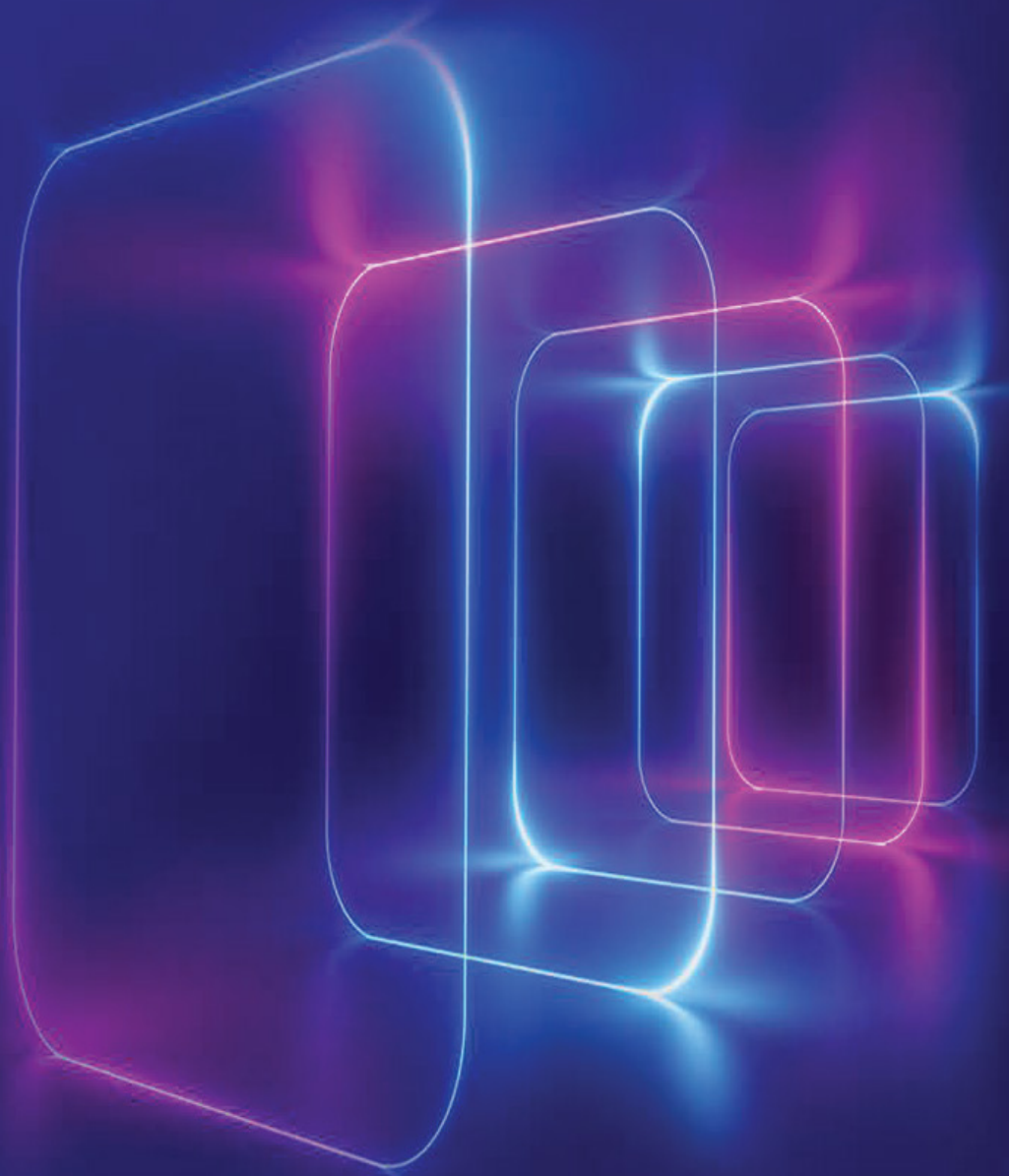
KPMG

Conocimientos en materia de seguridad en el ciberespacio 2022 de KPMG

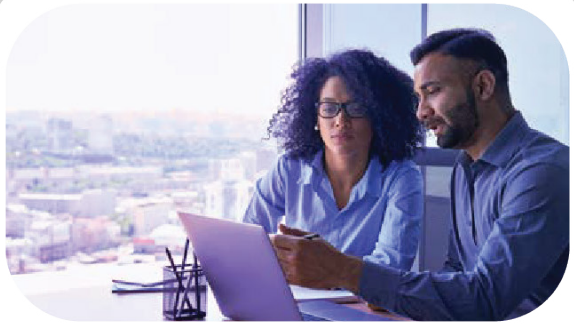


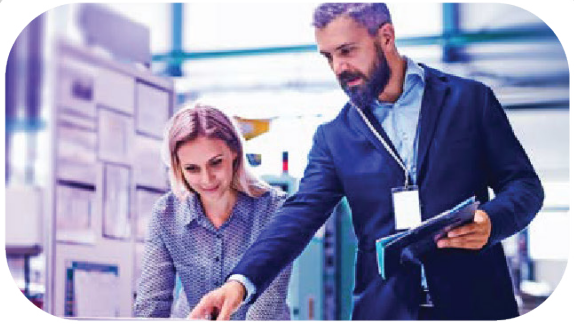
Construir la confianza a través de la seguridad y privacidad en el ciberespacio

