KPMG

KPMG Cyber trust insights 2022

Generando confianza a través de la ciberseguridad y la privacidad

Enero 2023 | kpmg.com.br

Contenido

Visión general

Cinco pasos cruciales para generar confianza a través de la ciberseguridad y la privacidad

Cada vez más, las empresas reconocen el valor de la confianza. En un entorno incierto y en constante cambio, los clientes, empleados e inversores valoran aquellas organizaciones en las que saben que pueden confiar. Para construir, fortalecer y mantener este sentimiento, es esencial que las diversas áreas actúen en armonía, entregando al cliente la coherencia e imagen unificada que tanto valora.

Ahora que vivimos en un mundo digitalizado, en el que los datos son el punto de partida para muchas decisiones y estrategias, es esencial que se recopilen y traten de manera ética, completa y transparente; también es fundamental que los sistemas sean resistentes, confiables y capaces de responder rápidamente a los desafíos que surgen diariamente.

El cliente quiere sentirse seguro al realizar transacciones y ser parte del ecosistema de formado por socios, inversores, reguladores y la sociedad que rodea cualquier organización. La confianza digital es importante.

La ciberseguridad y la privacidad juegan un papel clave en la construcción y el mantenimiento de la confianza. Las empresas están aumentando la recopilación de datos, expandiendo el uso de tecnologías como la inteligencia artificial (IA) y el aprendizaje automático (ML) y adoptando la agenda ambiental, social y de gobierno (ESG), al tiempo que necesitan adaptarse a estándares regulatorios extremadamente complejos.

En este documento, titulado **KPMG Cyber Trust Insights 2022,** abordamos la confianza cibernética en 2022. El estudio se basa en opiniones proporcionadas por 1.881 ejecutivos y una serie de discusiones con líderes y profesionales corporativos de todo el mundo, realizadas con el objetivo de comprender cómo ven los ejecutivos el desafío de la confianza y cuáles serán sus próximos pasos en este viaje. También exploramos el papel clave que los directores de seguridad de la información (CISO) pueden desempeñar en este movimiento.

Como resultado, se han identificado cinco pasos cruciales para generar confianza a través de la ciberseguridad: **abordar la privacidad y la ciberseguridad como un asunto de suma importancia; construir alianzas internas; reimaginar el papel del CISO; asegurar el apoyo del liderazgo; y actuar en sinergia con el ecosistema.**

Principales conclusiones

Tormenta de datos

Las empresas están extrayendo datos a escala. Esto plantea preocupaciones sobre cómo se protegen, usan y comparten estos datos.

La mayoría de los encuestados participaron en una recopilación o análisis más completo de los datos de los clientes en el último año.

Invertir en actividades basadas en datos se ha convertido en una prioridad en las organizaciones.

Desafíos de inteligencia artificial y aprendizaje automático

Existen crecientes preocupaciones empresariales y sociales sobre las implicaciones éticas, de seguridad y privacidad en la adopción de soluciones de IA y ML para el análisis de big data.

78% están de acuerdo en que la IA y ML traen desafios únicos en ciberseguridad

3 en 4 Dicen que AI y ML plantean preguntas éticas fundamentales

Valor y confianza

¡La confianza nunca ha sido más importante de lo que es ahora! Y no se trata solo de mantener una buena reputación: aumentar la confianza crea una ventaja competitiva y genera resultados.

Más de 1/3

Las organizaciones reconocen que el aumento de la confianza aumenta las ganancias.

65% informan que los requisitos de seguridad de la información están atados al compliance, en vez de a las ambiciones estratégicas de largo plazo.

Aumento de la regulación

Los reguladores estan atentos a estos problemas, y las organizaciones están preocupados por moverse a través de un panorama global cada vez más complejo desde el punto de vista regulatorio.

36% De los encuestados están preocupados por su capacidad para satisfacer las regulaciones de ciberseguridad cuando se externalizan actividades

34% Esta preocupado por la divulgación de informes corporativos relacionadas con la ciberseguridad.

Comunidades y confianza

Las asociaciones externas tienden a desempeñar un papel cada vez más vital para el éxito en ecosistemas hiperconectados; Sin embargo, las barreras prácticas pueden obstaculizar la colaboración.

79% Dicen que la colaboración constructiva con proveedores y clientes es vital, pero solo el 42% informa vivir esto en la práctica.

60% admiten que su cadena de suministro es vulnerable a los ataques.

CISO en evolución

Las organizaciones reconocen el papel que el CISO puede desempeñar en la incorporación de un enfoque de confianza digital en toda la organización?

1/2 de los ejecutivos tienen dudas que la relación entre el directorio y el CISO esté basada en la confianza

1/3 dicen que el CISO no es visto como un ejecutivo clave; por lo tanto tiene menos influencia que la necesaria para proteger eficazmente la organización y sus datos.

Propósito de la confianza

¿Reconocen las empresas el vínculo entre la confianza digital y la agenda ambiental, social y de gobernanza (ESG)?

Menos de 1 de cada 5

dijo que el equipo de CISO es parte del equipo de ESG.

50% informa que el equipo de CISO desempeña un papel muy limitado dentro de los criterios ESG.

Source: KPMG Cyber trust insights 2022

1

Transformación digital

Caso de negocio: invertir en confianza

¿Qué entendemos por confianza?

Una definición clara de confianza puede ayudar a las empresas a asumir un papel activo en la medición, el aumento y, por lo tanto, el aprovechamiento de una amplia gama de beneficios potenciales tangibles.

La confianza digital es la confianza que las partes interesadas depositan en la capacidad de una organización para aprovechar la tecnología digital, proteger sus intereses y defender las expectativas y valores de la sociedad.

Si bien es probable que cada organización tenga diferentes prioridades y pueda usar diferentes lenguajes para describir aspectos de la confianza digital, el concepto generalmente cubre:

Seguridad y fiabilidad

En este sentido, la prioridad es garantizar que la tecnología y los datos de una organización estén bien protegidos mientras operan según lo diseñado.

Uso inclusivo, ético y responsable

De esta manera, se asegura que una organización diseñe, construya y opere sus herramientas tecnológicas y utilice los datos con plena responsabilidad en relación con los individuos, la sociedad en general, el entorno en el que se inserta y todos sus grupos de interés.

Responsabilidad y supervisión

La organización debe definir claramente sus responsabilidades con respecto a la confianza y observarlas y cumplirlas estrictamente.

