselo. Los datos ahora son parte integral de su transformación digital centrada en el cliente.

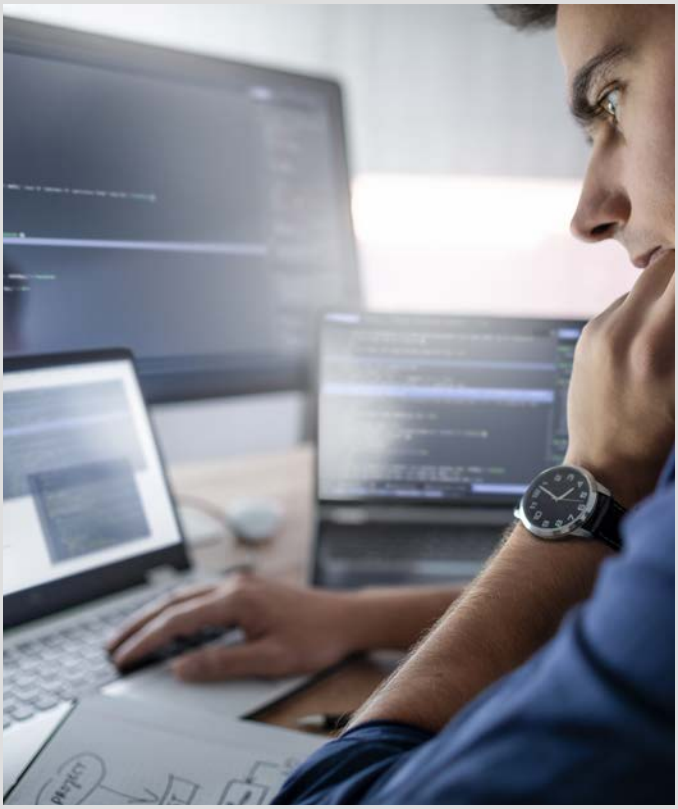
Un tercio de los CMO, CDO y CPO dice que siempre usan datos para monitorear los comentarios de los clientes y crear experiencias personalizadas. Más de una cuarta parte usa datos de manera constante para encontrar segmentos desatendidos y hacer crecer su negocio.

Gráfica 21: Recopilación, procesamiento y uso de datos de clientes. ¿Qué están haciendo las organizaciones?