KPMG International

kpmg.com/cybertrust

Contenido





Descripción

Cinco pasos fundamentales para erigir la confianza a través de la seguridad y privacidad en el ciberespacio

Para los negocios hoy en día, la seguridad lo es todo. En un ambiente incierto y en constantes cambios, los clientes, empleados e inversionistas se encuentran en la búsqueda de organizaciones en las que puedan confiar plenamente. Sin embargo, erigir y proteger ese sentido de confianza y seguridad requiere que cada segmento de la organización trabaje coordinadamente para brindar una visión coherente y unificada.

Estamos viviendo en un mundo digital y cada parte del negocio depende de elementos como la equidad, integridad y transparencia en el modo como se recopila y procesa información. Los sistemas deben ser resilientes, confiables y capaces de responder rápidamente ante cualquier disrupción. Independientemente de que usted sea un cliente que desea sentirse seguro al momento de llevar a cabo transacciones con una organización, o que forme parte de un ecosistema más amplio de socios, inversionistas, entes reguladores y la sociedad en el que se desenvuelve cada organización – la seguridad en el ámbito digital es de suma importancia.

La seguridad y privacidad en el ciberespacio juegan un papel clave en la edificación y preservación de esa seguridad. Las empresas están acelerando la recopilación de datos, expandiendo el uso de tecnologías basadas en la inteligencia artificial (IA) y el aprendizaje de máquina (ML) - Machine Learning, por sus siglas en inglés -, y adoptando la agenda en materia medioambiental, social y de gobernanza (ESG); mientras afrontan normas regulatorias cada vez más rigurosas.

En el estudio denominado Cyber trust insights 2022 (Conocimientos en materia de seguridad en el ciberespacio) de KPMG, 1.881 ejecutivos fueron encuestados y condujeron a una serie de discusiones con líderes y profesionales corporativos de todo el mundo, con miras a explorar en qué medida los miembros del más alto nivel gerencial reconocen esta situación, cómo se enfrentan al desafío que representa y qué necesitan hacer próximamente. También exploramos el papel clave que juegan los oficiales de seguridad de la información (CISO) al momento de ayudarles con todo lo indicado anteriormente. Identificamos cinco pasos fundamentales para la edificación de la confianza a través de la seguridad en el ciberespacio: **este aspecto de la vida corporativa tiene que ser tratado como un hilo conductor inserto en el tejido empresarial; se deben erigir alianzas a nivel interno; se debe replantear el papel del CISO; se debe garantizar el apoyo por parte de los integrantes del liderazgo; y se debe procurar un alcance total dentro del ecosistema.**

Hallazgos clave

Avalancha de datos

Las empresas están extrayendo datos a gran escala. Por ende, surgen distintas preocupaciones en torno a cómo se protegen, usan y comparten esos datos.

La mayoría de los encuestados han sido partícipes en proyectos más amplios que implican la recopilación o análisis de datos de los clientes durante el año pasado.

La inversión en actividades impulsadas por datos va en aumento como prioridad en las organizaciones.

Retos de la IA y ML

Existen crecientes preocupaciones dentro de la sociedad y las empresas por las implicaciones éticas, de seguridad y privacidad en la adopción de soluciones basadas en IA y ML para grandes proyectos de análisis de datos.

78% concuerda en que la IA y ML traen consigo desafíos únicos en materia de seguridad en el ciberespacio

3 de cada 4 expresa que la IA y ML hacen surgir interrogantes fundamentales en materia de ética.

Valor y confianza

La confianza goza de mayor importancia que nunca, y no sólo se trata de un asunto reputacional. Reforzar la confianza genera ventajas competitivas y se suma a los resultados financieros.

Más de 1/3

de las organizaciones reconoce que el incremento en la confianza conlleva a una mejoría en la rentabilidad.

Sin embargo, el 65%

reporta que los requerimientos en materia de seguridad de la información han sido formulados con base en las necesidades de cumplimientos, en lugar de las ambiciones estratégicas en el largo plazo.

Aumento en las reglamentaciones

Los reguladores están prestando una mayor atención a esta materia, y muchas organizaciones están preocupadas acerca de cómo deberán moverse en un panorama regulatorio global cada vez más complejo.

36% Se preocupa acerca de su capacidad para cumplir con reglamentos de ciberseguridad, nuevos o ya existentes, cuando se tercericen sus actividades a los proveedores de servicios digitales.

34% Se preocupa por sus revelaciones de información corporativa relacionada con la ciberseguridad.

Comunidades de confianza

Se espera que las asociaciones externas también sean vitales para el éxito en los ecosistemas hiperconectados, pero las barreras prácticas se interponen en el camino de la colaboración.

79% Afirma que la colaboración con los proveedores y clientes es vital, pero solo el 42% informa haberlo hecho.

60% Admite que sus cadenas de suministro los dejan vulnerables antes los ataques.