Por qué es importante: una mayor confianza puede aumentar las ganancias y generar clientes

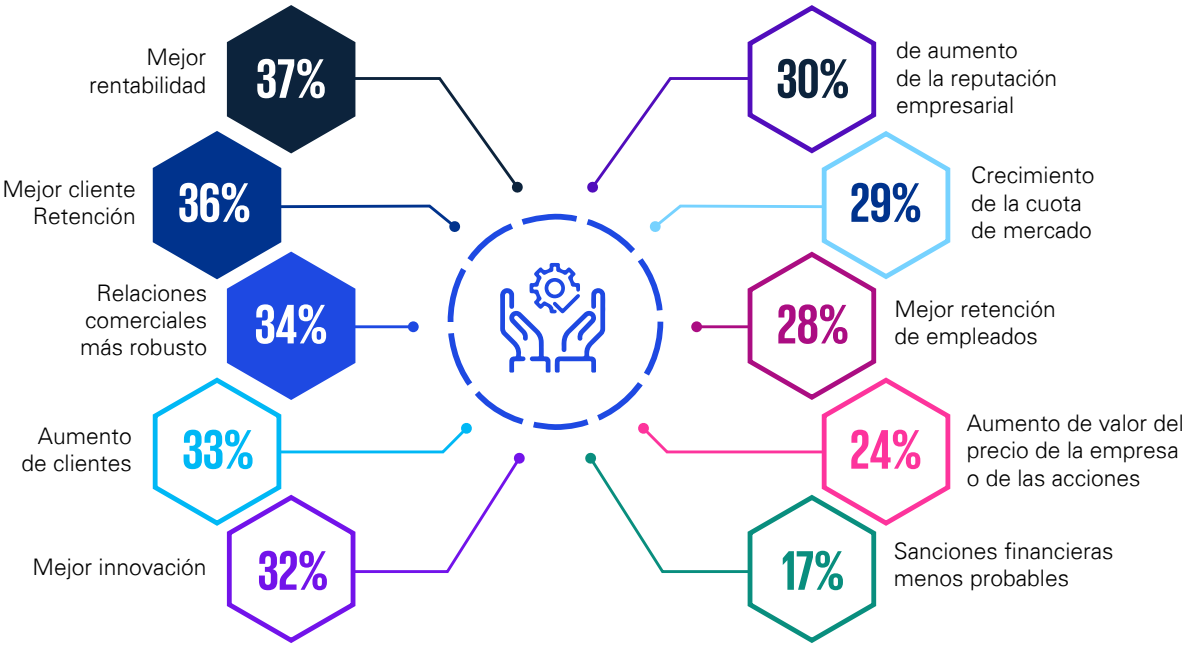
Según nuestros encuestados, los tres principales beneficios esperados de una mayor confianza son:

1. Mejor rentabilidad
2. Mejor retención de clientes
3. Relaciones comerciales más sólidas

Otras ganancias potenciales incluyen una mayor innovación, una mayor retención de empleados y una mayor participación en el mercado.

Los principales beneficios de una mayor confianza

La tabla muestra el porcentaje de encuestados que seleccionaron cada opción de las tres primeras.



Source: KPMG Cyber trust insights 2022

Las empresas están invirtiendo en datos y centrándose en la experiencia del cliente

La transformación digital está en marcha: en todas las industrias, las empresas están analizando la tecnología y poniendo datos avanzados y análisis sofisticados en el centro de las operaciones. Durante los próximos tres años, las organizaciones planean realizar una serie de inversiones en herramientas digitales para impulsar el crecimiento, optimizar las interacciones con los clientes, aumentar las operaciones comerciales e impulsar el valor de los datos. Sin embargo, cada nueva actividad de datos expone a las empresas a posibles vulnerabilidades y riesgos de reputación.

Según el Global Tech Report de KPMG, el **61% de las empresas espera adoptar nuevas plataformas tecnológicas revolucionarias dentro de dos años;** en hasta tres años, pueden aumentar la inversión en Internet de las cosas (IoT), computación de vanguardia y 5G. En menor medida, también pueden invertir en realidad virtual y realidad aumentada.

En el mismo informe de KPMG, **la digitalización de los canales de clientes se cita como el segundo desafío de ciberseguridad más serio al que se enfrentan las organizaciones,** justo detrás de la adopción de entornos de trabajo híbridos.El 37% de los encuestados esta focalizado en el uso de datos de experiencia para personalizar las interacciones digitales en tiempo real, mientras el 36% está invirtiendo en la integración multicanal para mejorar la experiencia del cliente.

A medida que estas tendencias se consolidan y se extienden, las expectativas de privacidad del cliente también cambian. Cada vez más, los usuarios esperan poder personalizar los controles de privacidad en sus dispositivos y canales, lo que requiere que las organizaciones ofrezcan controles flexibles sobre sus futuros productos y servicios.

Las principales áreas de inversión en experiencia digital

La tabla muestra el porcentaje de encuestados que seleccionaron cada opción entre las tres primeras.

Source: KPMG Cyber trust insights 2022

> **Invertir en ciberseguridad y protección de la privacidad es necesario para mantener la confianza."**
>
> **Bashar Abouseido**
> Vicepresidente Senior y CISO,
> Charles Schwab

La ciberseguridad está cambiando y los datos importan más que nunca

Las empresas deben fortalecer su seguridad en áreas clave para garantizar la confianza de sus grupos de interés. Más del 80% de los encuestados reconoció la importancia de mejorar la ciberseguridad y la protección de datos, incluida una mayor transparencia en relación con el uso de datos. Más de la mitad (51%) de los encuestados considera extremadamente importante proteger los activos de TI de ataques.

A medida que las organizaciones impulsan la transformación digital, las inversiones en ciberseguridad y privacidad deben incluirse en un presupuesto y cumplirse al pie de la letra como parte integral de las iniciativas estratégicas. "El éxito de los servicios digitales transformadores probablemente dependerá de que las organizaciones incorporen la seguridad y la privacidad en su desarrollo e implementación", dice Allan Cocksaur, CISO de Shell.

"Estamos priorizando lo que llamamos 'seguridad mediante la redacción de estándares' en la forma en que construimos tecnología. Queremos que estos estándares sean transparentes para los clientes porque nuestra obligación es mantener y aumentar la confianza", dice.

"Proteger la confianza del cliente es lo que impulsa nuestras inversiones en ciberseguridad y privacidad", dice Bashar Abouseido, vicepresidente senior y CISO de Charles Schwab. Para mantener confianza de los clientes, estamos dispuestos a ir más allá a través de mejoras proactivas y continuas en los controles de privacidad y la transparencia sobre nuestras medidas de protección de datos".

KPMG Perspective: La confianza se está convirtiendo en clave para el éxito de las tecnologías emergentes

Las tecnologías emergentes como la tecnología de contabilidad distribuida (DLT), la computación cuántica, 5G, redes AI / ML, realidad aumentada y virtual se están desarrollando rápidamente, y prometen transformar la forma en que operan las empresas.

Sin embargo, el lanzamiento exitoso de aplicaciones futuras (economía conectada, sistemas inteligentes, NFT, metaverso, etc.) que dependen de estas tecnologías probablemente se regirá por la capacidad de la organización para infundir confianza en varias dimensiones. Esto significa incorporar controles de seguridad y privacidad con transparencia, confiabilidad e integridad.

Atul Gupta
Socio Jefe de Servicios de Confianza Digital
y Seguridad Cibernética
en KPMG en India

2

Tendencias en confianza digital

Comprender los factores que impulsan la confianza

Cómo abordar los desafíos éticos de la IA

El creciente uso de las tecnologías de IA está imponiendo nuevos problemas de confianza que aún no se comprenden completamente. La investigación de KPMG muestra que las empresas están decididas a adoptar herramientas de IA, con expectativas de beneficios que van desde una mayor eficiencia y productividad a la expansión de la capacidad de generar insights predictivos sobre los clientes y mercados.

El peligro es que estas tecnologías, si no obtienen el enfoque correcto, pueden plantear riesgos para la ciberseguridad y la privacidad, con potencial de daños a la reputación y a sanciones regulatorias.

