Digital Trust Insights 2022

Edición México

pwc

Ciberseguridad, simplemente segura

La pandemia de COVID-19 aceleró los planes de digitalización de las organizaciones, ya sea permitiendo el trabajo remoto o aumentando sus capacidades tecnológicas. Sin embargo, esto ha ocasionado que los ciberataques sean más sencillos de perpetuar, tengan una mayor frecuencia e impacto.

Con el objetivo de conocer el estado de la ciberseguridad y privacidad, llevamos a cabo la encuesta *Digital Trust Insights 2022,* en la que entrevistamos —entre julio y agosto de este año— a 132 ejecutivos de las áreas de tecnología, información, finanzas, seguridad de la información, así como directores generales.

Principales hallazgos

58%

destacó que aumentará el presupuesto de ciberseguridad en más del 5% para 2022

63%

prevé un aumento de ciberataques a sus servicios de nube e Internet de las cosas (IoT, por sus siglas en inglés)

53%

indicó que tiene una comprensión limitada sobre los riesgos en el software de la cadena de suministro

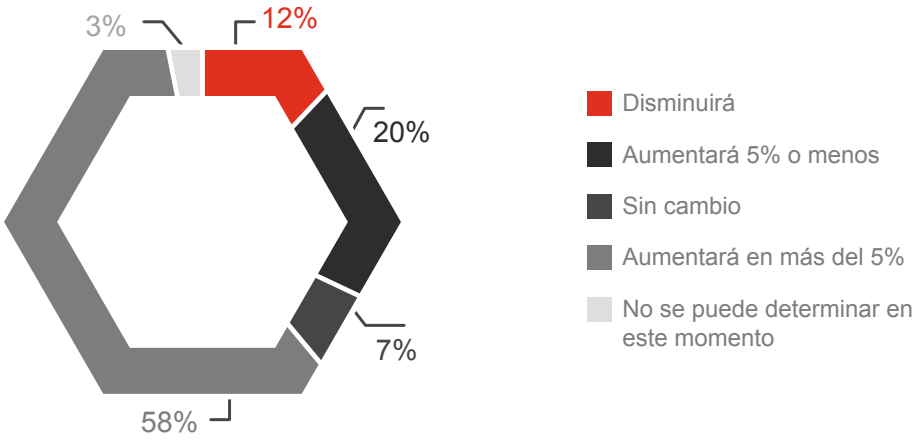
48%

señaló que el CEO brinda un apoyo significativo a crear una cultura en ciberseguridad

Inversiones en ciberseguridad en aumento

Las empresas están priorizando la ciberseguridad en su estrategia general de negocio, pues el 58% de los directores encuestados proyecta que el presupuesto en ciberseguridad aumentará entre 6 y 15% o más para 2022, un crecimiento de 20 puntos porcentuales respecto al año pasado.

¿Cómo está cambiando el presupuesto en ciberseguridad para 2022?



Fuente: Digital Trust Insights 2022 México, julio – agosto. Base: 132

Los ejecutivos destacaron la **integración de controles y procesos** (ej., en áreas como riesgo, ciberseguridad, cumplimiento y/o privacidad), **reestructuración del equipo de seguridad** y **la reducción de la tecnología obsoleta** o que ya llegó al final de su vida útil como las principales iniciativas en donde se asignará mayor presupuesto para simplificar la ciberseguridad en los próximos dos años.

El aumento de la inversión en ciberseguridad refleja cómo las organizaciones buscan protegerse ante incidentes cibernéticos que continúan a la alza, especialmente los relacionados a ciberataques al ***software* de la cadena de suministro, *malware*,** así como de la minería de criptomonedas.

Además, los encuestados indicaron que los criminales cibernéticos se mantienen como su principal ciberamenaza, tanto en México como en el resto del mundo. No obstante, más de la mitad de los directores mexicanos (52%) considera que un empleado actual podría perpetrar un ciberataque, casi en el mismo porcentaje (50%) que un *hacktivista*.

