Digital Trust Insights

PwC Interaméricas

La creciente digitalización en las empresas, los efectos de la pandemia y las disrupciones de los últimos años han dejado en evidencia la necesidad de una estrategia de ciberseguridad aplicable a toda la organización, desde las partes administrativas hasta las operativas, junto con todo el equipo de liderazgo. Con cada cambio, vienen nuevos riesgos cibernéticos, los cuales requieren de la unión de fuerzas con C-suites, quienes reconocen que el progreso de sus compañías incrementa la exhibición de sus activos digitales y que esto va más allá del cumplimiento de una potencial legislación en ciberseguridad.

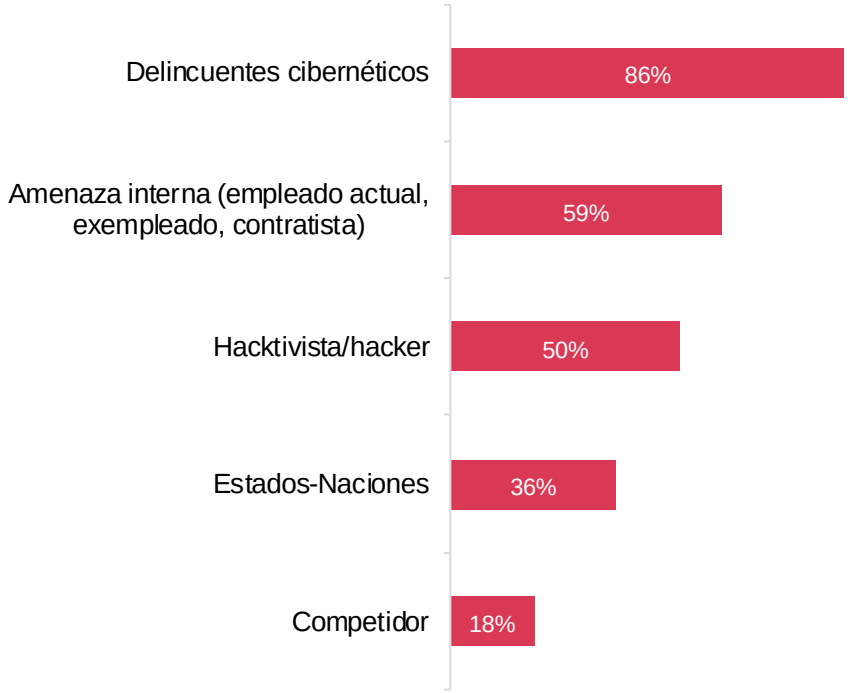
PwC a nivel global ha estudiado por 20 años el estado de la ciberseguridad y la privacidad de las empresas. En esta ocasión, la encuesta Digital Trust Insights 2023 entrevistó —entre julio y agosto del 2022 a ejecutivos de Interamericas de las áreas de tecnología, información, finanzas, seguridad de la información, así como directores generales. A continuación, presentamos los principales hallazgos obtenidos de este estudio.

1 Principales preocupaciones de los ejecutivos

Las organizaciones a nivel global se enfrentan a una cantidad de amenazas cada vez mayor. Éstas amenazas fueron separadas por actores, vías y tipos de ataques y gracias a los ejecutivos encuestados, hemos identificado cuáles son los que podrían tener un rol más predominante en el siguiente año:

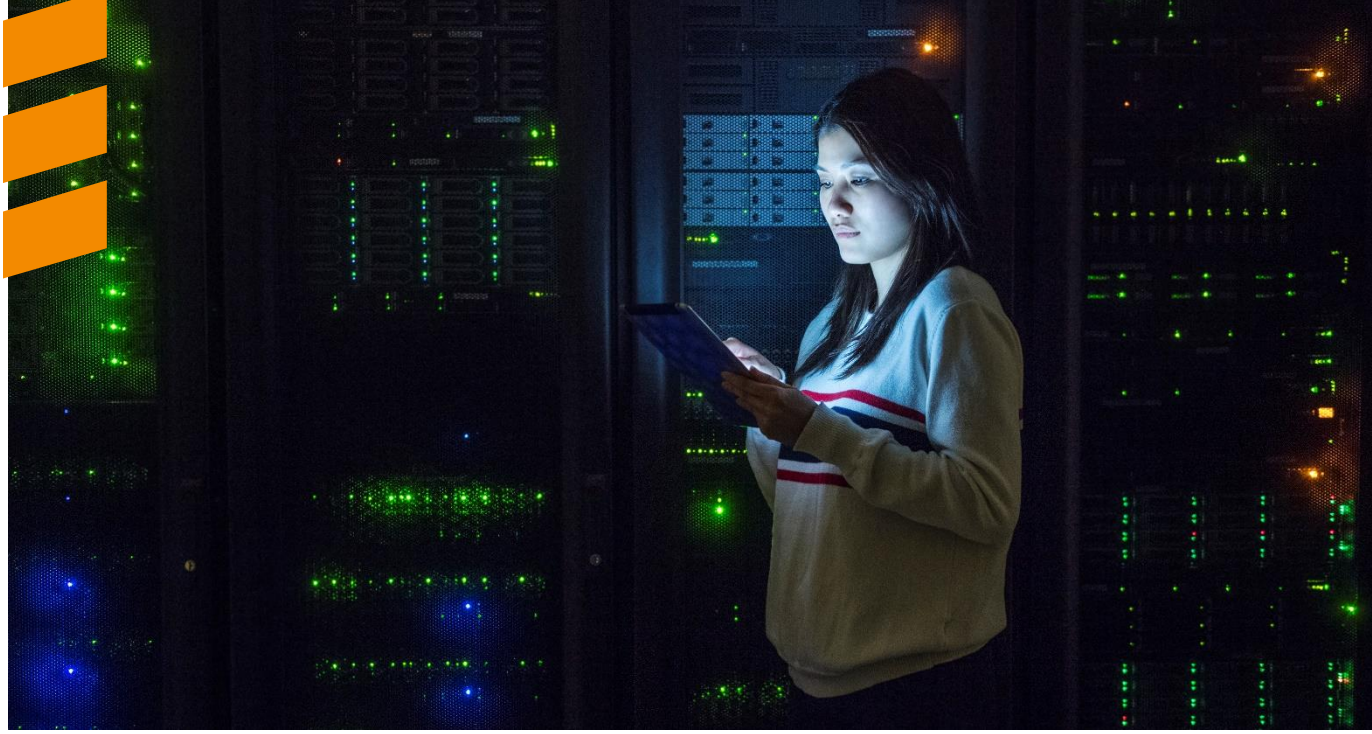
Actores de riesgo

La encuesta global nos indica que los delincuentes cibernéticos (65%), hackers (48%) y amenazas internas (44%) son los actores que se espera puedan ocasionar un riesgo para organizaciones alrededor del mundo. Para nuestra región los resultados son muy similares:



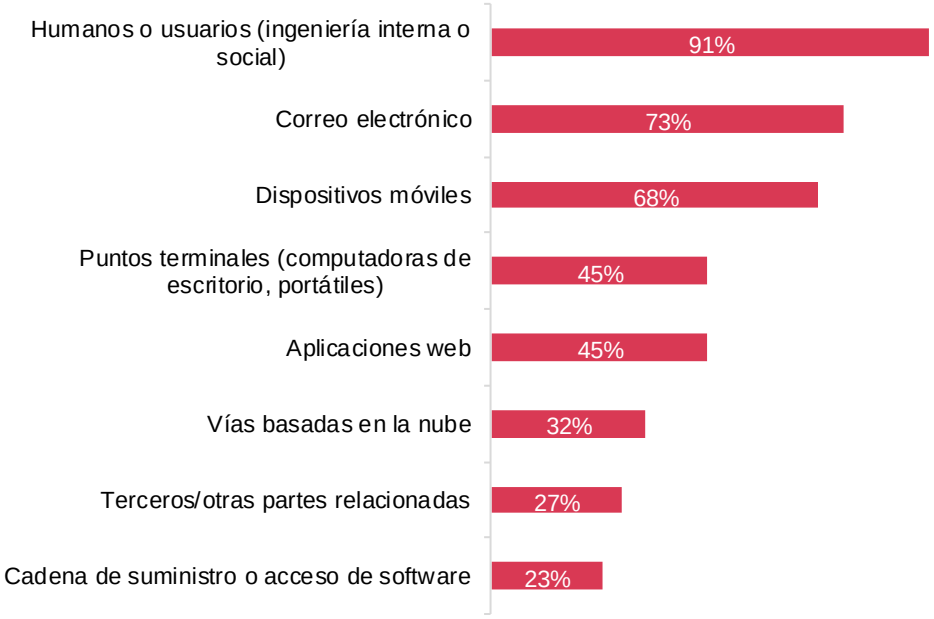
De cada uno de los siguientes actores de amenaza, ¿cuál(es) espera que afecte(n) significativamente a su organización en 2023 en comparación con 2022?