Oficial de seguridad de la Información (CISO) en evolución

¿Las organizaciones reconocen el papel del CISO al momento apoyar en la incorporación de enfoques en la confianza digital?

1/2 De los ejecutivos dudan que la relación entre la junta y el CISO se caracterice por un "alto grado de confianza".

1/3 Afirma que el CISO no está considerado como un ejecutivo clave y ejerce Influencia de la que se requiere para proteger a las organizaciones y su información.

Propósito de confianza

¿Los negocios han reconocido la conexión entre la confianza digital y sus planes de ESG?

Menos de 1 de cada 5 personas

considera que el equipo de CISO es una parte integral del equipo de ESG.

50% Considera que el equipo de CISO tiene un papel muy limitado, o nulo, en ESG.

Fuente: KPMG Cyber trust insights 2022

1

Evolución Digital

El caso de negocios para invertir en la confianza

¿Qué entendemos por confianza?

Una definición clara de la confianza puede ayudar a las empresas a adoptar un papel activo para medirla, aumentarla y desbloquear una amplia gama de beneficios potenciales tangibles.

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

Si bien cada organización tenga distintas prioridades y utilice un lenguaje diferente para describir los aspectos de la confianza digital, el concepto suele abarcar:

Seguridad y fiabilidad
El objetivo es garantizar que la tecnología y los datos de una organización estén bien protegidos, al tiempo que funcionan según lo previsto.

Uso inclusivo, ético y responsable
El objetivo es garantizar que una organización diseñe, construya y opere su tecnología y sus datos como un administrador de las personas, la sociedad en general, su entorno y otras partes interesadas.

Responsabilidad y supervisión
El objetivo es garantizar que una organización defina claramente las responsabilidades de la fiabilidad y asigne y controle dichas responsabilidades.

Por qué es importante: Una mayor confianza puede aumentar los beneficios y la fidelidad de los clientes

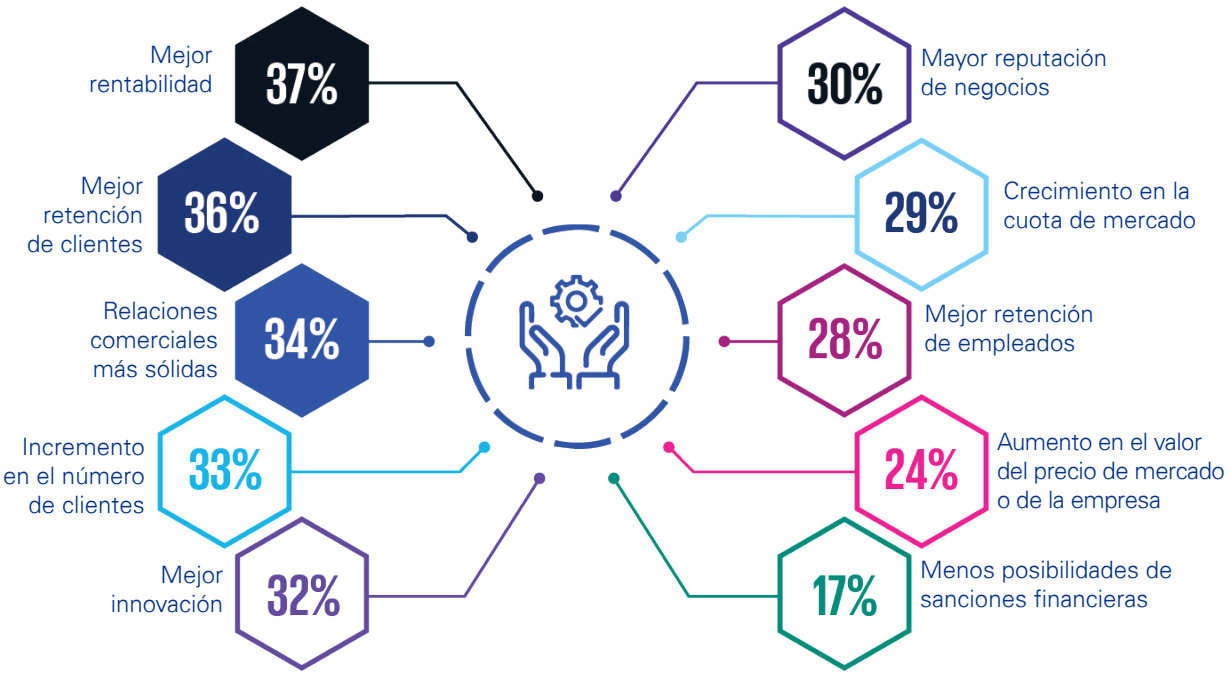
Según nuestros encuestados, los tres principales beneficios esperados de una mayor confianza son:

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

Otros beneficios potenciales son una mayor innovación, una mejor retención de los empleados y una mayor cuota de mercado.

Los principales beneficios de contar con mayores niveles de confianza

El gráfico muestra el porcentaje de encuestados que seleccionaron cada opción entre las tres principales.