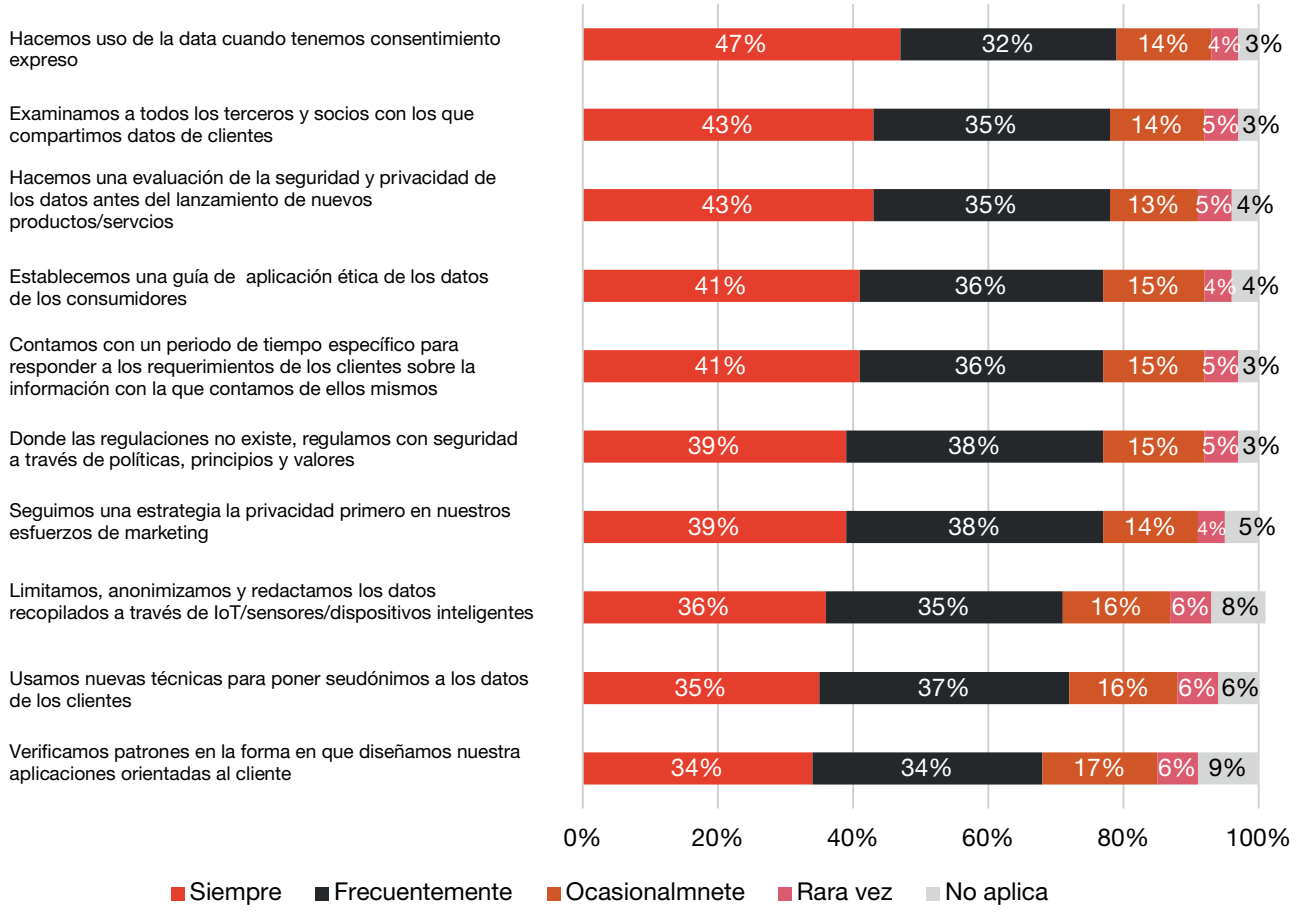
Fuente: Digital Trust Insights 2023

Para capturar el valor duradero de esta transformación, las empresas deben procesar y administrar datos y algoritmos de manera inteligente y eficiente. Al mismo tiempo, deben abordar las preocupaciones de privacidad y ética pública, así como cumplir con los estándares regulatorios.

Pero, ¿cuántos realmente toman en serio la autorización y la privacidad del cliente? Los enfoques para la gestión y el gobierno de datos que informan los altos ejecutivos son reveladores y, al mismo tiempo, no sorprenden.



Gráfica 22: Políticas y prácticas que las empresas están usando para garantizar la gestión y el gobierno de los datos de los clientes



Fuente: Digital Trust Insights 2023

La mitad dice que a veces pueden usar los datos de los clientes sin la autorización expresa.

Es posible que el 54% no siempre evalúe a todos los terceros y socios (encargados) con los que comparten datos de clientes. Este mismo porcentaje a veces podría lanzar nuevos productos y servicios sin una evaluación de seguridad y privacidad de datos.

Casi el 60% dice que es posible que no siempre verifiquen *"dark patterns"* (una interfaz de usuario que se ha diseñado cuidadosamente para influenciar a las personas para que tomen decisiones potencialmente perjudiciales para la protección de sus datos personales) en la forma en que diseñan las aplicaciones que usan sus clientes.

De hecho, el 50% de los ejecutivos dice que la falta de seguridad y gobierno son el principal obstáculo para un mayor uso de los datos para la toma de decisiones,

superando la falta de accesibilidad a los datos (47%), precisión (42%) y facilidad de uso. (42%).