Fuente: Encuesta Regional Digital Trust Insights 2023 de PwC Interaméricas.



Vías de riesgo

Las vías de riesgo son los canales por donde se pueden presentar ataques en las organizaciones, en el estudio se concluyó que las vías que deben tener mayor cuidado a nivel global son: dispositivos móviles (41%), correo electrónico (40%) y vías basadas en la nube (38%), en este caso, la lista para la región fue bastante diferente:



De todas las maneras en los adversarios pueden acceder a sus sistemas, seleccione la(s) que espera que afecte(n) de manera significativa a su organización en 2023 en comparación con 2022. Fuente: Encuesta Regional Digital Trust Insights 2023 de PwC Interaméricas.

Podemos ver como la mayor vía de riesgo en nuestra región es la vía humana o por usuarios (91%), la cual estuvo en la quinta posición en los resultados globales. También vemos como las vías basadas en la nube no entran en el top 5 de preocupaciones a nivel regional, mientras que a nivel global son la tercera. Nuevamente se evidencia que en nuestra realidad las personas continúan siendo un riesgo importante de ciberseguridad y existe una mayor preocupación por una amenaza interna que por un hacktivista o hacker externo.

Tipos de ataques

A nivel global las preocupaciones más predominantes son: delincuentes cibernéticos (65%), dispositivos móviles (41%), correo electrónico (40%) y vulnerabilidades de servicios de sistemas en la nube (38%). Para el caso de nuestra región, lo más preocupante sigue siendo los delincuentes cibernéticos (54%), mientras que los otros de la lista son: amenazas internas (50%), ingeniería social (40%), ransomware (36%), dispositivos móviles (27%) y correo electrónico (27%).

Cabe destacar que en nuestra región las personas siguen siendo el punto más vulnerable y crítico de atender tanto desde el punto de vista interno (personal interno) como externo (ingeniería social).

2 Progreso en la ciberseguridad desde el 2020

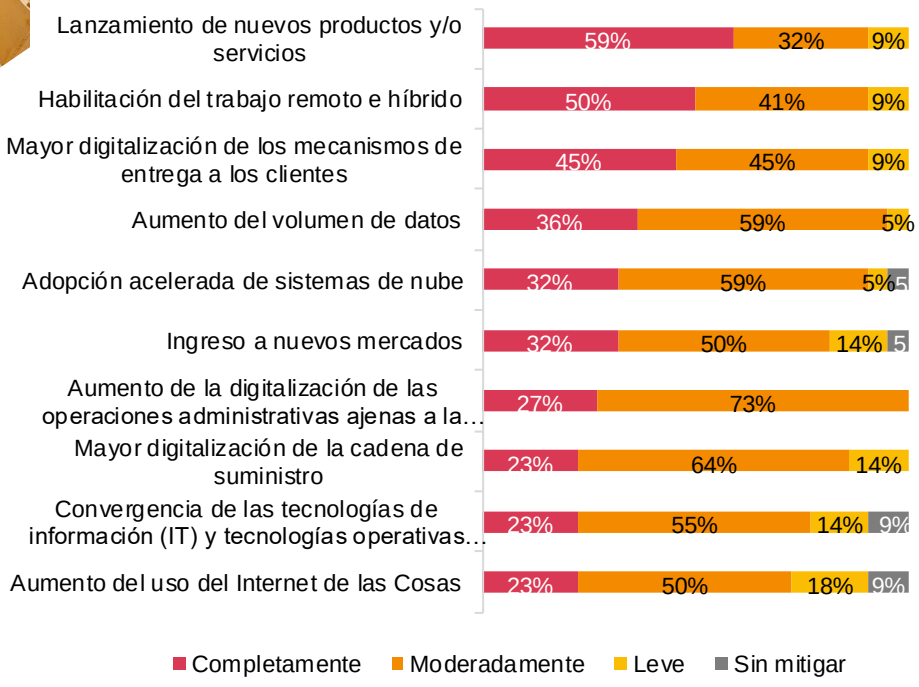
El creciente panorama digital trae a su vez la exposición de los activos digitales de las empresas. Es importante mantener las defensas a través de una estrategia de ciberseguridad que brinde resiliencia y pueda adaptarse a las nuevas amenazas.

La ciberseguridad organizacional no es algo que funcione por un período de tiempo definido, con las crecientes adversidades, es necesaria una permanente revisión y actualización del programa para así estar preparado ante una posible amenaza.

Mitigaciones

Más del 80% de los negocios y ejecutivos de tecnología entrevistados vieron mejoras en cuanto a ciberseguridad de su empresa este año — gracias a inversiones cumulativas y colaboración de los C-suite. Más de un 18% reportó progreso en las 10 áreas que identificamos como críticas para la madurez cibernética.

Para la región, el 9% de los encuestados dice haber mitigado completamente los riesgos que se presentaron desde el año 2020. En comparación, a nivel global tan solo el 3% asegura haber mitigado dichos riesgos.



Indique si el equipo de ciberseguridad de su organización ha logrado lo siguiente en los últimos 12 meses
Fuente: Encuesta Regional Digital Trust Insights 2023 de PwC Interaméricas.

El lanzamiento de nuevos productos (59%) y la habilitación de trabajo remoto (50%) captaron la mayor atención, en comparación, a nivel global fueron la habilitación de trabajo remoto (38%) y la adopción acelerada de sistemas en la nube (35%). Menos del 10% de los encuestados dicen haber mitigado completamente los 10 riesgos. Más del 13% dice no haber mitigado al menos uno de los riesgos.