Fuente: KPMG Cyber trust insights 2022

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

La transformación digital está muy avanzada: en todos los sectores, las empresas están revisando su tecnología y situando los datos avanzados y los análisis sofisticados en el centro de sus operaciones. En los próximos 3 años, las organizaciones tienen previsto realizar una serie de inversiones en herramientas digitales para impulsar su crecimiento, optimizando sus interacciones con los clientes, agilizando las operaciones comerciales y liberando el valor de sus datos. Cada nueva actividad relacionada con los datos expone a las empresas a posibles vulnerabilidades y a un riesgo para su reputación del que hay que protegerse para mantener la confianza.

Según el informe Global Tech Report de KPMG, **el 61% de las empresas esperan adoptar nuevas plataformas tecnológicas disruptivas en un plazo de 2 años** y, en los próximos 3 años, afirman que aumentarán su inversión en el Internet de las cosas (IoT), la computación de borde y el 5G y, en menor medida, la realidad virtual (VR) y la realidad aumentada (AR).

En el mismo informe de KPMG, **la digitalización de los canales de los clientes se cita como el segundo reto más grave en materia de ciberseguridad al que se enfrentan las organizaciones, solo por detrás de la adopción de entornos de trabajo híbridos**. Preguntamos a las empresas dónde estaban invirtiendo en su experiencia digital. El 37% de las empresas se centra en el uso de datos de experiencia para personalizar las interacciones digitales en tiempo real, mientras que el 36% invierte en la integración multicanal para mejorar la experiencia del cliente.

A medida que estas tendencias se aceleran en todos los sectores, las expectativas de privacidad de los clientes también están cambiando. Cada vez más, los usuarios esperan poder personalizar los controles de privacidad a través de sus dispositivos y canales, lo que requiere que las organizaciones incorporen controles flexibles en el diseño de futuros productos y servicios.

Las principales áreas de inversión en experiencia digital

El gráfico muestra el porcentaje de encuestados que seleccionaron cada opción entre las tres principales.

Fuente: KPMG Cyber trust insights 2022

> **Proteger la confianza del cliente es lo que impulsa nuestras inversiones en ciberseguridad y privacidad".**
>
> **Bashar Abouseido**
> SVP y CISO, Charles Schwab

La ciberseguridad está cambiando y los datos han cobrado más importancia que nunca

En este contexto, las empresas deben reforzar sus salvaguardias en las áreas que son cruciales para asegurar la confianza de los interesados. Más del 80% de nuestros encuestados reconocen la importancia de mejorar la ciberseguridad y la protección de los datos, incluyendo una mayor transparencia en el uso de los mismos. En particular, el 51% consideró que la protección de los activos informáticos frente a los ataques era extremadamente importante.

A medida que las organizaciones impulsan la transformación digital, el presupuesto para la inversión en ciberseguridad y privacidad debe seguir, y cada vez más ser visto como parte integral de esas iniciativas estratégicas. "El éxito de los servicios digitales transformacionales dependerá probablemente de que las organizaciones puedan entrelazar la seguridad y la privacidad en su diseño e implementación", afirma Allan Cockriel, CISO de Shell. Además, señala que "nos estamos centrando en lo que llamamos "estándares de seguridad por diseño" en la forma en que construimos la tecnología. Queremos que esos estándares sean transparentes para nuestros clientes porque nuestra obligación es mantener y mejorar la confianza".

"Proteger la confianza de los clientes es lo que impulsa nuestras inversiones en ciberseguridad y privacidad", dice Bashar Abouseido, SVP y CISO de Charles Schwab. "Vamos más allá para mantener la confianza que tenemos con nuestros clientes tanto a través de la mejora proactiva y continua de los controles de privacidad como de la transparencia en torno a cómo protegemos sus datos".

Perspectiva de KPMG: La confianza se está convirtiendo en algo fundamental para el éxito de la tecnología emergente

Las tecnologías emergentes, como la tecnología de libro mayor distribuido (DLT), la computación cuántica, las redes 5G, la IA/ML y la realidad aumentada y virtual, se están desarrollando rápidamente y prometen transformar la forma de operar de las empresas.

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

Atul Gupta
Socio y Director de Servicios de Confianza Digital y Ciberseguridad KPMG en la India

2

Tendencias en confianza digital

Conociendo los impulsores de confianza

Afrontar los retos éticos de la IA

El creciente uso de las tecnologías de IA y ML en muchas empresas está creando un nuevo (y, hasta la fecha, mal entendido) conjunto de problemas de confianza. La investigación de KPMG muestra que las empresas están decididas a adoptar la IA y el ML, con beneficios esperados que van desde el aumento de la eficiencia y la productividad hasta la mejora de la capacidad de generar conocimientos predictivos sobre los clientes y los mercados.

El peligro real es que estas tecnologías, si se manejan mal, plantean riesgos de ciberseguridad y privacidad con potencial de daño a la reputación y sanción regulatoria.

Las organizaciones están empezando a reconocer estos riesgos. Más de tres cuartas partes de nuestros encuestados (78%) están de acuerdo en que la IA y el ML plantean retos de ciberseguridad únicos.

Casi la misma cantidad cree que hay cuestiones éticas fundamentales que resolver a medida que adoptan estas tecnologías y dicen que las organizaciones tendrán que comunicar más abiertamente cómo están gestionando esas cuestiones.