Solo entre una quinta y una tercera parte de los CMO, CDO, CPO y CISO están totalmente de acuerdo en que su programa o equipo de ciberseguridad y de privacidad:

- Les da seguridad en la capacidad para fomentar la confianza de sus clientes (27%).
- Ayuda a su área de Marketing a cumplir de manera eficiente y efectiva con las regulaciones (25%).
- Les permite pensar en cualquier compensación entre seguridad y privacidad por un lado, y crecimiento rentable por el otro (24%).
- Les da una ventaja competitiva en el mercado (24%).
- Les da una ventaja competitiva con los clientes (21%)

Mensaje a CDO y CPO

Se tiene que hacer un mejor trabajo al gobernar los datos y proteger la privacidad. Entre las empresas identificadas en la Encuesta de ganadores del mercado de 2022 de PwC, el manejo de los datos de los clientes para mejorar la confianza y el intercambio de términos de privacidad de datos en un lenguaje amigable para el cliente, se ubicaron en la parte superior los planes de inversión en ciberseguridad para los próximos dos años.

Los equipos que necesitan llevar a cabo estos planes ya están comprometidos. Los CMO, CDO y CPO dicen que tienen relaciones laborales muy efectivas con:

- Director de datos (41%).
- Equipo de análisis de datos de clientes (41%).
- Equipo de seguridad (41%).
- Científico jefe de datos (40%).
- Director digital (40%).
- Equipo de privacidad (39 %).
- Equipo de desarrollo de productos (37%).
- Oficial de riesgos de marketing (37%).
- Los equipos DevOps (34%).
- Director de seguridad de la información (31%).

Los beneficios potenciales de una estrategia comercial que prioriza la privacidad son enormes para aumentar la lealtad del cliente, validar la autorización para usar datos y mejorar la satisfacción del cliente, pero el potencial de esfuerzos desarticulados también es enorme. Cuando las responsabilidades se superponen entre los directivos (CISO, CDO y CPO) se puede afectar el liderazgo frente a la gestión de datos y la protección de la privacidad. Con frecuencia la posición de CDO no existe, solo el 21% de las 2.500 empresas más grandes del mundo tienen un CDO a nivel ejecutivo senior, y estos se concentran en unos pocos sectores (Seguros, Banca y Medios y Entretenimiento) y regiones (América). El 42% de los CDO no son miembros del C-suite.

¿Cómo puedes gobernar y proteger los datos de tus clientes para que se mantengan privados y seguros para que la empresa los use? Comienza con el gobierno de los datos. Articula tus objetivos y comprende las diferentes responsabilidades y las posibles transferencias de información personal.

Llamado a la acción:

El CDO, CPO y CISO deben crear y trabajar con *playbooks* que les permitan cubrir todos los ángulos importantes de la seguridad y privacidad de los datos, incluyendo el gobierno, la accesibilidad y la exactitud.

Los CISO y CHRO están rompiendo paradigmas

La deserción es un problema creciente para el 39% de los CISO, CIO y CTO. Está obstaculizando el progreso de los objetivos de ciberseguridad en otro 15%.