Ante un mundo digital cada vez más peligroso, la confianza tendrá que ser fundamental para una estrategia de ciberseguridad. El CEO deberá establecer la seguridad y privacidad como un imperativo que aminore los riesgos y aumente los beneficios.

¿Puede el CEO marcar la diferencia en la ciberseguridad de la empresa?

Hoy más que nunca los directores generales deberán tener un mayor involucramiento en los asuntos de ciberseguridad y privacidad de datos de su organización. Ante un aumento en los ciberataques, los CEO tendrán que enfocarse tanto en temas tecnológicos como de negocio para generar una estrategia de ciberseguridad cuyo slogan sea: *"simplemente seguro".*

¿Qué nivel de apoyo brinda el CEO al equipo de seguridad para lograr lo siguiente?

Fuente: Digital Trust Insights 2022 México, julio – agosto. Base: 132

Los ejecutivos encuestados indicaron que el CEO brinda apoyo significativo al equipo de ciberseguridad en garantizar que se tengan suficientes recursos, prioridades y financiamiento (48%), crear una cultura competente de ciberseguridad en la empresa (46%) y conectar con confianza con los clientes y socios comerciales (45%).

Aunque existe un apoyo real por parte de los directores generales, es importante destacar que, en la mayoría de los casos, este se involucra en los esfuerzos de ciberseguridad y privacidad cuando ya ocurrió un ciberataque. Para ello, el *Chief Information Security Officer* (CISO) deberá apoyar al CEO en despejar el camino para prácticas de ciberseguridad que sean simples y seguras.

Los CEO deberán considerar la ciberseguridad al centro de cada decisión empresarial. Los modelos de negocio son cada vez más digitales, por lo tanto, asegurar un crecimiento y confianza con los clientes dependerá de propiciar una gestión de los ciberriesgos eficazmente.

Los tres principales objetivos en relación a la estrategia de ciberseguridad, personal e inversiones son:

1. Mejorar la confianza de los líderes en su habilidad de gestionar amenazas presentes y futuras
2. Incrementar la prevención de ataques efectivos
3. Lograr tiempos de respuesta más rápidos a incidentes y disrupciones

La estrategia de ciberseguridad que los líderes de la organización tendrán que diseñar deberá enfocarse en tres aspectos fundamentales: tecnología que simplifique y mejore la ciberdefensa; establecer un marco regulatorio que permita cumplir responsabilidades y rinda cuentas, así como desarrollar una fuerza laboral cibernética diversa.

Considera lo siguiente:

- El CEO debe priorizar la ciberseguridad para asegurar el crecimiento de la empresa, así como la confianza con los clientes.
- Los directores generales tienen que hacer frente a los problemas y riesgos de los nuevos modelos de negocio y ajustar los cambios.
- El CISO deberá conocer la estrategia del negocio y su incidencia en la ciberseguridad para generar confianza y crecimiento en la organización.

¿La empresa es demasiado compleja para protegerla?

La complejidad no es mala en sí misma, suele ser un subproducto del crecimiento. Sin embargo, cuanto más grande sea una empresa, más compleja será y, naturalmente, necesitará más personas y tecnología para atender su demanda de clientes.

En su opinión, ¿qué nivel de complejidad tienen las siguientes operaciones en su empresa, en una escala del 1 al 10?