Todo ello resalta el importante papel que desempeñan los equipos de ciberseguridad y privacidad para ayudar a dar forma al debate ético y gestionar los riesgos.

"Estamos trabajando mucho en la IA adversa -cosas como el envenenamiento de datos, la deriva de la máquina, los ataques de IA- porque creemos que será la próxima ola de ataques", dice Ann Johnson, Vicepresidenta Corporativa de Desarrollo de Negocios de Seguridad de Microsoft.

La IA y el ML crean nuevos retos para el equipo de seguridad de la información

El cuadro muestra el porcentaje de encuestados que está de acuerdo o muy de acuerdo

78%	76%	76%	76%	75%
La adopción de AI/ML conlleva retos únicos de ciberseguridad que requieren atención especial	La adopción de AI/ML requiere que establezcamos custodias adicionales acerca de cómo entrenamos los sistemas de AI/ML y monitoreamos su desempeño	La adopción de AI/ML requiere que seamos más transparentes en cómo transmitimos el uso de las técnicas de AI/ML	La adopción de AI/ML trae consigo inquietudes éticas que requieren de supervisión y gobernabilidad minuciosa	La adopción de AI/ML trae consigo preocupaciones claves acerca de cómo agregamos y analizamos datos de clientes y socios

Fuente: KPMG Cyber trust insights 2022

Perspectiva de KPMG: IA Ética

Las organizaciones saben que deben orientarse a los datos o se arriesgan a ser irrelevantes. Muchas están ampliando 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 impulsar la desigualdad y violar la privacidad, además de limitar la capacidad de toma de decisiones autónomas e individuales.

No se puede culpar simplemente al propio sistema de IA de los resultados no deseados. Una IA ética y de confianza no es un lujo, sino una necesidad empresarial. Un número cada vez mayor de líderes empresariales lo reconocen, pero la confianza no se asegura sin esfuerzo ni desafíos.

Además, lo que se considera ético y digno de confianza en un sector o región puede no serlo en otro. No existe una solución única para todos los casos y copiar los marcos existentes es ineficaz. Una IA digna de confianza sólo puede lograrse con un enfoque holístico, independiente de la tecnología y ampliamente respaldado de la concienciación, la gobernanza de la IA y la gestión de riesgos.

Por ejemplo, las evaluaciones del impacto de la IA deben incluir a las partes interesadas adecuadas para identificar los riesgos. La IA debe alinearse con los valores de la organización y de las partes interesadas. Las organizaciones deben evaluar cuidadosamente el cumplimiento de las leyes y reglamentos, así como el rendimiento de la inversión en IA. Las decisiones deben ser rastreables y auditables. Y todas estas protecciones deben aplicarse sin impedir la innovación.

Sander Klous
Socio, Desarrollo de Negocios D&A
KPMG en los Países Bajos

> “Estamos trabajando mucho en la IA adversaria porque creemos que será la próxima ola de ataques”
>
> **Ann Johnson**
> Vicepresidente corporativo
> *Microsoft Security Business Development*

El panorama normativo

A medida que aumenta la preocupación de la sociedad por la confianza digital, también lo hace el interés de los legisladores y reguladores, con mayores exigencias de transparencia y supervisión. Según la encuesta Cyber trust insights 2022 de KPMG:

36%

de los encuestados se preocupan por su capacidad para cumplir con la regulación existente o nueva en materia de ciberseguridad cuando las actividades se subcontratan a proveedores de servicios digitales.

34%

se preocupan por la divulgación de informes corporativos relacionados con la ciberseguridad.

31%

se preocupan por las crecientes exigencias en torno a las infraestructuras críticas, que son objeto de una creciente regulación en el Reino Unido, la UE y los Estados Unidos.

Para aumentar la carga, las organizaciones internacionales deben hacer frente a un tapiz cada vez más complejo, diverso y a veces contradictorio de regulación extraterritorial. “Uno de los retos para los CISO es que las partes interesadas de las distintas regiones interpretan de forma diferente la misma normativa”, afirma Ulrich Baisch, CIO de Bechtle, uno de los mayores proveedores de TI de Europa. “Hay que tener un concepto claro de lo que se puede y no se puede hacer”.

Perspectiva de KPMG: Impulsores reglamentarios

A nivel mundial, el crecimiento de la normativa sobre ciberseguridad y privacidad se está acelerando. Más de 137 países cuentan ya con algún tipo de régimen de protección de datos, que a menudo reclaman una jurisdicción extraterritorial sobre los servicios ofrecidos en el país o los datos de los ciudadanos de ese país. Los regímenes de protección de la intimidad más maduros están entrando en una segunda generación de regulación, al tiempo que se enfrentan a nuevos retos en materia de privacidad impulsados por la adopción de la tecnología. Por ejemplo, los debates sobre la regulación de la IA se están formalizando en proyectos de ley.

Además, los países están aplicando reglamentos de ciberseguridad de infraestructuras críticas cada vez más estrictos, a medida que aumenta la preocupación por los ataques a los sistemas de control industrial. Estas regulaciones están pasando de la autoevaluación a marcos de control más directivos, incluyendo la notificación obligatoria de incidentes y la auditoría externa.