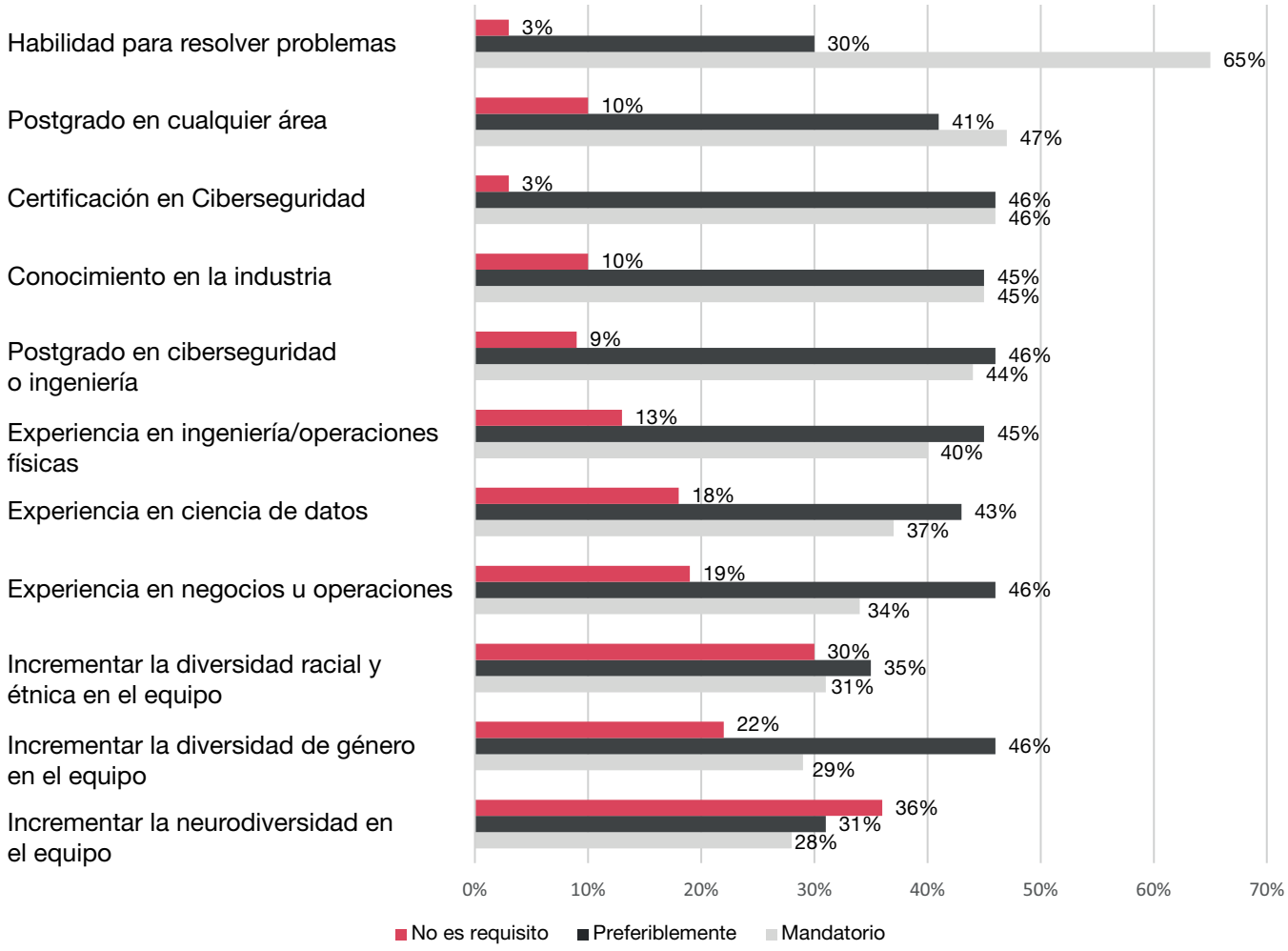
En respuesta, tal vez, los CISO y los CHRO están rompiendo paradigmas para ocupar puestos de ciberseguridad más rápido y retener el talento actual.

Están ampliando los parámetros de búsqueda para contrataciones más allá de las certificaciones y títulos profesionales, reconociendo que algunos rasgos, como las habilidades para resolver problemas, son al menos, igual de importantes.

Este nuevo pensamiento puede ampliar el grupo de candidatos. Un título universitario o posgrado, en cualquier área, ha superado a un título universitario en ciberseguridad, informática o ingeniería como requisito. Para alrededor del 10% ni siquiera se requiere.

Mientras tanto, se prefiere aumentar la diversidad de género cuando los candidatos son iguales en todas las demás calificaciones.

Gráfica 23: Características consideradas al momento de la contratación



Fuente: Digital Trust Insights 2023

Para ayudar a cerrar la brecha de talento, los CISO han descubierto que estos tres enfoques se encuentran entre los más efectivos:

- Mejora de las habilidades (45%).
- Incentivos de contratación, por ejemplo, bonos de inicio de trabajo (41%).
- Servicios gestionados para ciberseguridad (36%).