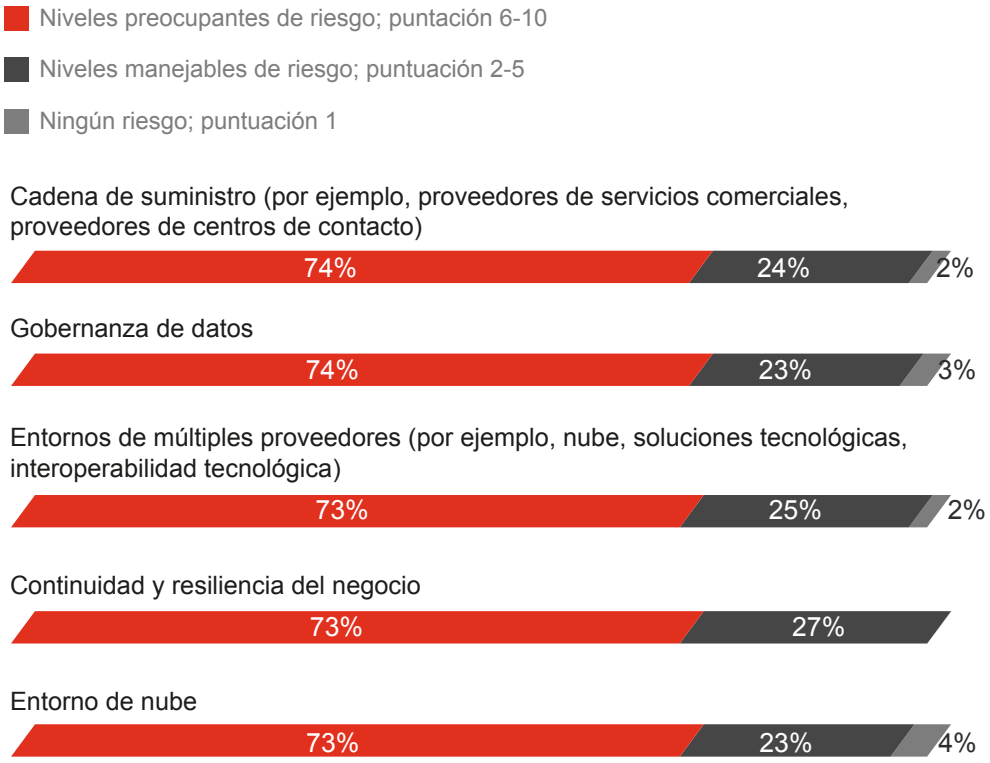
Fuente: Digital Trust Insights 2022 México, julio – agosto. Base: 132

En México, siete de cada 10 encuestados indicó que las tres principales operaciones con mayor complejidad que pueden ser evitables e innecesarias son la infraestructura de datos, la continuidad y resiliencia del negocio, así como la gobernanza de proyectos o implementaciones tecnológicas.

En la gran mayoría de los casos, las organizaciones no identifican los costos que conlleva tener una complejidad innecesaria y termina siendo difícil saber qué reducir para simplificar las operaciones. No es sino hasta que un ciberataque ocurre para priorizar lo que debe ser mejorado.

La complejidad representa un riesgo relevante para la ciberseguridad y privacidad. En México, las principales áreas que son críticas para las operaciones de la organización son: la gobernanza de datos, la cadena de suministro, así como los entornos de múltiples proveedores (ej., nube, soluciones tecnológicas, interoperabilidad tecnológica).

¿Qué importancia tienen los riesgos cibernéticos y de privacidad que plantea la complejidad en estas áreas de tu empresa?



Fuente: Digital Trust Insights 2022 México, julio – agosto. Base: 132

Por ejemplo, si una empresa aún conserva los datos sensibles sobre un cliente con el cual ya no tiene una relación comercial, es muy probable que si una incidencia llegara a ocurrir, un *hacker* pudiera beneficiarse de esto.

Tanto en México como a nivel global, los ejecutivos destacaron que **las consecuencias más importantes respecto a la complejidad de sus negocios** son:

1. Incapacidad para innovar tan rápido como se presentan las oportunidades en el mercado.
2. Pérdidas financieras debido a violaciones de datos o ciberataques exitosos.
3. Falta de resiliencia operativa o incapacidad para recuperarse de un ciberataque o falla tecnológica.