Las organizaciones están empezando a reconocer estos riesgos. Más de tres cuartas partes de los encuestados (78%) están de acuerdo en que la inteligencia artificial trae desafíos únicos de ciberseguridad.

Los encuestados también señalaron la existencia de problemas éticos fundamentales que deben resolverse a medida que se adoptan estas tecnologías, y dicen que las organizaciones deberán comunicarse más abiertamente sobre cómo están manejando estos problemas.

Todo esto enfatiza el importante papel de los equipos de ciberseguridad y privacidad en la configuración del debate ético y la gestión de riesgos.

"Estamos trabajando en "adversarial IA" -cosas como el envenenamiento de datos, ataques IA-, porque creemos que será la próxima ola.", dice Ann Johnson, vicepresidenta corporativa de Microsoft Security Business Development.

La IA y la inteligencia artificial crean nuevos desafíos para el equipo de seguridad de la información

La tabla muestra el porcentaje de encuestados que están totalmente de acuerdo o de acuerdo.

78%	76%	76%	76%	75%
La adopción de IA / Inteligencia Artificial plantea desafíos únicos de ciberseguridad que requieren atención especial	La adopción de IA/ML requiere implementar salvaguardas adicionales sobre cómo entrenamos los sistemas IA/Inteligencia artificial y monitorear tu rendimiento	La adopción de IA / ML requiere que seamos más transparentes en la forma en que comunicamos cómo usamos las técnicas de IA / Inteligencia Artificial	La adopción de IA/ML plantea cuestiones éticas fundamentales que requieren una gobernanza y supervisión cuidadosas	La adopción de AI y ML plantea preocupaciones clave sobre la privacidad y la forma en que agregamos y se analizan datos de clientes y empleados comerciales

Fuente: KPMG Cyber trust insights 2022

Perspectiva de KPMG: IA ética

Las organizaciones saben que necesitan ser impulsadas por los datos. Muchos están expandiendo la IA para automatizar la toma de decisiones basada en datos, pero la IA conlleva nuevos riesgos para la marca y la rentabilidad. La tecnología tiene el potencial de estimular la desigualdad, violar la privacidad y limitar la capacidad de toma de decisiones.

No se puede culpar al propio sistema de IA por los resultados no deseados. Una IA ética y confiable no es un lujo, sino una necesidad comercial. Un número creciente de líderes empresariales reconoce esto, pero la confianza no se asegura sin esfuerzo o desafíos.

No menos importante, lo que se considera ético y apropiado en un sector o región puede no verse de la misma manera en otros contextos. No hay una única solución.

Simplemente copiar soluciones existentes no es efectivo. La IA confiable requiere un enfoque holístico, agnóstico y amplio dirigido a la concientización, la gobernanza de la IA y la gestión de riesgos.

Por ejemplo, las evaluaciones de impacto de la IA deben involucrar a las partes interesadas adecuadas para identificar los riesgos. Además, las organizaciones deben evaluar cuidadosamente el cumplimiento de las leyes y regulaciones y medir el retorno de la inversión de la IA.

Las decisiones deben ser ser trazables y auditables, y todas estas protecciones deben ponerse en práctica sin convertirse en un impedimento para la innovación.

Sander Klous
D&A Business Development Partner
KPMG en los Países Bajos

> # Estamos trabajando mucho en "adversarial IA" porque creemos que esa será la próxima ola de ataques"
>
> **Ann Johnson**
> **Vicepresidente corporativo,**
> **Desarrollo de negocios de seguridad de Microsoft.**

Perspectivas regulatorias

A medida que crecen las preocupaciones sociales sobre la confianza digital, los legisladores y reguladores tienden a demandar más transparencia y supervisión. La encuesta 2022 de KPMG sobre ciberconfianza destaca lo siguiente:

36%

Los encuestados están preocupados por su capacidad para cumplir con las regulaciones de ciberseguridad (existentes o nuevas) cuando las actividades se subcontratan a proveedores de servicios digitales.

34%

Esta preocupado por la divulgación de información corporativa relacionada con la ciberseguridad.

31%

están preocupados por las crecientes demandas en torno a la infraestructura crítica, que es el objeto de creciente regulación en el Reino Unido, la Unión Europea y los Estados Unidos.

Para aumentar la carga, las organizaciones internacionales deben ocuparse de reglamentaciones extraterritoriales cada vez más complejas e incluso restrictivas. "Un desafío para los directores de TI es que las partes interesadas de diferentes regiones tienen interpretaciones distintas de las mismas regulaciones", dice Ulrich Baisch, CIO de Bechtle, uno de los proveedores de servicios de TI más grandes de Europa. "Necesitas tener un concepto claro de lo que puedes y no puedes hacer".

Perspectiva de KPMG: factores que influyen en los organismos reguladores

A nivel mundial, hay un crecimiento acelerado en las regulaciones de ciberseguridad y privacidad. Más de 137 países tienen algún tipo de régimen de protección de datos, a menudo reclamando jurisdicción extraterritorial sobre los servicios ofrecidos en el país o los datos de sus ciudadanos. Los regímenes de privacidad más maduros están entrando en la segunda generación de regulaciones y enfrentando nuevos desafíos, que son impulsados por la adopción de tecnología. Por ejemplo, las discusiones sobre la regulación de la IA están formalizandose en proyectos de ley.

Además, a medida que crecen las preocupaciones con respecto a los ataques a los sistemas de control industrial, los países implementan regulaciones de ciberseguridad de infraestructura cada vez más estrictas. Estas regulaciones están pasando de la autoevaluación a estructuras de control, incluida la preparación y divulgación obligatorias de información sobre incidentes y auditorías externas.

Los organismos reguladores también están siendo más prescriptivos en sus estructuras de control, al tiempo que buscan fortalecer la independencia del CISO y su papel en la definición de las normas de control. También están surgiendo requisitos de resiliencia más holísticos, centrados en la recuperación empresarial en escenarios extremos pero plausibles, en sectores como las finanzas. Los requisitos de transparencia corporativa sobre los riesgos cibernéticos están en discusión con los crecientes requisitos para la divulgación de incidentes de ransomware.

Las empresas deben invertir para automatizar el monitoreo del cumplimiento , la preparación y divulgación de información, el cumplimiento de la regulación, y considerar las tendencias regulatorias en privacidad y seguridad al desarrollar nuevos servicios y productos.

David Ferbrache
Socio global de futuros cibernéticos
de KPMG en el Reino Unido

Más allá de la regulación

La confianza digital, que implica ciberseguridad y protección de la privacidad, debe formar parte de la agenda ESG de las empresas. "Las cuestiones ESG son una parte integral de la empresa en su conjunto, pero, por supuesto, el CISO desempeña un papel clave, especialmente cuando se trata de cuestiones sociales y de gobernanza", dice Ulrich Baisch de Bechtle.

Sin embargo, menos de una de cada cinco organizaciones describe la seguridad como una parte integral del equipo ESG. Y en su mayor parte, los encuestados dicen que desempeña un papel menor.

Las organizaciones también necesitan reconocer imperativos sociales y expectativas crecientes en torno a estos temas.

En las organizaciones, las personas responsables de cuestiones ESG deben trabajar en colaboración con los responsables de ciberseguridad (a menudo el CISO) y privacidad. (a menudo el DPO).