Protección de los servicios gestionados

El servicio de seguridad gestionada ocupa el segundo lugar después de la seguridad de la red como una de las principales prioridades de inversión para la ciberseguridad en 2023.

Así como el gasto y la dependencia de los proveedores de seguridad gestionada (MSP, por sus siglas en inglés) está ganando fuerza, también lo ha hecho la actividad maliciosa dirigida a los MSP. En mayo de 2022, las autoridades de ciberseguridad del Reino Unido, Australia, Canadá y Estados Unidos emitieron un aviso conjunto a las empresas para protegerse en medio de esta tendencia.

Aproximadamente la mitad de los CISO manifiestan que han implementado completamente una serie de medidas para administrar sus riesgos de terceros.

El 57% informa que deshabilitó las cuentas de MSP que ya no administran la infraestructura. El 45% aplica la autenticación multifactor en todos los servicios y productos, pero queda más trabajo, ya que solo el 2,2% ha implementado todas estas prácticas de seguridad en todos los ámbitos.

Mensaje a los CHRO

La rotación de empleados está aumentando en una variedad de mercados, mientras que los temores de una recesión están causando ansiedad en las empresas sobre los planes de contratación. En medio de la incertidumbre, es posible que se demoren en hacer cualquier cosa, especialmente cuando saben que necesitan probar algo nuevo para evitar la crisis en medio de los fenómenos descritos de diversas formas como el “gran replanteamiento”, la “gran renuncia” y el “abandono silencioso”.

Los CISO y los ejecutivos de riesgos deben ayudar a los CHRO a determinar los efectos y los riesgos operativos en cascada del desgaste de los empleados. Independientemente de las respuestas creativas que empleen las empresas para retener y contratar talento, los altos ejecutivos también deben ayudar a gestionar los riesgos reputacionales.

Llamado a la acción:

Pregunta qué habilidades realmente necesitas en tu programa de ciberseguridad, actualiza tu proceso de selección y brinda a tu talento incentivos y caminos de crecimiento que generen razones para quedarse. Tu dependencia en servicios gestionados y otros recursos y servicios externos seguirá siendo fuerte, incluye controles, acuerdos de niveles de servicio y cláusulas de ciberseguridad en tus contratos.

Conclusiones:

Las defensas de ciberseguridad y privacidad pueden fortalecerse a través de los siguientes elementos:

- Incluir una estrategia de ciberseguridad que priorice los riesgos y vulnerabilidades de la empresa y ponderar los activos que son más valiosos para la organización.
- Diseñar un plan de resiliencia que afronte las disrupciones de manera eficaz integrando a todas las partes del negocio.
- Definir un presupuesto de ciberseguridad con base en la cuantificación de los riesgos de ciberseguridad.
- Integrar a la alta dirección en asuntos de ciberseguridad para identificar riesgos oportunamente.
- Mantener el desarrollo de habilidades en ciberseguridad para el equipo de tecnología, pero más importante, para los colaboradores en general.
- Comunicar, a través de informes y/o reportes, las incidencias de ciberseguridad interna y/o externamente para generar confianza con las partes interesadas.

Escenarios para ilustrar la necesidad de colaboración en el C-suite

¿Cómo pondrán a prueba, los escenarios que enfrentan las organizaciones en 2023, la capacidad de los altos ejecutivos para trabajar juntos en medio de la crisis y evitar interrupciones comerciales?

Un ciberataque con altos impactos y compromiso de información sensible es un escenario crítico que las organizaciones consideran para fortalecer sus capacidades de resiliencia para este año.

Es la preocupación número uno casi unánime. Solo los directores financieros lo clasificaron en segundo lugar, después de la recesión mundial y junto con las preocupaciones sobre otra crisis de salud, como el resurgimiento del COVID-19.

Estos escenarios requieren que el C-suite y la alta dirección trabajen juntos, pero la ciberseguridad puede ser el único problema que requiere todas las manos para resolverlo, y uno sobre el cual una organización posiblemente tenga cierto control.