La complejidad no solo amenaza a las operaciones de la organización, también detiene el crecimiento, así como nuevas oportunidades que podrían devenir a futuro.

Considera lo siguiente:

- Los directores de operaciones y de transformación pueden incentivar el cambio operativo y cultural por medio de una pregunta clave: ¿cuál es el plan de ciberseguridad que simplifique las operaciones?
- Colocar la ciberseguridad en el centro de cada decisión evitará tener complejidades innecesarias y costosas.
- Incluir al CISO y a los equipos de seguridad en las primeras etapas de transformación digital, (ej., migración a la nube), podría reducir la complejidad y tener una estrategia de ciberseguridad exitosa.
- El CISO y CIO deben atreverse a restar. La tecnología y los datos tienden a multiplicarse o dividirse, lo que reduce la eficiencia y seguridad.
- Reducir el exceso teniendo en cuenta los objetivos de seguridad:
  - Evaluar los almacenes de datos y eliminar todo lo que no se necesita.
  - Mover las aplicaciones a un entorno de nube para una gestión más sencilla.
  - Consolidar, liquidar y automatizar lo más posible.
- Reconsiderar los procesos de inversión tecnológica y ciberseguridad.
- Concentrarse primero en simplificar donde los beneficios son mayores.

¿Estás utilizando datos e inteligencia para protegerte contra los riesgos más importantes?

Tanto las empresas en México como a nivel mundial no están implementando prácticas avanzadas de confianza en los datos, es decir, se están arriesgando a tomar decisiones con poca o ninguna información. Solo alrededor de un tercio de las organizaciones encuestadas destacó que sí utiliza datos e inteligencia para protegerse contra riesgos de ciberseguridad.

Las principales herramientas y metodologías que forman parte integral del modelo operativo de las empresas

Fuente: Digital Trust Insights 2022 México, julio – agosto. Base: 132

Las principales herramientas y metodologías que usan las empresas de forma integral en su modelo operativo son la **inteligencia de amenazas en tiempo real (45%), detección autónoma de amenazas (45%),** en particular, seguridad cognitiva y el **uso de estándares y marcos ampliamente aceptados (ej., NIST, CMMC, ISO, etc.)** en herramientas de evaluación y diagnóstico (42%).

Los datos e inteligencia son primordiales para que las organizaciones puedan cuantificar el riesgo cibernético eficazmente. En el caso de los encuestados mexicanos, los utilizan para evaluar continuamente el panorama de riesgos y las prioridades frente a los cambios en los objetivos comerciales, justificar las solicitudes de inversión en ciberseguridad, y para identificar y justificar las mejoras o la transformación de las capacidades de protección.

El panorama de las amenazas para 2022

De acuerdo a nuestros encuestados en México, se tiene previsto un incremento en los incidentes relacionados a un ataque en el *software* de la cadena de suministro (55%), *malware* a través de una actualización de *software* (52%), minería de criptomonedas y un ataque a los servicios en la nube (51%, respectivamente).

Por otro lado, seis de cada 10 encuestados tienen previsto que los principales vectores con mayor posibilidad de ser una amenaza serán los proveedores de servicios en la nube, el Internet de las cosas (IoT, por sus siglas en inglés) y el teléfono celular.