Los reguladores también están siendo más cuidadosos con sus marcos de control, al tiempo que buscan reforzar la independencia del CISO y su función en el establecimiento de estándares de control.

También están surgiendo requisitos de resiliencia más holísticos, centrados en la recuperación de la empresa en escenarios extremos pero plausibles, en sectores como el financiero.

Los requisitos corporativos de transparencia sobre los riesgos cibernéticos son objeto de debate, junto con los crecientes requisitos de divulgación de los incidentes de ransomware. Las empresas deben invertir para automatizar la supervisión y la presentación de informes sobre el cumplimiento de la normativa, mantener una vigilancia reglamentaria y tener en cuenta las tendencias normativas en materia de privacidad y seguridad a la hora de desarrollar nuevos servicios y productos.

David Ferbrache
Global Head of Cyber Futures
KPMG International

Ver más allá de la normativa

La confianza digital debe formar parte de la agenda de ESG y, por supuesto, la ciberseguridad y la privacidad probablemente formarán parte de ella. "La ESG es parte integral del negocio en su conjunto, pero naturalmente el CISO desempeña un papel clave, en particular cuando se trata de cuestiones sociales y relacionadas con la gobernanza", afirma Ulrich Baisch, de Bechtle.

Pero hay que seguir trabajando para que esto sea una realidad. Menos de una de cada cinco organizaciones describen la seguridad como parte integral del equipo de ESG, y la mayoría afirma que desempeña un papel muy limitado. Las organizaciones también deben reconocer los imperativos sociales y las crecientes expectativas en torno a estos temas.

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

> **"ESG es parte integral de la empresa en su conjunto, pero naturalmente el CISO desempeña un papel clave, en particular cuando se trata de cuestiones sociales y relacionadas con la gobernanza."**
>
> **Ulrich Baisch**
> CIO, Bechtel

Perspectiva de KPMG: ESG y responsabilidad social

Las organizaciones que realmente adoptan la agenda ESG pueden ganarse la confianza de sus clientes y reforzar la fortaleza de sus marcas. En el mundo digital actual, las juntas directivas, los inversionistas, los reguladores, los clientes y el público en general esperan informes transparentes sobre la postura de ciberseguridad y privacidad de la organización. Las partes interesadas quieren tener la certeza de que las juntas directivas y los ejecutivos aprecian las implicaciones sociales de esforzarse por garantizar la resistencia y la integridad de los servicios críticos, al tiempo que protegen la información en la que confían.

Las consideraciones clave para estas partes interesadas incluyen:

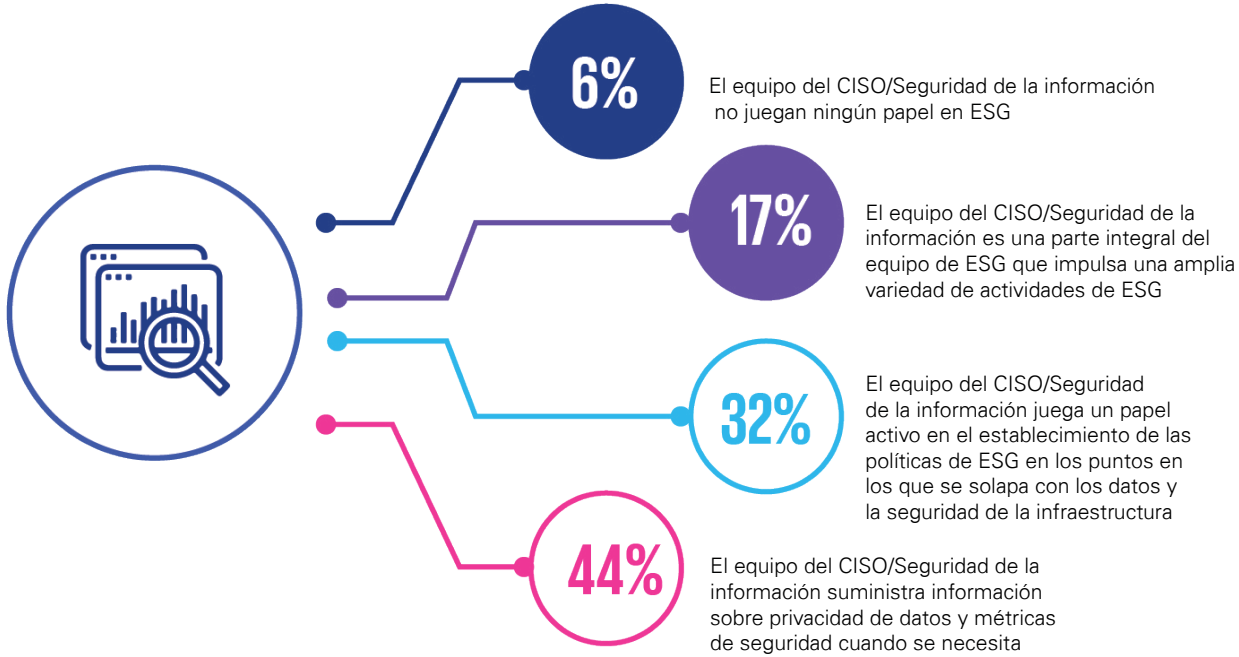
- Monitoreo proactivo de activos digitales para garantizar el acceso a contenido Seguro y confiable en tiempos de creciente explotación y armamento de la información en línea a través de mensajes como '*fake news*' y '*deep fakes*'.
- Ayudar a proteger a los clientes, en particular a los que están por debajo del umbral de la ciber pobreza, contra el fraude y la usurpación de identidad por medios cibernéticos.
- Tratar de garantizar la adopción ética de tecnologías como la IA y el ML, que recogen y analizan los datos de los clientes.
- Mantener la fiabilidad, integridad y disponibilidad de los servicios digitales en los que, como sociedad, hemos llegado a confiar.
- Demostrar un compromiso más amplio con la creación de habilidades y capacidades cibernéticas, dentro de su ecosistema de proveedores y más allá.