Este tipo de ataques pueden tener repercusiones catastróficas, poniendo a prueba la coordinación y respuesta con el C-suite. Dos tercios de los ejecutivos consideran que el delito de ciberseguridad es su amenaza actual más importante. Los ciberdelincuentes, que utilizan cada vez herramientas más sofisticadas y robustas, pueden perpetrar y orquestar una variedad de ataques, poniendo en riesgo incluso la supervivencia de la organización.
La ciberdelincuencia como servicio y herramientas estandarizadas permiten a los delincuentes perpetrar y orquestar una variedad de ataques rentables. Las operaciones de *ransomware*, por ejemplo, ahora se ejecutan como empresas en las que el operador principal “arrienda” el *ransomware*. Luego, los ciberdelincuentes pueden implementar *ransomware* arrendado a gran escala en múltiples objetivos.

A partir de 2021, el grupo *PwC Threat Intelligence* también vio más “intendentes comerciales “ o empresas que venden herramientas de ciberdelincuencia como spyware, exploits de día cero y otros tipos de *malware* a más clientes, en múltiples países.

Estas operaciones globales facilitan el inicio de una vida de ciberdelincuencia: los actores de amenazas ya no necesitan desarrollar su propio malware. Al mismo tiempo, el malware distribuido dificulta la identificación de los culpables.
Estas herramientas disponibles comercialmente son efectivas contra una amplia gama de objetivos, incluidos, quizás, funcionarios gubernamentales y ejecutivos del sector privado. Las organizaciones que han considerado este tipo de amenazas fuera de su ámbito deben replantear esa postura.

Escenarios para ilustrar la necesidad de colaboración de C-suite

Hemos seleccionado 3 de los tipos de eventos de ciberseguridad más preocupantes para los altos ejecutivos. Aunque las tácticas y técnicas asociadas a estos escenarios pueden requerir experiencia técnica para su comprensión integral, hay algo que debería quedar claro: las consecuencias de este tipo de incidentes en las áreas de operaciones, finanzas, datos y gestión de riesgos debe ser administradas.

El llamado a la acción para cada ejecutivo del C-suite no pretende ser obligatorio. En su lugar, ilustra los diversos ángulos que podrían necesitar ser abordados para una respuesta completa y duradera ante un ataque. En ciberseguridad, un ejecutivo desconectado es un punto de falla.

Escenario 1: Ataques basados en la nube

En la mesa: CISO + CIO +CTO + CDO + Alta dirección.

El 38% espera ataques más graves a través de la nube en 2023

La brecha: los atacantes explotan una configuración incorrecta en una aplicación de Internet alojada en la nube de una empresa y roban datos de usuarios para venderlos en el mercado negro.

Consecuencias:

Notificaciones costosas a los propietarios de los datos. Una posible demanda colectiva contra la empresa. Daño a la reputación de la empresa.

Lo que salió mal:

Seguridad inadecuada, ausencia de defensa en profundidad, errores de codificación, pruebas inadecuadas a desarrollos y librerías, y datos cifrados incorrectamente.

Cómo trabajar juntos para una mejor defensa:

- **CIO:** Debe habilitar DevSecOps en el desarrollo de aplicaciones, así como en pruebas exhaustivas previas al lanzamiento. También, corregir las configuraciones incorrectas tanto de los usuarios como de despliegues automatizados.
- **CISO:** Debe establecer y hacer cumplir políticas y procedimientos para asegurar aplicaciones y datos, pruebas de vulnerabilidad y penetración, aplicación de parches regulares, monitoreo continuo de cumplimiento, y monitoreo de incidentes y eventos de seguridad (SIEM).
- **CTO:** Debe pedir que los proveedores de servicios en la nube y terceros proporcionen reportes y herramientas para detectar errores de configuración en sus ambientes.
- **CDO:** Debe confirmar que las aplicaciones cumplan con los requisitos de privacidad y que los datos de los clientes están repartidos y cifrados para una mejor protección. Implementar soluciones que cifren datos en reposo, en tránsito y mientras están en uso.