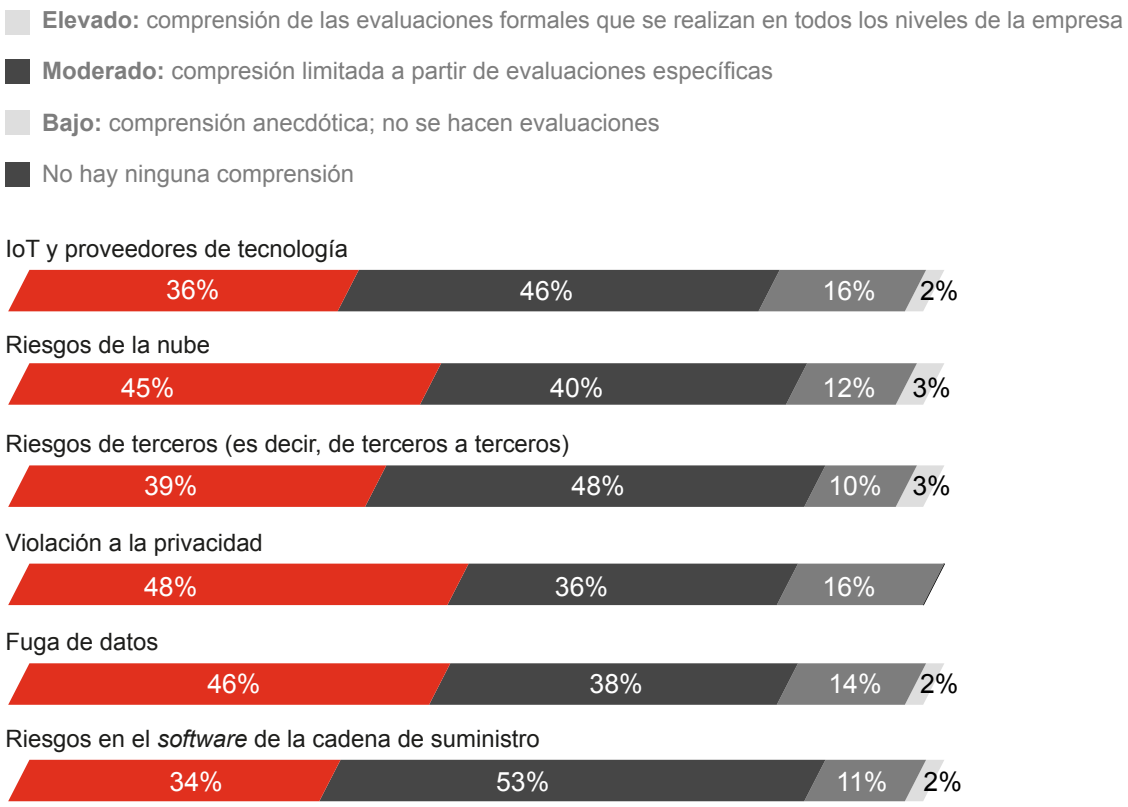
Considera lo siguiente:

- El CFO debe colaborar con el CISO para decidir un presupuesto en ciberseguridad enfocado al crecimiento y basado en el riesgo.
- El CISO tendrá que construir una base sólida de confianza en los datos y crear una hoja de ruta desde la cuantificación del riesgo hasta los informes en tiempo real.
- Relacionar los riesgos de ciberseguridad con los de la empresa, y en última instancia con los efectos en el negocio.
- Al tener una cuantificación de los riesgos de ciberseguridad, se podrá identificar lo que funciona en el modelo de negocio y lo que podría simplificarse.

¿Qué tan bien conoces los riesgos que plantean tus terceros y la cadena de suministro?

Las empresas no pueden proteger lo que no pueden ver y, de hecho, los encuestados señalaron tener problemas para observar los riesgos asociados a terceros debido a las complejidades comerciales, así como de sus redes de proveedores.

Las principales herramientas y metodologías que forman parte integral del modelo operativo de las empresas



Fuente: Digital Trust Insights 2022 México, julio – agosto. Base: 132

Las principales áreas en donde las organizaciones tienen un nivel alto de conocimiento del riesgo que representa trabajar con terceros o proveedores son en la violación a la privacidad (48%), fuga de datos (46%) y riesgos de la nube (45%). Por otro lado, se tiene una comprensión moderada en temas como los riesgos en el *software* de la cadena de suministro (53%), riesgos de terceros (48%), es decir, de terceros a terceros, y de IoT y proveedores de tecnología (46%).