> **ESG es una parte integral del negocio en su conjunto; pero, por supuesto, el CISO juega un papel clave cuando se trata de cuestiones de gobernanza.**
>
> **Ulrich Baisch**
> CIO, Bechtel

Perspectiva de KPMG: ESG y responsabilidad social

Las organizaciones que realmente adoptan la agenda ESG pueden ganar la confianza del cliente y fortalecer la fortaleza de las marcas. En el mundo digital de hoy, consejos de administración, inversores, reguladores, clientes y el público en general esperan una preparación y divulgación transparentes de información sobre la postura de ciberseguridad y privacidad de la organización.

Las partes interesadas quieren sentirse seguras de que las juntas directivas y los ejecutivos aprecian las implicaciones sociales para garantizar la resiliencia y la integridad de los servicios críticos, al tiempo que protegen la información en la que confían.

Las consideraciones clave para las partes interesadas incluyen:

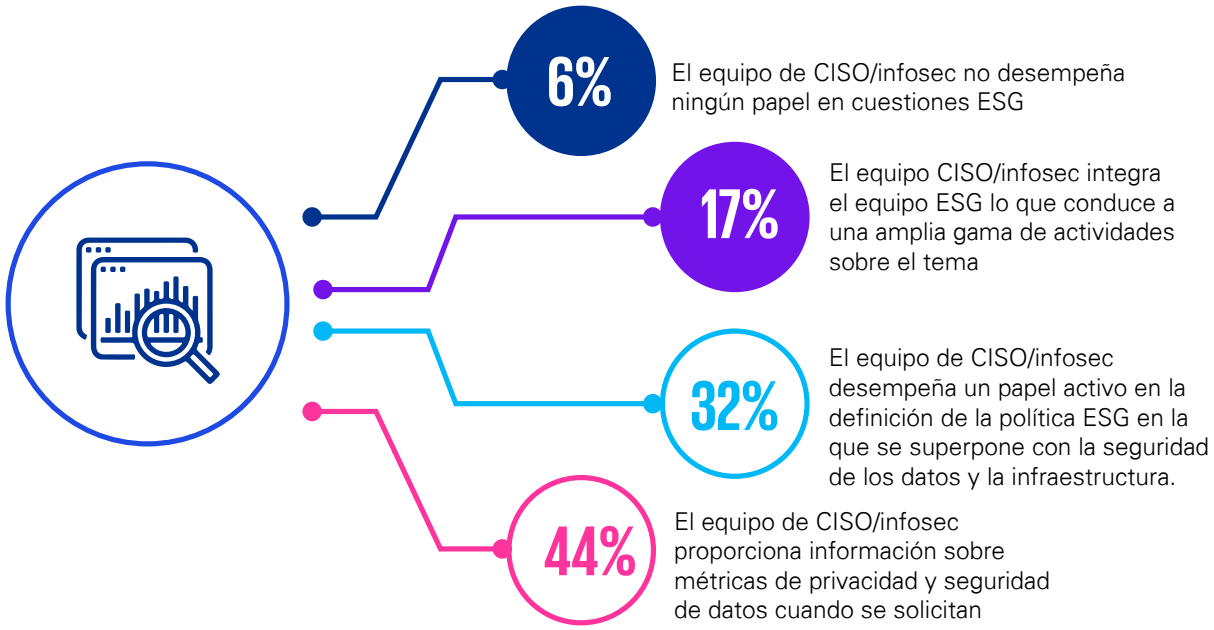
- Monitoreo proactivo de activos digitales para ayudar a garantizar el acceso a contenido seguro y confiable en un momento de alta explotación en línea y la "armamentización" de la información mediante "fake news" y "deep fakes".
- Ayudar a proteger a los clientes, particularmente aquellos por debajo de la línea de pobreza cibernética, del fraude digital y el robo de identidad.
- Garantizar la adopción ética de tecnologías como IA y ML, que recopilan y analizan los datos de los clientes.
- Mantener la fiabilidad, integridad y disponibilidad de los servicios digitales en los que nos basamos como sociedad.
- Demostración de un compromiso más amplio con las habilidades cibernéticas y la capacitación en el ecosistema de proveedores.

Srinivas Potharaju
Partner, Digital Trust
KPMG en India

Siddharth Durbha
Director, Digital Trust
KPMG en India

La mayoría de los directores de TI tienen una participación pasiva en las políticas y actividades de ESG

La tabla muestra el porcentaje de encuestados que seleccionaron la opción que consideraron mejor.



Fuente: KPMG Cyber trust insights 2022

Perspectiva de KPMG: cómo estimular la confianza yendo más allá del mínimo regulatorio

Las organizaciones con visión de futuro están incorporando métricas de privacidad de datos en los marcos de preparación y divulgación de información ESG.

De esta manera, ganan confianza para garantizar que los requisitos reglamentarios se cumplan mínimamente. Es como si las organizaciones buscaran proactivamente extrapolar estándares regulatorios mínimos, para que las partes interesadas se sientan más seguras de que su información personal se recopila, utiliza o divulga adecuadamente, no solo desde un punto de vista legal, sino desde una perspectiva que encaja en la narrativa articulada de ESG de la organización.

Sylvia Klasovec Kingsmill
Socio líder mundial de privacidad de KPMG en Canadá

3

Construyendo una comunidad de confianza

El poder de la colaboración

Las empresas digitalizadas de hoy no operan en el vacío, son parte cada vez más importante de asociaciones y colaboraciones más amplias. Esto aumenta el desafío que enfrentan los equipos ciberseguridad: Deben construir ecosistemas confiables para sus organizaciones, en sintonía con aliados que ayuden a garantizar la seguridad mutua y mantener la confianza en el ecosistema en su conjunto.

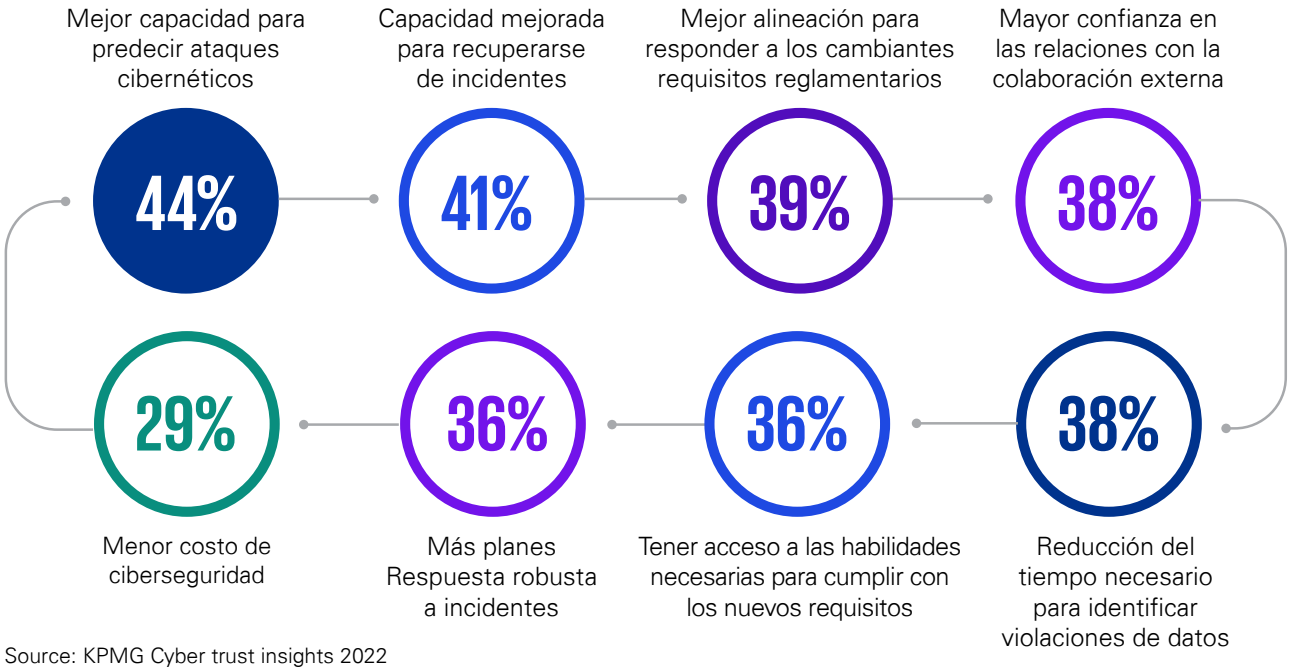
Hay fuerza en los números. En este estudio, casi la mitad de los encuestados (44%) dice que la colaboración en ciberseguridad en todo el ecosistema les ayudará a predecir ataques, por ejemplo.