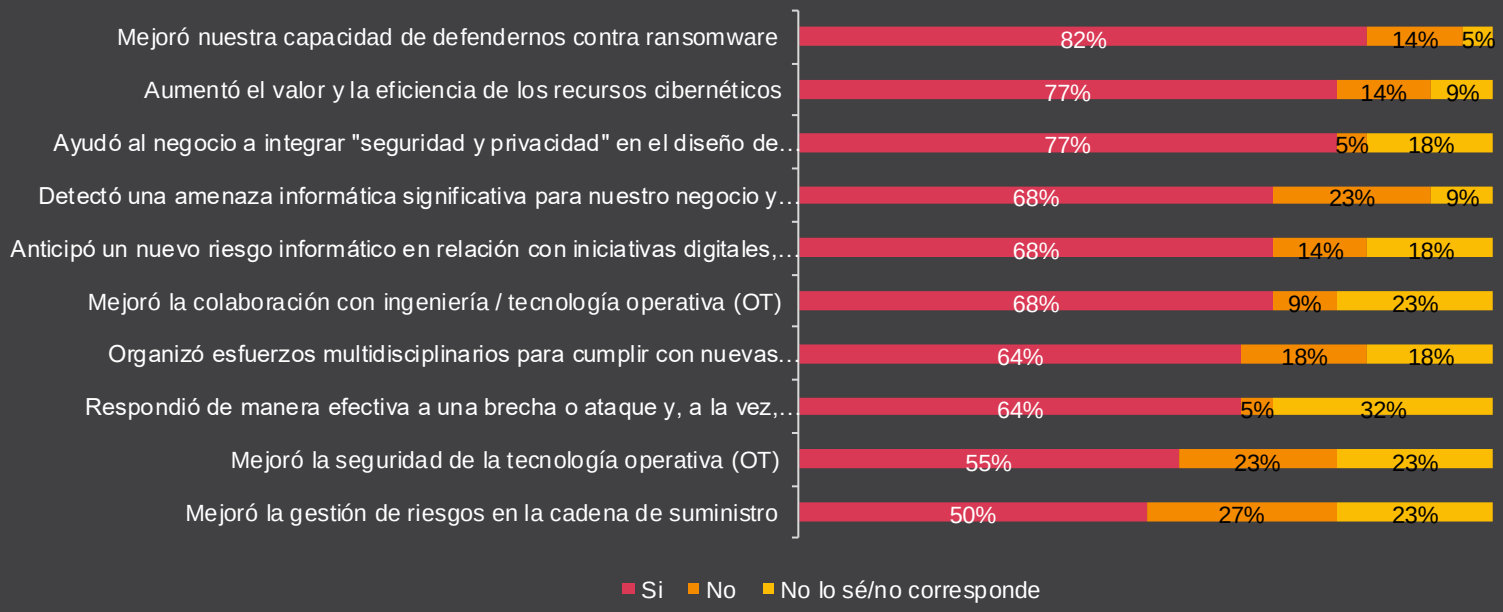
La adopción de la nube es uno de los elementos más importantes para la generación de ingresos a mediano plazo, ya que esta es la forma de crear modelos de negocio digitales. Sin embargo, esta debe ser acompañada de una buena estrategia de ciberseguridad ya que genera una mayor exposición de los activos digitales.

Logros en ciberseguridad

Para cada organización, es importante que su estrategia de ciberseguridad cumpla con los objetivos que se identifiquen como necesarios.

A nivel global se identificaron los 10 objetivos más críticos para éstas y se consultó a los ejecutivos acerca del progreso en estos. A continuación, los resultados:

El 26% de los encuestados a nivel global, asegura que su equipo de ciberseguridad ha cumplido con las 10 metas que identificamos como críticas para mejorar en 2022. A nivel regional, tan solo el 18% dice haberlas cumplido. Las 3 metas que más cumplieron las empresas encuestadas a nivel global fueron: mejorar la seguridad de la tecnología operativa (79%), mejorar nuestra capacidad de defendernos contra ransomware (77%) y ayudar al negocio a integrar “seguridad y privacidad” en el diseño de nuevos productos y servicios (75%).

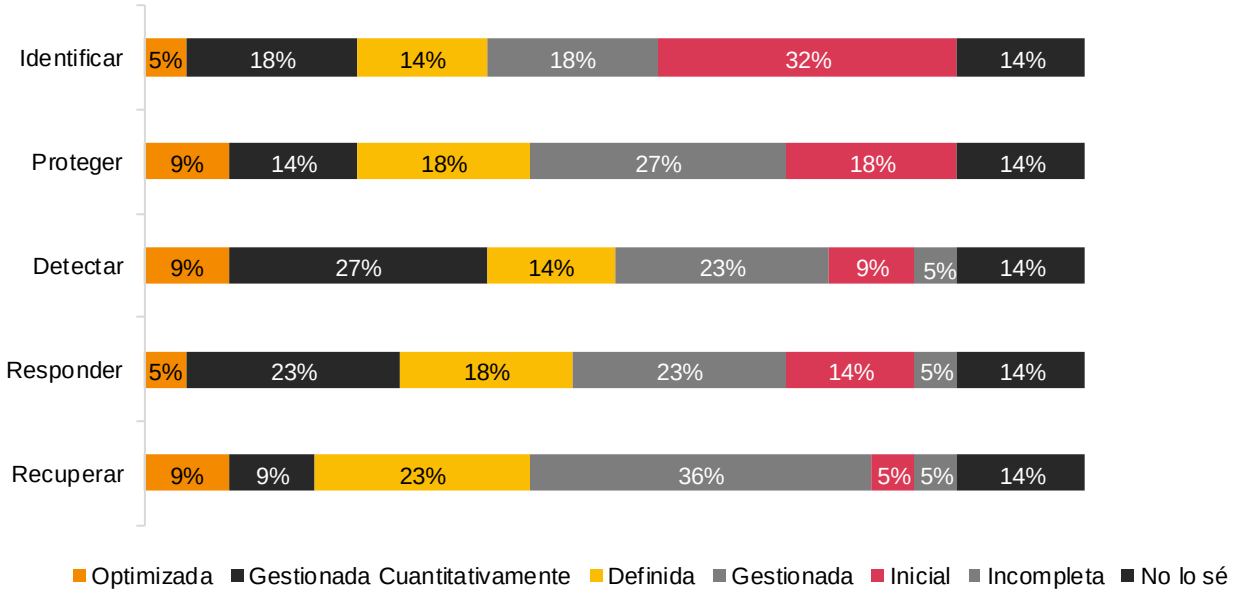


Indique si el equipo de ciberseguridad de su organización ha logrado lo siguiente en los últimos 12 meses

Fuente: Encuesta Regional Digital Trust Insights 2023 de PwC Interaméricas.

Las metas siguen creciendo

La digitalización hace que la seguridad sea asunto de todos. El futuro promete sistemas más conectados con una cantidad de datos exponencialmente mayor y adversarios más organizados, es decir mayores riesgos. Como mitigación de estos riesgos el National Institute Institute of Security and Technology (NIST) de los Estados Unidos en su Cybersecurity Framework describe 5 capacidades cibernéticas que son críticas para tener una buena estrategia de ciberseguridad, consultamos a los ejecutivos de diferentes organizaciones en la región hasta qué punto lograron implementar dichas capacidades en sus empresas. Estos fueron los resultados:



Pensando en sus capacidades de ciberseguridad, indique qué tan madura es su organización en cada una de las siguientes áreas. Piense en cada área en su totalidad, considerando las áreas individuales de capacidad que se encuentran dentro de la categoría.

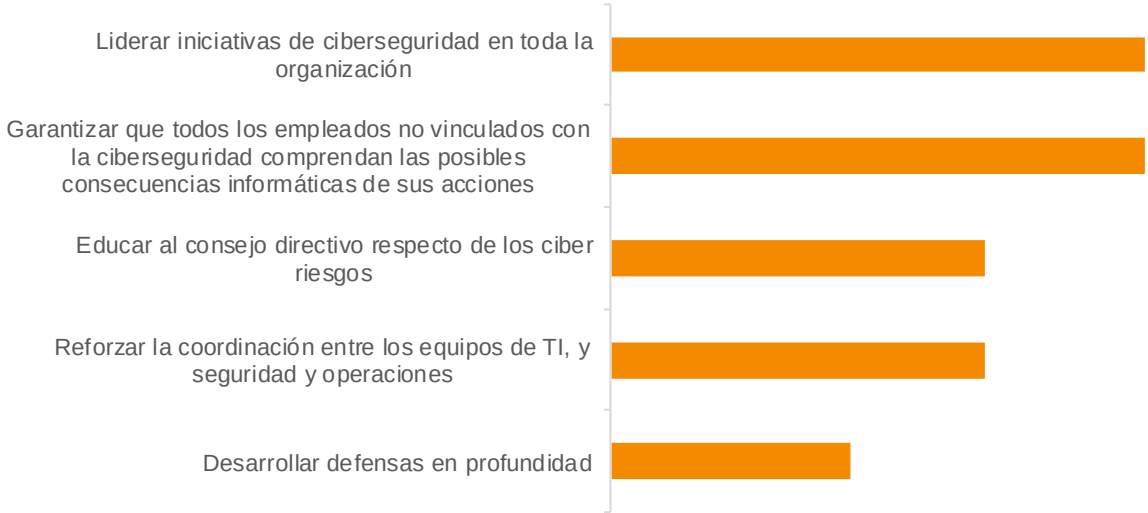
Fuente: Encuesta Regional Digital Trust Insights 2023 de PwC Interaméricas.