Cabe destacar que, las organizaciones que tienen mejores resultados en su estrategia de ciberseguridad han simplificado a los proveedores de tecnología.
Al reducir la complejidad se aumenta la capacidad para saber qué tan seguros son los terceros.

Entre los elementos clave que las empresas implementaron en los últimos 12 meses para reducir al mínimo los riesgos a terceros o proveedores en su ecosistema de cadena de suministro son:

- Auditar o verificar la postura de seguridad y el cumplimiento de los terceros o proveedores **(58%).**
- Perfeccionar los criterios para incorporar y evaluar permanentemente a los terceros **(52%).**
- Realizar una diligencia debida más estricta **(51%).**

Considera lo siguiente:

- COO y directores de cadena de suministro deben mapear los sistemas, en especial los más críticos, y usar un rastreo de terceros para encontrar los eslabones más débiles de la cadena de suministro.
- El *software* y las aplicaciones que utiliza la empresa deben someterse al mismo nivel de escrutinio y pruebas que los usuarios y dispositivos de red.
- Tanto el CRO como el CISO deben desarrollar una capacidad tecnológica y organizativa para detectar, resistir y responder a ciberataques avanzados.
- Crear una oficina de gestión de riesgos de terceros.
- Fortalecer la base de confianza en los datos.
- Educar a la junta directiva sobre los riesgos comerciales y digitales de terceros y la cadena de suministro.

Implementar las 4P para potencializar la ciberseguridad

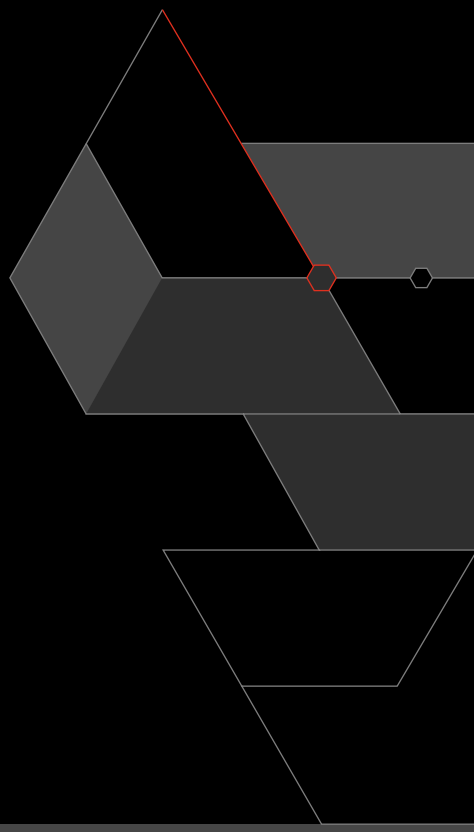
Los ciberataques continuarán en aumento y con una mayor velocidad. Las empresas no pueden bajar la guardia, sino que deben prepararse con una estrategia de ciberseguridad cuya base sea la confianza y permita simplificar la seguridad en la organización. Considerar las “4P” podría potencializar estos esfuerzos:

Principio. El CEO debe articular un principio fundamental explícito e inequívoco que establezca la seguridad y la privacidad como imperativo empresarial.

Personas. Colocar a un líder que permita que los equipos de seguridad y el CISO se conecten con los equipos comerciales. La gente puede ser la vanguardia de la simplificación incluso si existe una “buena complejidad” en el negocio.

Priorización. Los riesgos cambian continuamente a medida que aumentan las ambiciones digitales. Además, también se deberían utilizar datos e inteligencia para medir los riesgos continuamente.

Percepción. No puedes asegurar lo que no puedes ver. Descubre los puntos ciegos en las relaciones y cadenas de suministro.



Contactos:

Fernando Román
Socio Líder de Cybersecurity, Privacy y Forensics Services en PwC México

Juan Carlos Carrillo
Cybersecurity, Privacy & Forensic Services en PwC México