Cuando la colaboración es deseable, no siempre es directa. Más de un tercio de los encuestados (38%) dice que las preocupaciones de privacidad interfieren en el camino de las asociaciones externas de ciberseguridad, y el 36% se preocupa por el riesgo de "revelar demasiado" sobre sus propios esquemas de seguridad. Otros problemas incluyen restricciones regulatorias, falta de apoyo de los directores ejecutivos y falta de recursos.

> **Tener un estándar , y decir que las reglas de tu firewall se adecuan a ese estandar, es algo totalmente diferente, que no ofrece detalles intrincados y genera confianza".**
>
> **Mark Thompson**
> CSO de la Asociación Internacional de Profesionales de la Privacidad (IAPP)

La colaboración en ciberseguridad basada en ecosistemas puede ayudar a las organizaciones a anticipar y recuperarse de los ataques

La tabla muestra el porcentaje de encuestados que seleccionaron cada ventaja entre las tres primeras.



Source: KPMG Cyber trust insights 2022

Hay soluciones prácticas, según Mark Thompson, CSO de la Asociación Internacional de Profesionales de la Privacidad (IAPP). "Si te doy los parámetros de mi firewall, existe el riesgo de que veas alguna vulnerabilidad o una brecha", explica. "Pero tener un estándar y decir que las reglas de firewall cumplen con el mismo, es algo que no ofrece detalles intrincados y ayuda a la confianza".

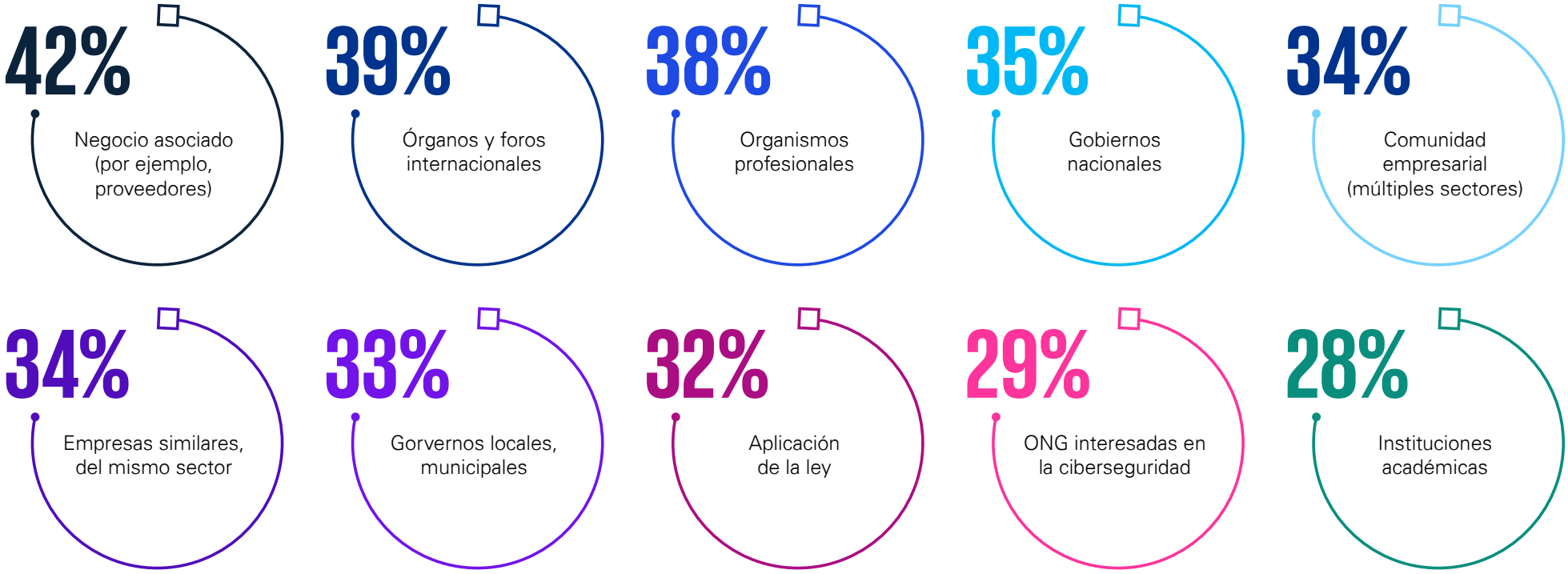
La inmadurez de los estándares de intercambio de información y las mejores prácticas puede ayudar explicar por qué menos de la mitad de las empresas colaboran o intercambian información con socios clave. Mientras que el 79% dice que el compromiso constructivo de los proveedores es crucial para una ciberseguridad efectiva, solo el 42% de los encuestados dijo que realmente estaban trabajando juntos para lograrlo.

Pero esta renuencia puede causar daños graves. Más de la mitad de las empresas admiten que no saben si sus defensas son lo suficientemente fuertes como para prevenir que los ciberdelincuentes ataquen las vulnerabilidades de la cadena de suministro y la contratación de bienes y servicios.

Este enfoque más limitado de la colaboración no puede continuar porque impide que se ofrezca suficiente protección a las organizaciones y ecosistemas, disminuyendo la confianza entre ambos. No por casualidad, el 53% de los encuestados teme que sus respectivas organizaciones no sean lo suficientemente proactivas en sus colaboraciones de ciberseguridad.

Se necesitan más colaboraciones de ciberseguridad en todo el ecosistema

El gráfico muestra el porcentaje de encuestados que seleccionaron todas las opciones que se aplicaban a sus respectivos casos.



Fuente: KPMG Cyber trust insights 2022

Perspectiva KPMG: el valor de la unidad

La construcción efectiva de comunidades es crucial para abordar los desafíos de ciberseguridad: las organizaciones individuales deben trabajar juntas. Sin embargo, los problemas relacionados con la gestión de riesgos, la reputación, la ley y la estrategia aún pueden evitar cumplir con este objetivo.

Ninguna organización puede abordar estos desafíos por sí sola. Por lo tanto, es importante combinar los recursos y coordinarlos de manera efectiva trabajando juntos, tanto las organizaciones públicas como las privadas ganan.