Solo el cuatro por ciento respondió que lograron optimizar las cinco, muy parecido al tres por ciento a nivel global. Sin embargo, a nivel global se obtuvo un mayor porcentaje de optimización en cada una de estas capacidades; identificar (17%), proteger (21%), detectar (22%), responder (22%) y recuperar (24%).

Metas de las organizaciones

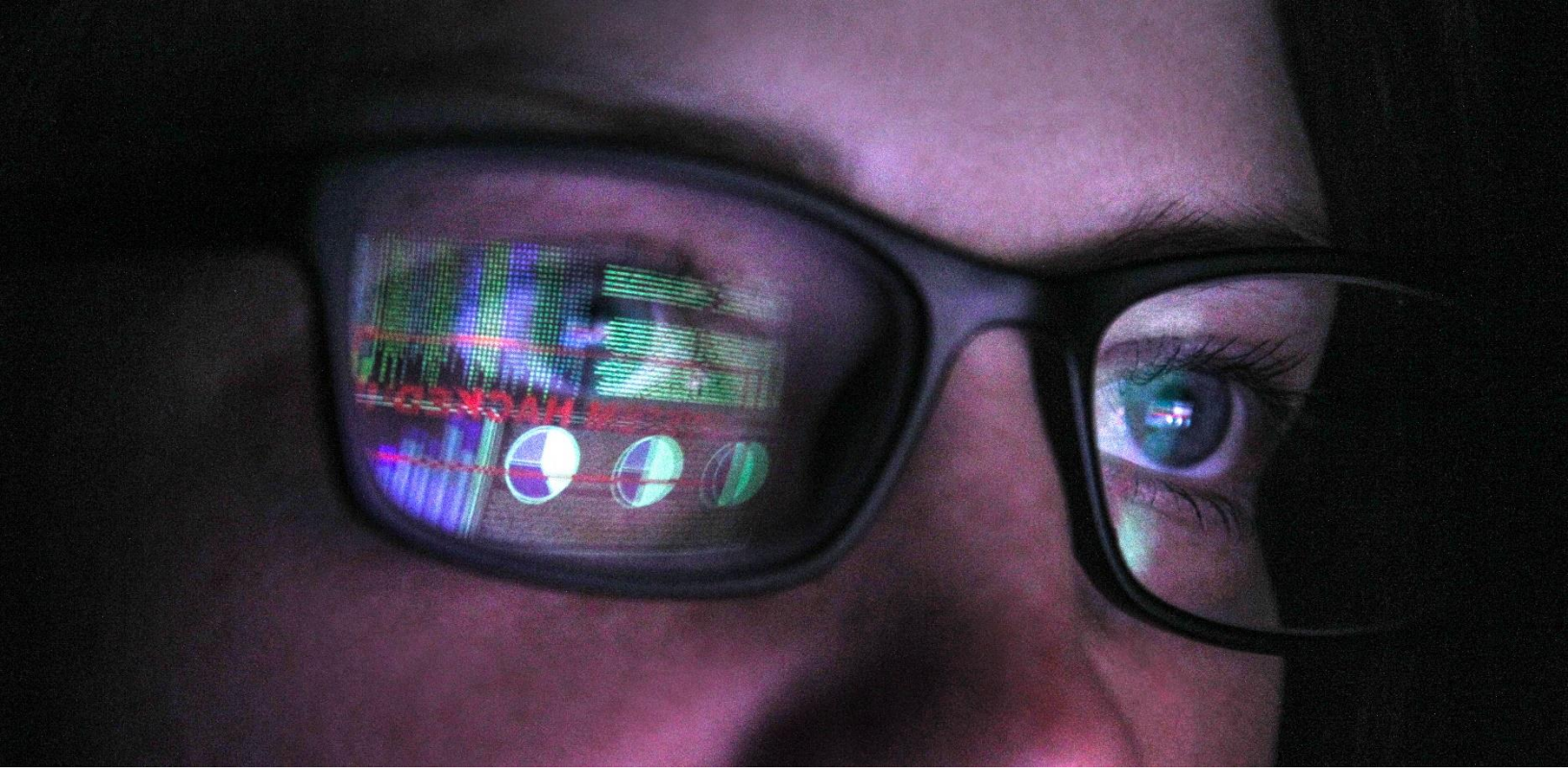
Tener una buena estrategia de ciberseguridad es crítica para poder ver una mejora en la eficiencia de los recursos y la preparación ante un posible incidente, por ende, es importante que las organizaciones tengan claro los protocolos a implementar para estar más protegidas.

Diferentes organizaciones aseguran que el liderar iniciativas de ciberseguridad en toda la organización y garantizar que todos los empleados no vinculados con la ciberseguridad comprendan las posibles consecuencias informáticas de sus acciones es lo que tendrá mayor impacto en cuanto a transformación de ciberseguridad para 2023.



Desde su punto de vista, ¿cuáles de las siguientes opciones tendrán mayor impacto en la transformación de la ciberseguridad de su organización en los próximos 12 a 18 meses?

Fuente: Encuesta Regional Digital Trust Insights 2023 de PwC Interaméricas.



Con las crecientes preocupaciones de los ejecutivos en cuanto a ataques por medio de ingeniería social o amenazas internas, es importante que todos los empleados comprendan los posibles riesgos y la responsabilidad que deben tener para cuidar los activos digitales de la organización. También es esencial que los ejecutivos de la alta dirección sean líderes que impulsen la ciberseguridad en toda la organización. Estos junto con el CISO, pueden generar un plan de resiliencia que identifique los puntos críticos de la organización ante disrupciones.

El éxito de una estrategia de ciberseguridad dependerá, en gran medida, del liderazgo del CISO, pues él es quien define las acciones que ayudan a mitigar los riesgos cibernéticos de forma efectiva.

Sin embargo, hay un camino desafiante para que los CISO de nuestra región tengan un rol más estratégico en la ciberseguridad. Nuestra experiencia en el mercado destaca que este rol ha sido más operacional y, en general, no es habitual en las empresas. Por ejemplo, el 27% de los encuestados dijo que el CISO es el responsable de coordinar la respuesta ante un incidente cibernético, pero solo el 18% señaló que el Chief Information Security Officer es el principal responsable de evaluar los riesgos de ciberseguridad asociados a las decisiones de negocio.

Además, el estudio reflejó que al menos la mitad de las organizaciones dicen que ninguno de los miembros del consejo ejecutivo tiene alguna experiencia en temas de ciberseguridad, lo cual genera un nuevo obstáculo para las labores deseables del CISO.