Srinivas Potharaju
Socio, Confianza Digital
KPMG en India

Siddharth Durbha
Director, Confianza
Digital KPMG en India

La mayoría de los CISO sólo participan de forma pasiva en las políticas y actividades ESG

El gráfico muestra el porcentaje de encuestados que seleccionaron una opción como la principal.



Fuente: KPMG Cyber trust insights 2022

Perspectiva de KPMG: Impulsar la confianza yendo más allá del mínimo reglamentario

Las organizaciones con visión de futuro están incorporando métricas de privacidad de datos en los marcos de información ESG. Esto les permite fomentar la confianza al tiempo que ayudan a garantizar que se cumplen, como mínimo, los requisitos normativos. A menudo, como parte del impulso de una mayor confianza, las organizaciones buscan proactivamente superar las normas mínimas reglamentarias, para que las partes interesadas se sientan más seguras de que su información de identificación personal se está recopilando, utilizando o divulgando de forma adecuada, no sólo desde una perspectiva legal, sino desde una perspectiva que encaja con la narrativa ESG articulada de la organización".

Sylvia Klasovec Kingsmill
Líder Global de Privacidad
KPMG International y Socia
KPMG en Canadá

3

Construir una comunidad de confianza

El poder de la colaboración y la sociedad

Las empresas digitalizadas de hoy en día no operan en el vacío; cada vez más, son miembros activos de asociaciones y colaboraciones más amplias. Esto se suma al reto al que se enfrentan los equipos de ciberseguridad: deben crear fe en los ecosistemas que habitan sus organizaciones, colaborando con los socios para ayudar a garantizar la confianza mutua, y la confianza en el ecosistema en su conjunto.

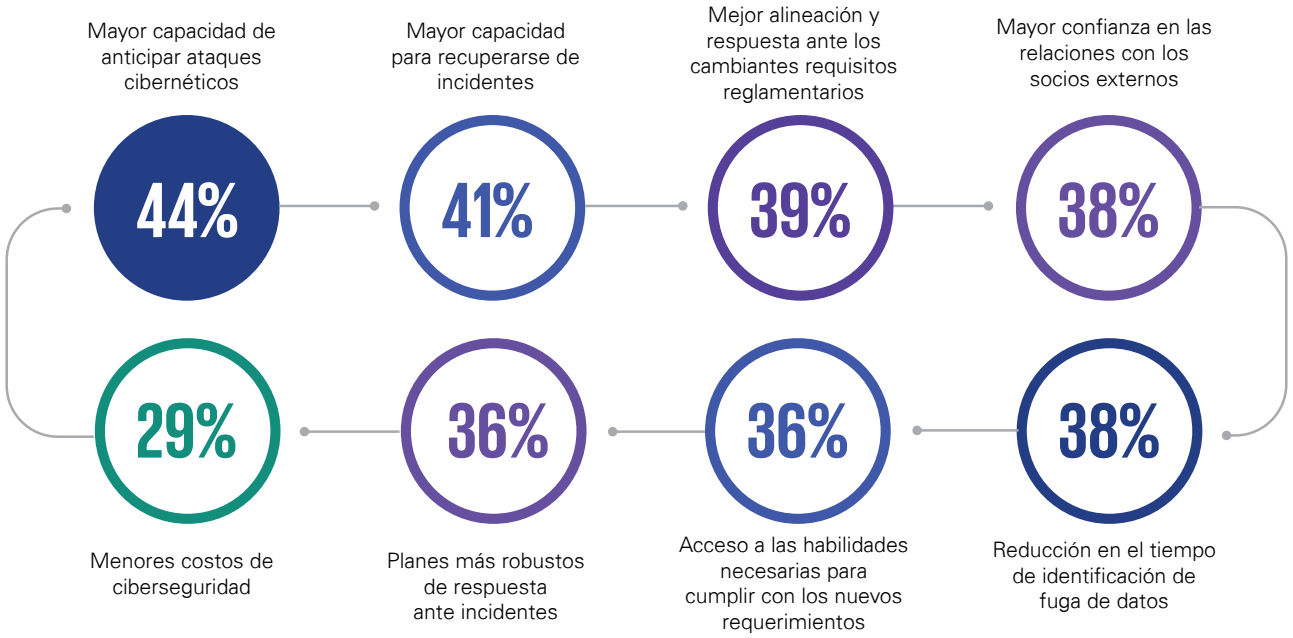
La unión hace la fuerza. En la encuesta Cyber trust insights 2022 de KPMG, casi la mitad de los encuestados (44%) afirma que la colaboración en materia de ciberseguridad en todo el ecosistema les ayudará a anticiparse a los ataques, por ejemplo.