Para generar confianza y espíritu comunitario, cada parte debe identificar las barreras y las formas de superarlas. Por ejemplo, algunas organizaciones utilizan protocolos existentes, como el marco de ciberseguridad del NIST, para desarrollar un lenguaje y terminología comunes al establecer asociaciones con otras organizaciones. Hay empresas que prefieren priorizar en cómo la información propietaria permanecerá en la organización. Los acuerdos de cooperación basados en principios operativos comunes pueden ayudar a establecer relaciones y apoyar la infraestructura digital, manteniendo al mismo tiempo la privacidad y fortaleciendo la confianza mutua.

También es necesario reconocer que el paradigma de seguridad tradicional es menos pertinente en un escenario interconectado. En esto, el enfoque debe estar en la resiliencia. Entonces, en lugar de tratar de derrotar a los malos actores a través del aislamiento y el control de los sistemas, uno debe buscar un enfoque más coordinado y cooperativo.

Prasad Jayaraman
El socio líder de servicios de seguridad cibernética
de KPMG en los Estados Unidos

4

La evolución del CISO

La contribución del CISO al desarrollo de la confianza

El CISO

Los CISO a menudo eran vistos como aquellos que restringían los cambios; ahora, deben ser cada vez más reconocidos como "fundamentales" para hacerlos factibles. Actuando como guardianes de la confianza de la organización, tienen todo para proporcionar la base para el éxito.

"Los CISO pueden aumentar y mejorar la confianza; pero por lo general lo que hacen es actuar sobre sus prioridades organizativas", explica Mark Thompson de IAPP. Existe la necesidad de que comiencen a ayudar a la organización a impulsar y transformar la dinámica", dice.

Los propios CISO reconocen lo que está en juego: el 77% de los encuestados dice que aumentar la confianza es un objetivo clave de sus programas de riesgo cibernético.

Y las organizaciones muestran altos niveles de confianza en sus capacidades de ciberseguridad: el 74% dice que ha visto mejoras en la ciberseguridad en los últimos 12 meses. Esta confianza se combina con una gran creencia en la capacidad del CISO para realizar tareas cruciales.

Pero, ¿confían estos profesionales en su propia capacidad para cumplir con estas expectativas?

Las organizaciones muestran altos niveles de confianza en CISO

El gráfico muestra el porcentaje de encuestados que clasifican cada actividad como "efectiva".

- **80%** Servicio Requisitos legales de la empresa en materia de ciberseguridad y protección de datos
- **80%** Poner en práctica la tecnología que protege los datos cliente/cliente/socio de manera efectiva
- **80%** Implementación de tecnología que protege los activos de TI de los ataques
- **79%** Investigación y mitigar el efecto de los ataques cibernéticos y las violaciones de datos
- **79%** Mayor transparencia Uso de datos y privacidad/protección de datos
- **78%** Diseminación y conciencia de los problemas de ciberseguridad
- **78%** Construcción de relaciones con organismos reguladores para crear un sentimiento de confianza mutua
- **78%** Manejo de las relaciones con las partes interesadas y los mensajes públicos después de una violación cibernética
- **78%** Apoyo a socios internos en la transformación empresarial
- **77%** Fortalecimiento de la ciberseguridad de los terceros y la cadena de suministro

Fuente: KPMG Cyber trust insights 2022

Es interesante que muchos CISO estén luchando por tener autonomía para perseguir sus objetivos. "Puede haber conversaciones difíciles", dice Ann Johnson, de Microsoft. "¿Qué datos vamos a compartir? ¿Cómo vamos a almacenarlos y utilizarlos desde un punto de vista IA-ML? ¿Cómo vamos a protegerlos? El CISO tiene que estar involucrado en cada una de estas conversaciones, que no siempre son fáciles", agrega Johnson.

Casi dos tercios de los encuestados (65%) dicen que la seguridad de la información es vista por sus organizaciones como una actividad de reducción de riesgos, y no como impulsores de negocios. Además, el 57% dice que los líderes senior no entienden los beneficios competitivos de la mayor confianza generada por una mejor seguridad de la información.

Construir una relación con los líderes sénior

Sería poco realista e injusto esperar que los directores de TI aumenten por sí solos la confianza en la privacidad.

Sus interacciones con otros sectores y líderes son fundamentales. Si la colaboración es eficaz, entonces pueden producirse cambios significativos que se reflejan en una mayor confianza.

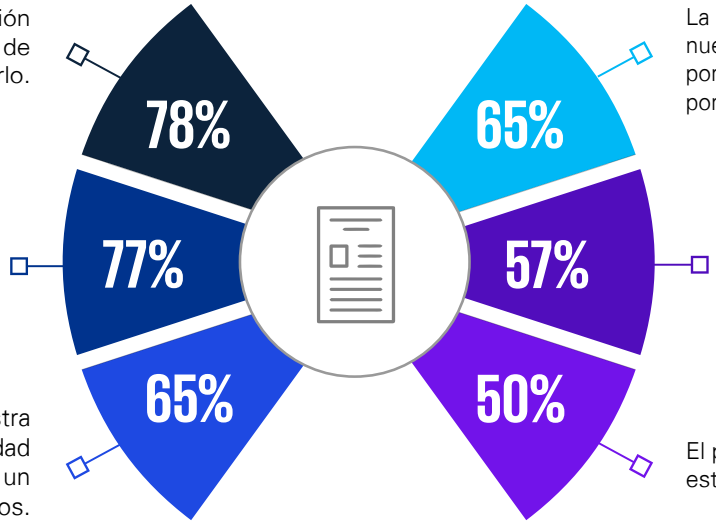
La buena noticia es que los líderes más influyentes creen que los CISO y el área de ciberseguridad deben involucrarse en la transformación desde el principio.

Según el 45% de los encuestados que ocupan puestos de mando, el CISO es un ejecutivo clave, cuya relevancia se ha visto impulsada en los últimos tiempos, gracias a la transformación digital, la necesidad de combatir el cibercrimen y el aumento de las regulaciones.

Los CISO deben tener en cuenta que las cuestiones técnicas seguirán en sus manos; pero es importante que también se centren en las necesidades comerciales y busquen garantizar que las estrategias cibernéticas se alineen con otras, como la estrategia, la planificación, la inversión y la entrega de resultados.

Los CISO están listos para ir más allá, pero ¿se les permite hacerlo?

El gráfico muestra el porcentaje de encuestados que están totalmente de acuerdo con las afirmaciones.



Nuestro equipo de seguridad de la información entiende su papel para garantizar la seguridad de la organización y se siente seguro de hacerlo.

La seguridad de la información en nuestra empresa está determinada por los requisitos de cumplimiento, no por una visión estratégica a largo plazo.

Aumentar la confianza de todas las partes interesadas es fundamental para nuestro programa de riesgo cibernético

Nuestros líderes senior no entienden completamente los beneficios competitivos de una mayor confianza que es posible gracias a una mejor seguridad de la información.