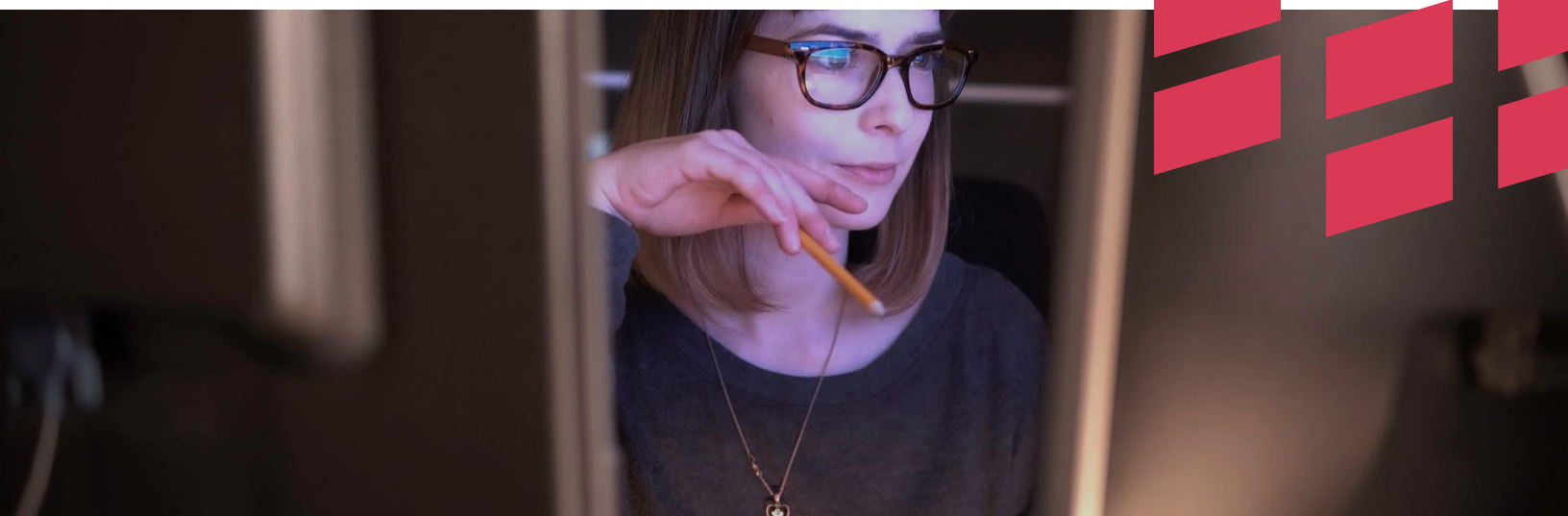
3 Transparencia y privacidad

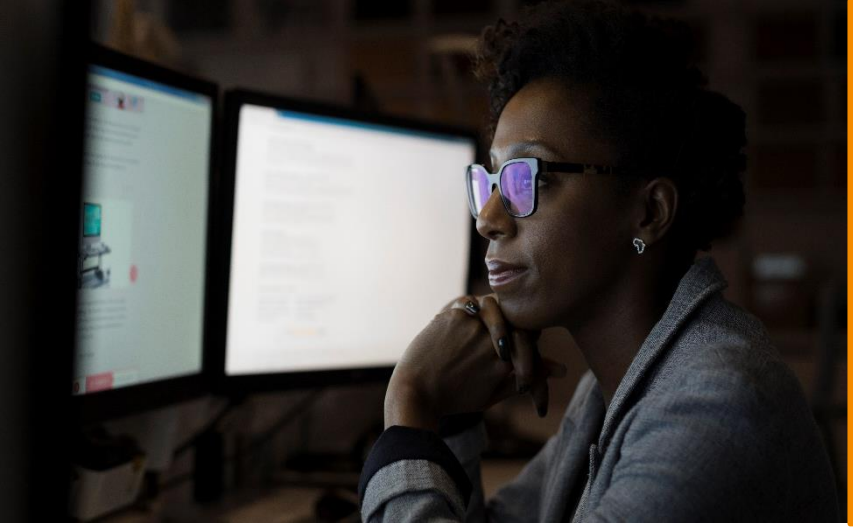
La transparencia y privacidad son elementos clave para establecer y mantener la confianza de los clientes e inversionistas en una organización. Es importante que las empresas implementen políticas claras y sólidas en estos temas para garantizar la privacidad de los datos de sus clientes y mantener una comunicación abierta y honesta con ellos. La transparencia permite a los clientes e inversionistas comprender cómo se manejan sus datos y cómo se toman las decisiones empresariales, mientras que la privacidad les garantiza que su información personal está segura. La combinación de estos dos aspectos es crucial para el éxito a largo plazo de una organización y para el fortalecimiento de la confianza en su marca.

También, la divulgación de incidentes cibernéticos es importante porque permite a las organizaciones y a la sociedad en general tomar medidas para protegerse contra futuros ataques. Al comprender los detalles de un incidente, las empresas pueden implementar medidas de seguridad más efectivas y estar mejor preparadas para enfrentar amenazas similares en el futuro. Además, la transparencia y la información compartida ayudan a construir confianza en la industria de la tecnología y a mejorar la conciencia sobre la seguridad en línea. En resumen, la divulgación de incidentes cibernéticos es crucial para mejorar la seguridad cibernética a nivel global.

¿En qué medida está de acuerdo o en desacuerdo con las siguientes afirmaciones con respecto a la capacidad de su organización de divulgar externamente prácticas, estrategias e incidentes de ciberseguridad?

Fuente: Encuesta Regional Digital Trust Insights 2023 de PwC Interaméricas.

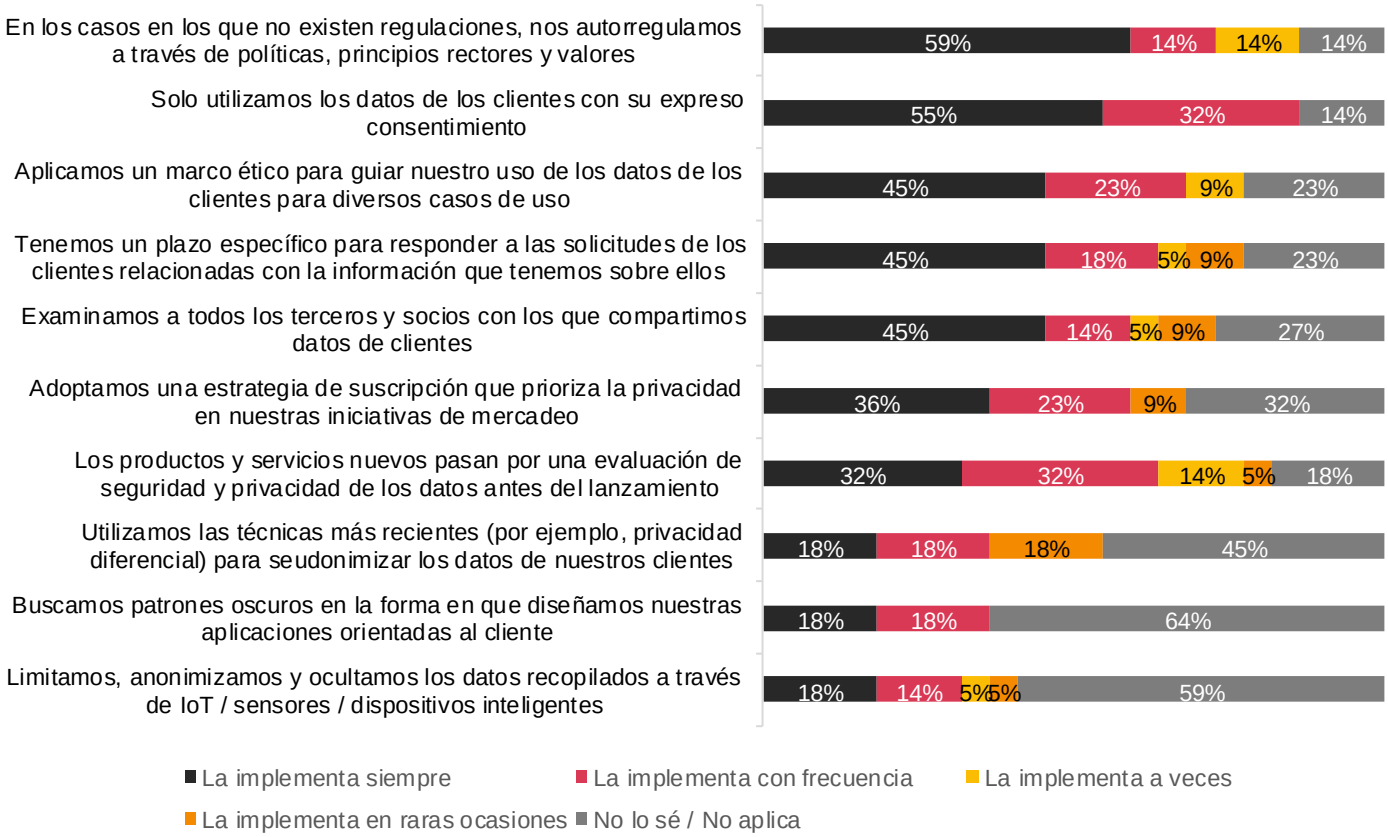




El 77% de los encuestados asegura que su organización es capaz de cumplir con las divulgaciones obligatorias de los ciber incidentes que requieren formatos comparables y coherentes son necesarias para ganarse la confianza de las partes interesadas, además, un 59% dice poder evaluar de manera efectiva la gravedad de un incidente informático con fines de informe.