Escenario 2: Ataques a la tecnología operativa

En la mesa: CISO + CRO + COO + CTO + CIO.

El 29% de las grandes organizaciones espera un aumento en los ataques OT

La brecha: un sistema de fabricación se ve afectado por un evento de *ransomware* debido a las vulnerabilidades explotables que existen en sistemas heredados.

Consecuencias:

La producción se detiene cuando los sistemas afectados se apagan para evitar que se propague el daño. Los impactos se propagan a través de la cadena de suministro.

Lo que salió mal:

Los piratas informáticos explotan vulnerabilidades para inyectar *ransomware*. Las vulnerabilidades afectadas se corrigieron previamente en los sistemas empresariales; sin embargo, debido a la falta de capacidades de administración de actualizaciones, monitoreo y detección en los sistemas heredados, las vulnerabilidades permanecieron sin detectar.

Cómo trabajar juntos para una mejor defensa:

- **CIO:** En conjunto con el CISO y el CTO, deben mapear las convergencias y las interdependencias críticas entre los sistemas de TI y OT.
- **CISO:** Debe trabajar con el CIO y el CTO para exigir la separación de TI y OT, desarrollar una zona de aterrizaje *(landing zone)* segura que proteja a OT del acceso directo y capacitar a los empleados sobre el acceso adecuado y los roles en la respuesta a incidentes.
- **CTO:** Junto al CISO y CIO, deben crear un plan para actualizar y monitorear dispositivos finales.
- **CRO:** Deben desarrollar la metodología para evaluar el riesgo de ciberseguridad en el entorno OT. Aquí se deben incluir escenarios y ensayar los procedimientos de respuesta a incidentes que unen los procesos de respuesta de TI y OT.
- **COO:** Debe considerar la ciberseguridad en el proceso de adquisición de sus sistemas de control industrial, en la contratación con proveedores de la nube y en la definición de acuerdos de servicio con proveedores de servicios externos.

Escenario 3: Ransomware

En la mesa: ¡Todos!

El 45% de los ejecutivos de seguridad y TI esperan un mayor aumento en los ataques de ransomware

La brecha: un empleado médico abre un documento en un correo electrónico de *phishing* y activa el *malware*.

Consecuencias:

Interrupción del servicio y cierre casi total de las redes.

Lo que salió mal:

El software antivirus se estaba quedando sin reglas actualizadas que no detectaban el *malware* incrustado en el archivo adjunto malicioso. La falta de autenticación multifactor permitió a los atacantes obtener acceso inicial. Inadvertidos en la red corporativa durante ocho semanas, los ciberdelincuentes realizaron un reconocimiento de la red y finalmente comprometieron una cuenta de administrador de dominio, lo que les otorgó privilegios elevados para lanzar *malware* que cerró gran parte de la infraestructura de TI central y comprometió las copias de seguridad.

Cómo trabajar juntos para una mejor defensa:

- **CEO:** Debe apoyar la formación en concientización en ciberseguridad en toda la organización.
- **CIO:** Debe revisar las conexiones entre los sistemas de TI y la infraestructura médica.
- **CTO:** Debe evaluar la vulnerabilidad de los dispositivos médicos en un escenario que esté dirigido a su afectación.
- **COO:** Debe ayudar al CIO y al CISO a evaluar los efectos en la seguridad del paciente.
- **CISO:** Debe cerrar las brechas de seguridad entre TI y los servicios de salud.
- **CDO:** Junto al COO, CISO, CPO deben evaluar el daño por robo/corrupción de datos de pacientes.
- **CRO:** Debe realizar pruebas de resiliencia con equipos de crisis y BC/DR.
- **CFO:** Debe trabajar junto al CISO, CIO en cualquier divulgación a los reguladores y al público. Revisar el gasto de ciberseguridad, incluido el seguro, con el CISO y el CIO a la luz de las vulnerabilidades descubiertas, y definir la política para el pago de *ransomware*.
- **Comité directivo:** Debe obtener información sobre los ejercicios y simulaciones de la administración para prepararse frente a un ataque de *ransomware*, y confirmar los protocolos para informar al comité directivo sobre un incidente de ciberseguridad o un ataque de *ransomware*.