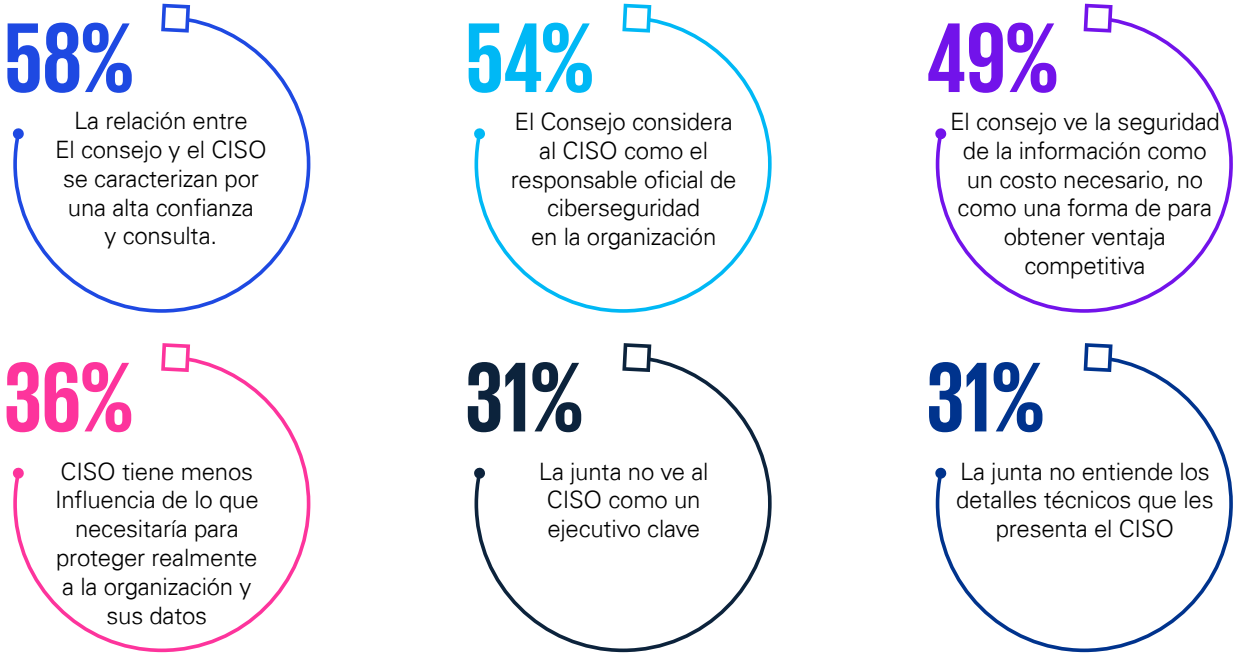
La seguridad de la información en nuestra organización se considera una actividad de reducción de riesgos en lugar de un habilitador de negocios.

El papel del CISO no es tan estratégico como debería ser

Fuente: KPMG Cyber trust insights 2022

Los consejos tienen opiniones encontradas sobre la influencia de los CISO

El gráfico muestra el porcentaje de encuestados que estuvieron de acuerdo con las afirmaciones.



Fuente: KPMG Cyber trust insights 2022

El reto de cuantificar el riesgo

Muchas organizaciones están haciendo un buen progreso en el modelado y la evaluación de riesgos en un área que ha sido notoriamente resistente al análisis. Tres cuartas partes de las organizaciones dicen que han implementado modelos de riesgo para cuantificar visualmente e informar el riesgo cibernético en el tablero, pero solo el 58% describe su enfoque para cuantificar los riesgos cibernéticos como "robusto" y están de acuerdo en que los escenarios de riesgo cibernético se adaptan a las necesidades comerciales.

Más positivamente, el 69% de los encuestados dicen que tienen un enfoque sólido para valorar la confianza digital, en lugar de verla como un concepto abstracto. Y el 65% dice que el modelado de riesgos impulsa la inversión en ciberseguridad, con vínculos claros entre los proyectos y la reducción de riesgos.

Por lo tanto, los CISO deben actuar con más intensidad de lo que ya lo hacen. También es necesario reconocer la naturaleza evolutiva del trabajo, ampliando su alcance en áreas donde existe potencial para estimular la confianza en la organización.

Perspectiva de KPMG: la importancia de medir el riesgo cibernético

Un modelado cuidadoso y la cuantificación puede ayudar a los tomadores de decisiones a comprender el nivel real de exposición al riesgo cibernético de la organización. Esto permite a la gerencia identificar los controles que más contribuyen a reducir ciertas exposiciones cibernéticas, ayudando a garantizar que los recursos se están dirigiendo a las zonas de mayor rendimiento.

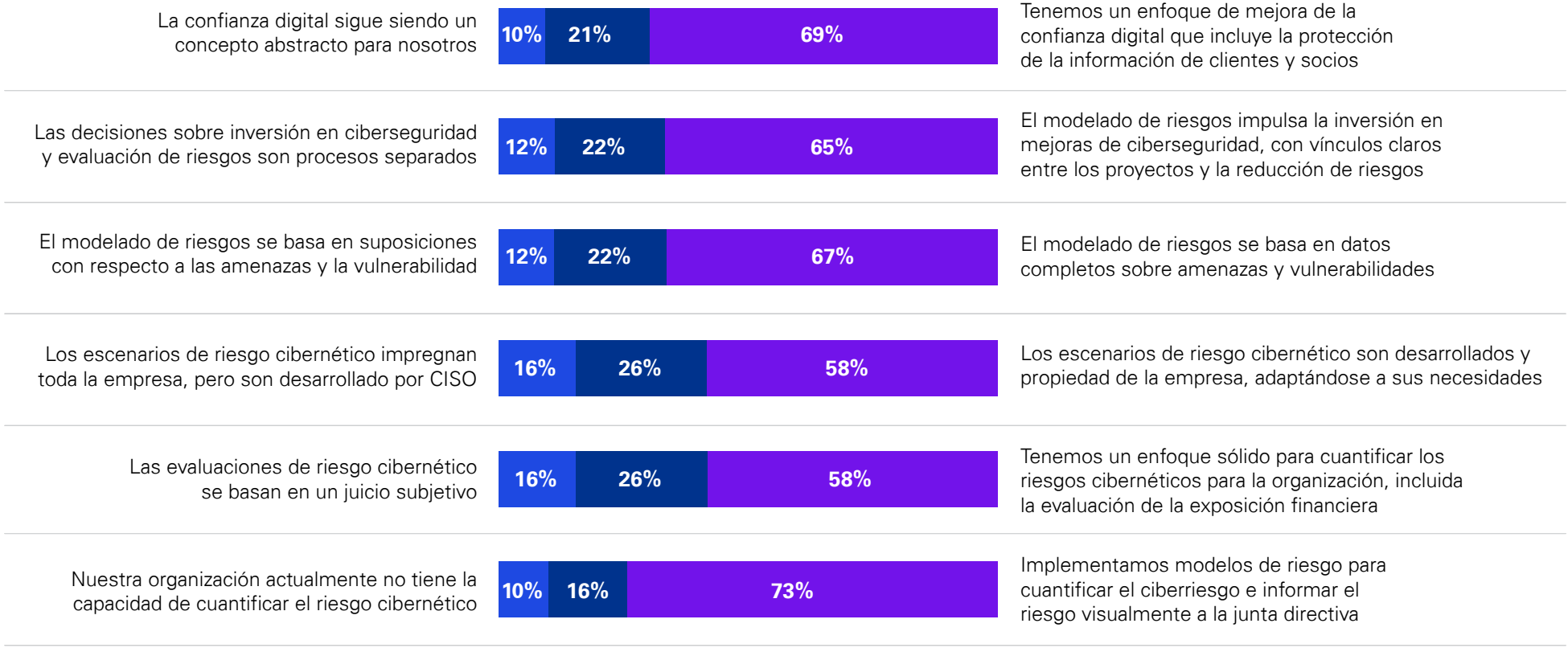
Para hacer esto bien, las organizaciones deben seguir cinco principios:

1. Alinear el modelo de riesgo con las estructuras de riesgo organizacionales.
2. Sea consistente en la definición del riesgo cibernético, considerando posibles eventos de pérdida para el negocio (trazar escenarios es una excelente manera de hacerlo).
3. Utilice el modelado de rutas de ataque para escalar cómo podrían materializarse estos riesgos.
4. Uso de datos del mundo real en los cálculos: las estimaciones de probabilidad e impacto deben contener datos empíricos internos y externos.
5. Comprender los beneficios y limitaciones del modelo y ser transparente al respecto.