La seguridad de datos y privacidad son la debilidad de muchas empresas, estos son aspectos críticos en el mundo digital y, a pesar de los esfuerzos por proteger esta información, muchas empresas todavía enfrentan desafíos en esta área. La cantidad de datos que se recopila y almacena digitalmente ha aumentado exponencialmente en los últimos años, lo que ha hecho que cada vez sea más difícil protegerlos adecuadamente.

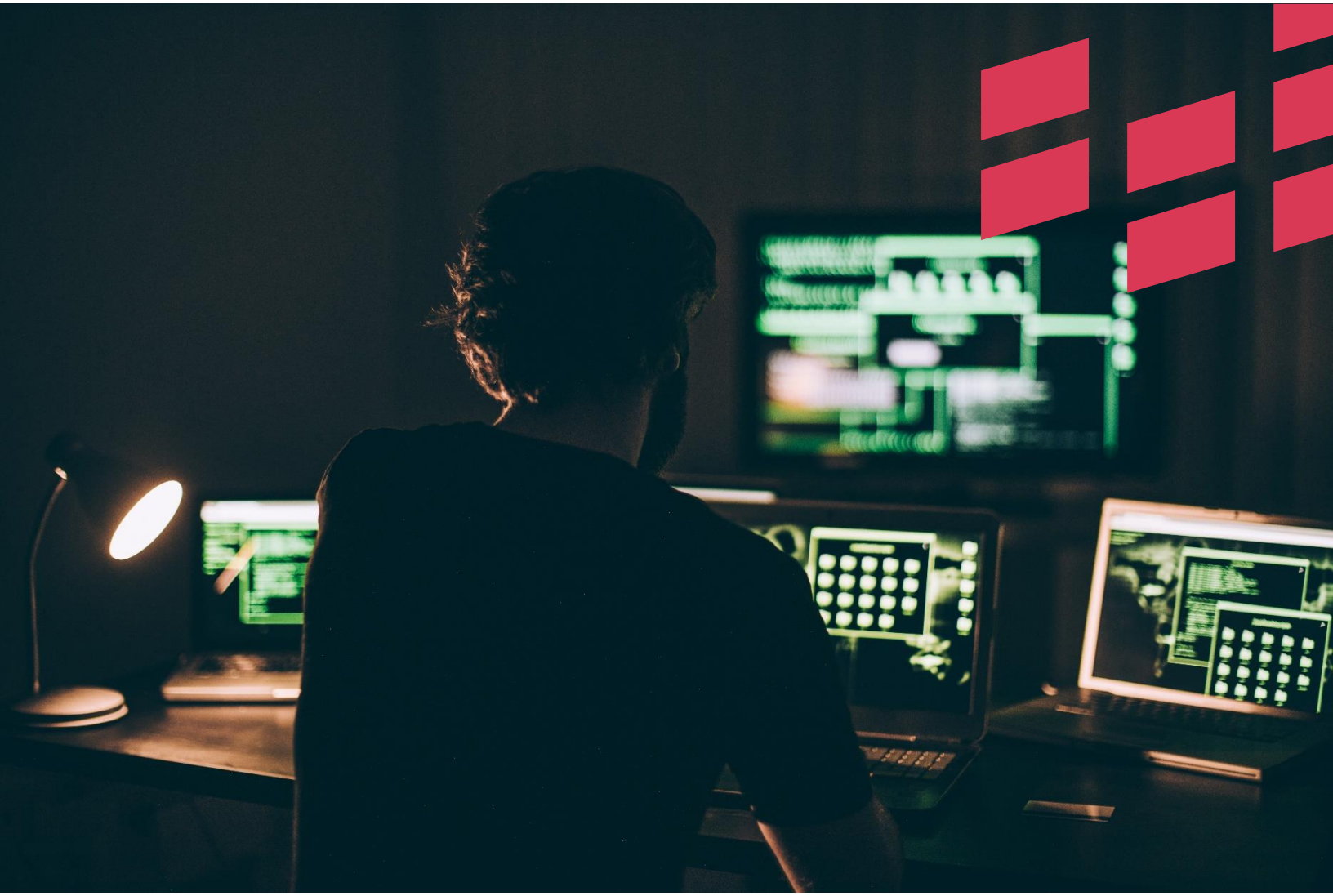
A nivel global, tan solo el 5% dice implementar todas estas prácticas y políticas, mientras que para la región es un 9%. A pesar de que las regulaciones respecto a ciberseguridad en la región no tengan el mismo nivel de madurez que otros países, es importante que se sigan estándares altos para así generar confianza con clientes, inversionistas y sociedad.



¿En qué medida su organización implementa las siguientes políticas y prácticas en relación con la gestión y el gobierno de los datos de los clientes?

Fuente: Encuesta Regional Digital Trust Insights 2023 de PwC Interaméricas.

Para nuestro territorio, la mayoría de las empresas aseguran autorregularse a través de principios rectores y valores y dicen solo usar los datos de los clientes con su expreso consentimiento, por ende, esto es uno de los puntos fuertes de la región. Sin embargo, queda mucho por hacer para proteger los datos de los clientes, tan solo el 18% asegura utilizar técnicas para seudonimizar los datos, buscar patrones oscuros en las aplicaciones para clientes y limitar y ocultar los datos recopilados a través de dispositivos inteligentes.

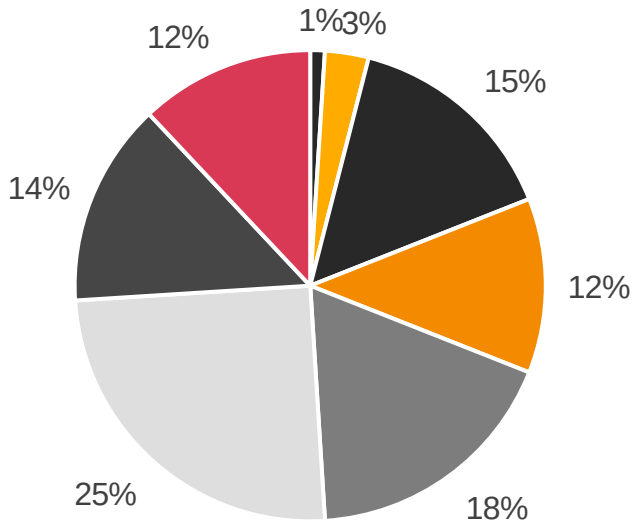


4 Presupuesto cyber

Un presupuesto en ciberseguridad debe ser adecuado con respecto a los riesgos y la exposición que presenten los activos digitales de las organizaciones, además, es importante que se tenga una buena estrategia de ciberseguridad que permita la utilización de los recursos de manera eficiente, para así cubrir el marco completo de protección en la empresa. A continuación, veremos cómo se encuentra el panorama de presupuestos en la región con respecto al global:

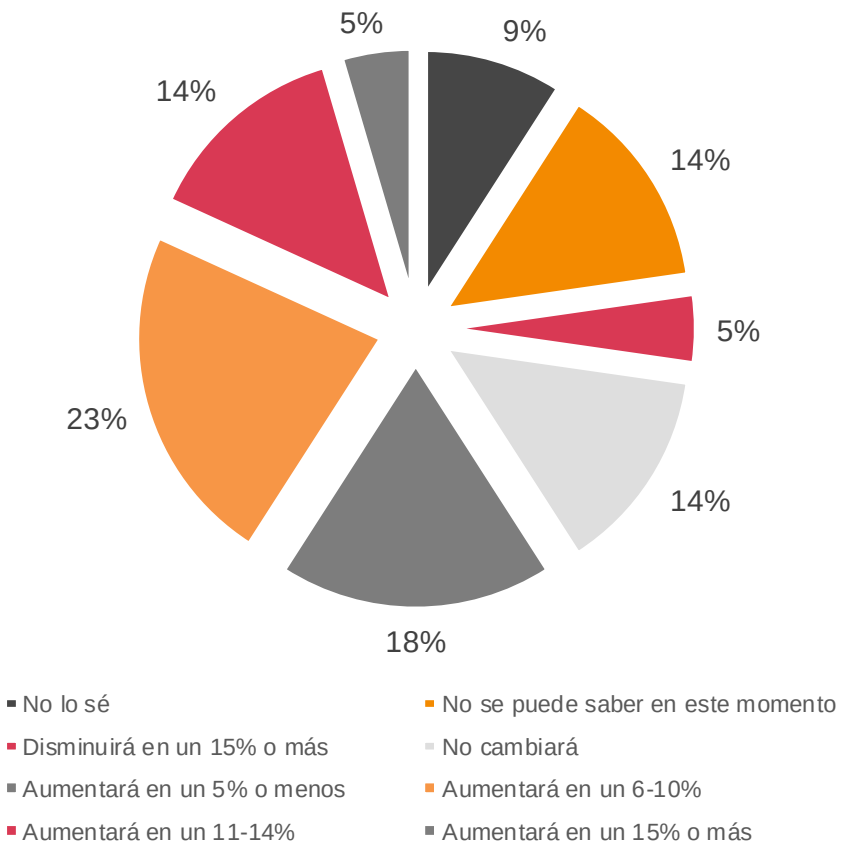
Las compañías continúan aumentando su presupuesto para ciberseguridad.

Sesenta por ciento de los ejecutivos de la región esperan ver un incremento, sin embargo, no es tanto como el 65% que se estima a nivel global. Por otro lado, tan solo un 5% de los encuestados en nuestro territorio asegura que su presupuesto para ciberseguridad disminuirá, a nivel global es un 15%.



Desde su punto de vista, ¿cuáles de las siguientes opciones tendrán mayor impacto en la transformación de la ciberseguridad de su organización en los próximos 12 a 18 meses?

Fuente: PwC 2023 Global Digital Trust Insights Survey.



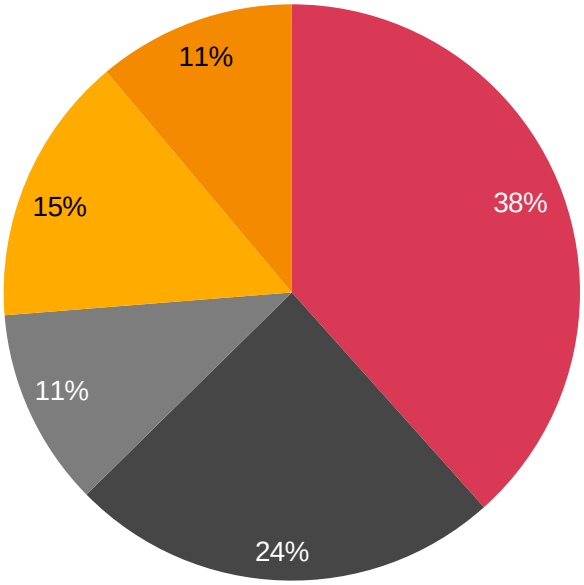
Desde su punto de vista, ¿cuáles de las siguientes opciones tendrán mayor impacto en la transformación de la ciberseguridad de su organización en los próximos 12 a 18 meses?

Fuente: Encuesta Regional Digital Trust Insights 2023 de PwC Interaméricas.

Un aumento en el presupuesto de ciberseguridad debe ser acompañado de una buena estrategia. En la región, un 82% asegura que mejoró su capacidad de defenderse contra ransomware y un 77% indica que aumentó el valor y la eficiencia de sus recursos cibernéticos.

¿Cómo se establecen los presupuestos para cyber?

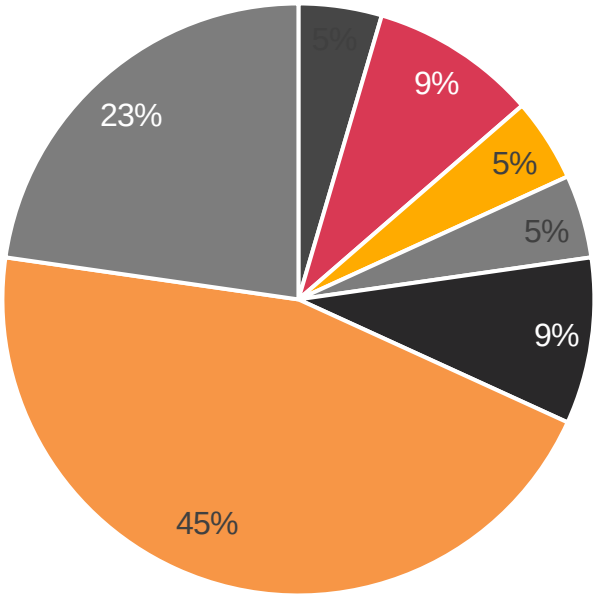
Es importante tener un criterio definido para dedicar los recursos adecuados a la ciberseguridad. Esto permitirá que se pueda tener una buena proporción entre los riesgos/exposición y los recursos disponibles para protegerse.



- Como un porcentaje de los gastos combinados en TI y automatización / tecnología operativa (OT)
- Como un porcentaje del gasto total en TI
- El que defina Tecnologías de la información
- Como un cambio porcentual con respecto al presupuesto de ciberseguridad del periodo anterior
- Como una suma de fondos/recursos propuestos para respaldar proyectos/actividades de negocio y de mitigación de riesgos aprobados

¿Cómo su organización establece su presupuesto de ciberseguridad?