Para ver un ejemplo de una revisión posterior al incidente de un evento de ransomware, consulte el ciberataque de Conti en el HSE.

Sobre la encuesta:

2023 Global Digital Trust Insights es una encuesta de 3.522 ejecutivos de negocios, tecnología y seguridad (CEO, directores corporativos, CFO, CISO, CIO y C-Suite Officers) realizada en julio y agosto de 2022. Las mujeres ejecutivas representan el 31% de la muestra.

El 52% de los encuestados son ejecutivos de grandes empresas (ingresos de mil millones de dólares o más). El 16% está en empresas con $10 mil millones o más en ingresos.

Los encuestados operan en una variedad de industrias: Fabricación industrial (24%), Tecnología, Medios, Telecomunicaciones (21%), Servicios financieros (20%), Mercados minoristas y de consumo (18 %), Energía, Servicios públicos y recursos (9%), Salud (5%), y Gobierno y servicios públicos (3%).

Los encuestados se encuentran en varias regiones: Europa occidental (31%), América del Norte (28%), Asia Pacífico (18%), América Latina (12%), Europa del Este (5%), África (4%) y Medio Este (3%).

La Encuesta Global Digital Trust Insights se conoce formalmente como la Encuesta Global sobre el Estado de la Seguridad de la Información (GSISS).

Referencias

Conti cyber attack on the HSE. (2021, 3 diciembre). PwC. Recuperado 1 de febrero de 2023, de https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

Digital Security Risk Disclosure | Financial Reporting Council. (s. f.). https://www.frc.org.uk/investors/frc-lab/digital-security-risk-disclosure

Government of India. (2022). No. 20(3)/2022-CERT-In Government of India. En Ministry of Electronics and Information Technology (MeitY) (Electronics Niketan, 6 CGO Complex, New Delhi-110003). Recuperado 1 de febrero de 2023, de https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2022/05/CERT-In_Directions_70B_28.04.2022-2.pdf

PricewaterhouseCoopers. (s. f.-a). A privacy reset — from compliance to trust-building. PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/privacy-reset.html

PricewaterhouseCoopers. (s. f.-b). Best performing businesses: COVID-19 and digital transformation. PwC. https://www.pwc.com/us/en/services/alliances/library/best-performing-businesses-covid-19-digital-transformation.html

PricewaterhouseCoopers. (s. f.-c). Cyber breach reporting to be required by law for better cyber defense. PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/cyber-breach-reporting-legislation.html

PricewaterhouseCoopers. (s. f.-d). Evolución de la ciberseguridad en la era digital PwC Colombia. PwC. https://www.pwc.com/co/es/pwc-insights/evolucion-ciberseguridad.html

PricewaterhouseCoopers. (s. f.-e). How CISOs and boards can prepare for the new era of cyber transparency. PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/sec-cyber-proposed-disclosure.html

Protecting Against Cyber Threats to Managed Service Providers and their Customers | CISA. (2022, 11 mayo). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-131a

PwC US. (2022, septiembre). The next move. Regulatory and policy developments in tech. Recuperado 1 de febrero de 2023, de https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/assets/pwc-next-move-regulatory-and-policy-developments-in-tech-september-2022.pdf

Agradecimientos y créditos

Agradecimientos:
Carolina Forero
Amparo Monrabal Pacheco

Redacción:
Natalia Andrea Galindo
Mauricio Arias

Diagramación:
Sharon Sierra
Nicolás Castillo Diaz

Edición de textos y revisión de estilo:
Maria de los Ángeles Mejía
Erika Arias

Contactos

Mauricio Arias
Socio Consultoría en Tecnología
mauricio.arias@pwc.com

Juan Carlos Malagón
Socio de Marketing & Sales
juan.malagon@pwc.com

Mauricio Fernando Sánchez
Gerente de Consultoría en Ciberseguridad y Privacidad
mauricio.m.sanchez@pwc.com