James Hanbury
Director de servicios de ciberseguridad
en KPMG uk

Muchas organizaciones están luchando para modelar y evaluar el riesgo cibernético

La tabla muestra el porcentaje de encuestados que señalaron las siguientes afirmaciones como más (o menos) alineadas con la realidad de sus respectivas organizaciones.



Fuente: KPMG Cyber trust insights 2022

5

Misión alcanzable

Cómo las organizaciones pueden generar confianza con la ayuda del CISO

Los ejecutivos entienden por qué es importante aumentar la confianza en sus organizaciones y ecosistemas. Están comprometidos a hacer del CISO un líder en este viaje. Ciberseguridad y privacidad.

son elementos clave para ganarse la confianza de los clientes, los reguladores y el público, abordando también cuestiones ESG.

Los propios CISO reconocen su responsabilidad de impulsar este objetivo y valoran que sus otros pares, es decir, los otros líderes de la organización, sean parte de este viaje. Sin embargo, nuestra investigación muestra que muchos están luchando para cumplir con este papel, pero aún no tienen una visión clara de lo que realmente significa la confianza digital y de qué manera pueden contribuir a lograrlo.

No es que este sea un trabajo que cualquier CISO pueda hacer por sí solo. Es esencial que haya apoyo de la alta dirección, colaboración de otras áreas y cooperación productiva con socios externos y terceros.

Aún así, el CISO es un campeón vital, la definición explícita de confianza puede ser un buen punto de partida, seguido del uso de la ciberseguridad y la privacidad como una forma de generar confianza en la organización, con todas las ventajas competitivas que puede proporcionar.

¿Y cómo hacerlo?

Cinco pasos cruciales para generar confianza a través de la ciberseguridad y la privacidad

01

Tratar la privacidad y la ciberseguridad como prioridades

Incorpore la ciberseguridad y la privacidad en los procesos comerciales, la gobernanza y la cultura de la organización, convirtiéndolos en una parte integral del negocio en lugar de un proceso de costos operativos requerido por el cumplimiento.

02

Cree colaboraciones internas e impulse la confianza

Trabaje con colegas con sus compañeros para ayudar a establecer, integrar y mantener la confianza digital.

03

Cambiar el tamaño del rol del CISO

Adopte una agenda más amplia y reconozca la capacidad de hacer contribuciones integrales en áreas que van desde cuestiones ESG hasta ética de la IA.

04

Apoyo de los líderes e inversión en confianza

Los CISO que obtienen el apoyo de la junta enfrentan menos dificultades para impulsar la agenda de confianza. Esto significa transformar el papel del CISO, es decir que pase de ser solo un protagonista técnico para transformarse en un habilitador estratégico dentro de la organización.

05

Ponte en contacto con el ecosistema

Identificar colaboraciones importantes en el ecosistema de la organización y colabore con ellos, buscando siempre aumentar la confianza y la resiliencia.

Metodología y reconocimientos

Sobre a pesquisa *KPMG Cyber Trust Insights 2022*

Realizado por KPMG entre mayo y junio de 2022, este estudio se basa en entrevistas realizadas con 1.881 ejecutivos y cinco líderes corporativos de todo el mundo. El objetivo central de este trabajo es comprender profundamente el papel que desempeñan la ciberseguridad y la privacidad en la construcción y el mantenimiento de la confianza.

Una proporción significativa de la muestra encuestada está compuesta por líderes senior: el 42% son miembros de la junta o miembros de la junta. Entre los encuestados se encuentran líderes de 31 mercados (24% de la región de Asia y el Pacífico, 50% de Europa, Oriente Medio y África, 16% de América del Norte y 10% de América del Sur) y seis sectores clave de la industria (energía y recursos naturales, servicios financieros, ciencias de la vida e industria farmacéutica, medios de comunicación, entretenimiento y tecnología, sector público y telecomunicaciones).

Entre los encuestados, el 45% tiene ingresos anuales superiores a $ 500 millones; el 23% tiene ingresos superiores a $ 1 mil millones; y el 7% tiene ingresos superiores a $ 5 mil millones.

KPMG agradece a los siguientes ejecutivos por sus contribuciones:

- Bashar Abouseido, vicepresidente sénior y CISO, Charles Schwab
- Ulrich Baisch, CIO da Bechtle
- Allan Cocksaur, CISO da Shell
- Ann Johnson, vicepresidenta corporativa de Microsoft Security Business Development
- Mark Thompson, CSO, Asociación Internacional de Profesionales de la Privacidad (IAPP)

Sobre a KPMG

KPMG es una organización global de firmas independientes que brindan servicios profesionales en las áreas de auditoría, impuestos y consultoría. Estamos presentes en 146 países y territorios. En el año fiscal 2020, el número total de profesionales que trabajan en las firmas miembro en todo el mundo fue aproximadamente 227.000. Cada firma es una entidad legal independiente y separada y se describe a sí misma como tal.

En Brasil, hay aproximadamente 5.000 profesionales distribuidos en 13 Estados y el Distrito Federal, 22 ciudades y oficinas ubicadas en São Paulo (oficina), Belém, Belo Horizonte, Brasilia, Campinas, Cuiabá, Curitiba, Florianópolis, Fortaleza, Goiânia, Joinville, Londrina, Manaus, Osasco, Porto Alegre, Recife, Ribeirão Preto, Río de Janeiro, Salvador, São Carlos, São José dos Campos y Uberlândia.

Guiado por su propósito de potenciar el cambio, KPMG se ha convertido en una empresa de referencia en el segmento en el que opera.

Compartimos valor e inspiramos confianza en el mercado de capitales y en las comunidades por más de 100 años, transformando personas y empresas y generando impactos positivos que contribuyan a la realización cambios sostenibles en nuestros clientes, gobiernos y sociedad civil.

Hable con nuestro equipo

Klaus Kiessling
Socio de Seguridad
Cibernética y Privacidad
KPMG en Brasil
E: kkiessling@kpmg.com.br

Algunos de los servicios o servicios descritos en este punto pueden no estar permitidos para los clientes de auditoría de KPMG y sus filiales o entidades relacionadas.

kpmg.com/socialmedia

Elaborado por Evalueserve.

Nombre de la publicación: Perspectivas de confianza cibernética de KPMG para 2022 | Número de publicación: 138298-G | Fecha de lanzamiento: octubre de 2022