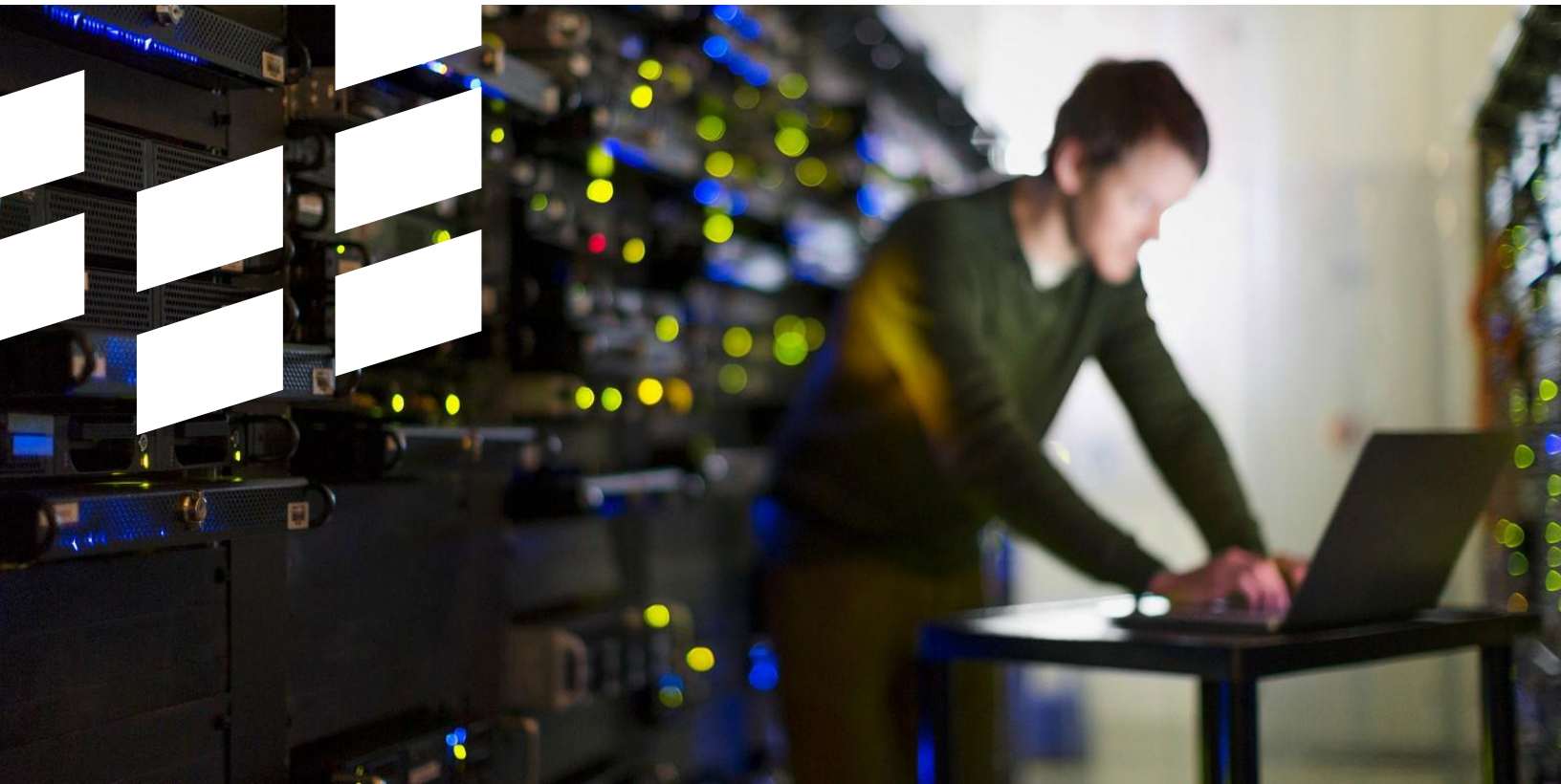
Fuente: PwC 2023 Global Digital Trust Insights Survey.



- Como un porcentaje de los gastos combinados en TI y automatización / tecnología operativa (OT)
- Como un porcentaje del gasto total en TI
- Es un tema nuevo y no existe una opción especifica para temas de presupuesto en CS
- El que defina Tecnologías de la información
- Como un cambio porcentual con respecto al presupuesto de ciberseguridad del periodo anterior
- Como una suma de fondos/recursos propuestos para respaldar proyectos/actividades de negocio y de mitigación de riesgos aprobados
- No lo sé

¿Cómo su organización establece su presupuesto de ciberseguridad?

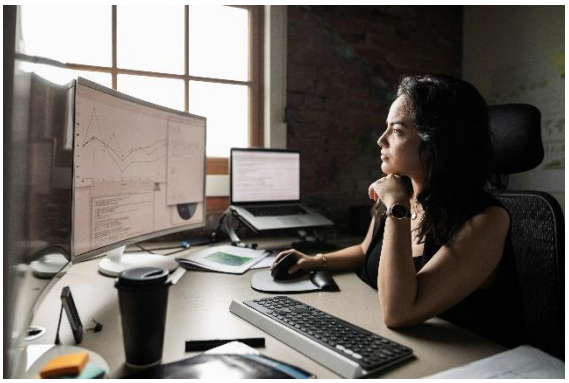
Fuente: Encuesta Regional Digital Trust Insights 2023 de PwC Interaméricas.



Las diferentes organizaciones a nivel global tienden a dedicarle un porcentaje de los gastos combinados en TI y automatización / OT o un porcentaje del gasto total en TI. Sin embargo, un presupuesto de ciberseguridad debe estar basado en la cuantificación de riesgos y alineado a la estrategia de negocio. En nuestra región el 45% de las empresas define su presupuesto de ciberseguridad como una suma de fondos propuestos para respaldar proyectos y mitigación de riesgos.

Muchos ejecutivos han empezado a cambiar su estrategia para invertir en ciberseguridad. Alrededor de un tercio dicen que “en gran medida” su inversión actual está alineada con 7 parámetros clave. En la siguiente tabla se comparan los resultados de nuestro territorio con los de nivel global:

En este caso, nuestro territorio sigue la tendencia global; los ejecutivos indican que su presupuesto refleja sus prioridades de ciberseguridad y está alineado con la estrategia de negocio, sin embargo, son pocos los que indican que el mismo está bien asignado según los riesgos a los que se enfrenta su organización. Esto puede indicar una subestimación de la importancia de la inversión en ciberseguridad para protección ante las crecientes amenazas digitales.



	Interamericas
Refleja nuestras prioridades de ciberseguridad	59%
Está alineado con la estrategia del negocio	55%
Es adecuado para que la ciberseguridad ayude a crear valor para mi organización	55%
Está equilibrado respecto a nuestras necesidades actuales y a largo plazo	45%
Se fundamenta en la cuantificación de los ciber riesgos	45%
Considera el apetito al riesgo de la organización	36%
Está bien asignado según los riesgos a los que se enfrenta nuestra organización	32%

5 El camino por seguir para fortalecer la ciberseguridad

El panorama actual de la ciberseguridad es complejo, ya que las amenazas digitales continúan evolucionando y aumentando en número e intensidad. Es importante que una estrategia de ciberseguridad no se limite a cumplir las posibles regulaciones de un ente gubernamental; constantemente se deben identificar posibles mejoras y establecer un plan para implementarlas. Para fortalecer la ciberseguridad, es importante seguir un camino que abarque las siguientes dimensiones:

Concientización y formación: Es fundamental que todos los miembros de la organización estén informados sobre las amenazas de ciberseguridad y sepan cómo proteger su información y la de la organización, desde la alta directiva, hasta todos los miembros del staff.

Evaluación y mitigación de riesgos: La organización debe realizar constantemente una evaluación exhaustiva de los riesgos de ciberseguridad y desarrollar un plan de mitigación para minimizar su impacto.

Implementación de soluciones de seguridad: La organización debe implementar soluciones de seguridad adecuadas para proteger sus sistemas, redes y datos, como firewalls, cifrado de datos y software de detección de intrusos.

Mantenimiento y actualización de soluciones: Es crucial mantener y actualizar las soluciones de seguridad de la organización para garantizar su efectividad ante nuevas amenazas.

Monitoreo y respaldo: La organización debe monitorear constantemente su sistema y realizar copias de seguridad regulares para minimizar el impacto de un posible ataque.

Además de estos pasos, es importante que el presupuesto dedicado a ciberseguridad sea monitoreado para así identificar los beneficios, ser eficientes con los recursos que se tienen e invertir en capacitación y tecnologías para fortalecer la ciberseguridad a futuro, especialmente en áreas como la inteligencia de amenazas y la ciberdefensa.

Contacto

Ignacio Perez Rubio
PwC | PwC InterAmerica Consulting Lead Partner
Office: +506 22241555 | Mobile: + 506 87035501 | Fax: +506 22435043
Email: ignacio.perez@pwc.com
PwC Costa Rica

Valentina Morales Chirimelli
PwC | Cybersecurity & Privacy Senior Manager
Office: +506 2224-1555 | Mobile: +506 83031716
Email: morales.valentina@pwc.com
PwC Costa Rica

Isaac Rodríguez Rojas
PwC | Cybersecurity & Privacy Manager
Direct: +506 2224-1555 | Mobile: +506 83031903
Email: isaac.rodriguez@pwc.com
PwC Costa Rica

Gabriel García Carrasquel
PwC | Cybersecurity & Privacy Manager
Direct: +506 2224 1555 | Mobile: +506 85807335
Email: gabriel.garcia.carrasquel@pwc.com
PwC Costa Rica