Aunque la colaboración puede ser deseable, no siempre es sencilla. Más de un tercio de los encuestados (38%) afirma que las preocupaciones sobre la privacidad se interponen en el camino de las asociaciones externas de ciberseguridad, y al 36% le preocupa revelar demasiado sobre sus propios acuerdos de seguridad. Otros problemas son las restricciones normativas, la falta de apoyo de los directivos y la falta de recursos.

> **Disponer de una norma y decir que las reglas del cortafuegos cumplen esa norma es un dato completamente diferente que, por lo general, no revela detalles intrincados y ayuda a generar confianza.**
>
> **MarkThompson**
> Chief Strategy Officer, International Association of Privacy Professionals (IAPP)

La colaboración en materia de ciberseguridad en todo el ecosistema puede ayudar a las organizaciones a anticiparse y recuperarse de los ataques

El gráfico muestra el porcentaje de encuestados que seleccionaron cada ventaja entre las tres principales.



Fuente: KPMG Cyber trust insights 2022

Existen soluciones prácticas, según Mark Thompson, Director de Estrategia de la Asociación Internacional de Profesionales de la Privacidad (IAPP). "Si te doy los parámetros de mis reglas de firewall, existe el riesgo de que veas una vulnerabilidad o una brecha", dice. "Pero tener un estándar, y decir que tus reglas de firewall cumplen ese estándar, es un punto de datos completamente diferente que generalmente no revela detalles intrincados y ayuda a permitir la confianza".

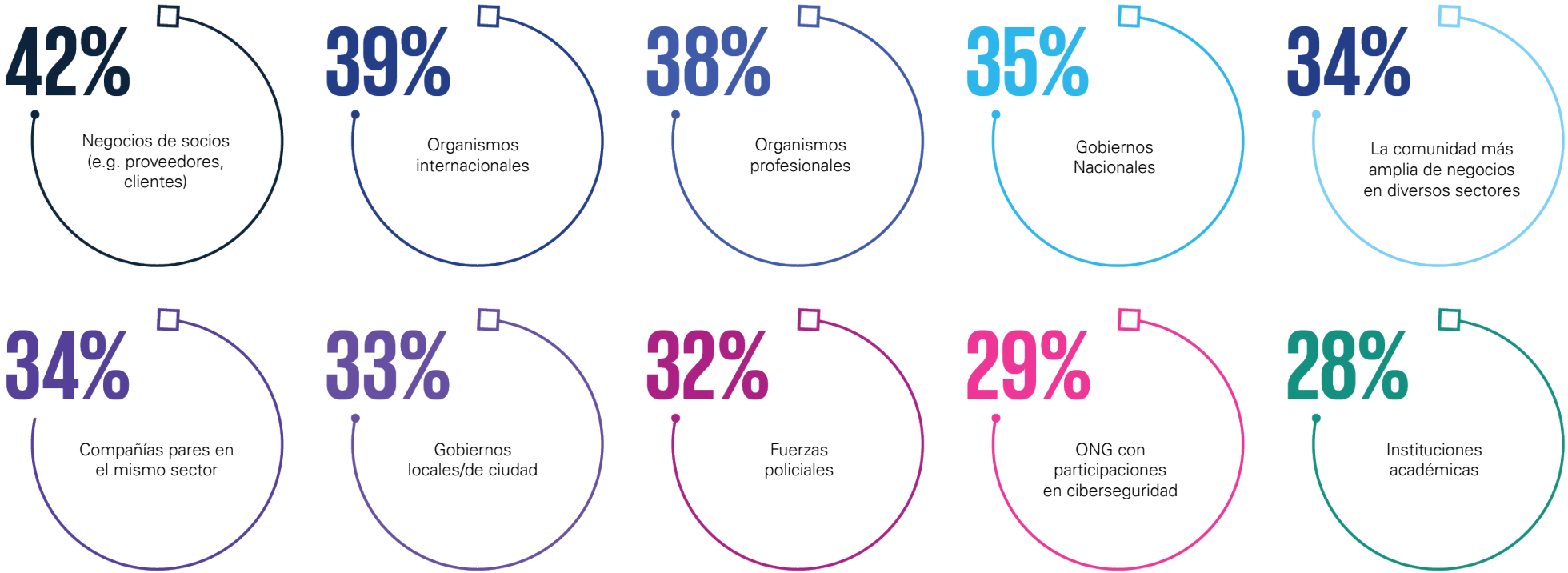
La inmadurez de las normas y las mejores prácticas para compartir información puede ayudar a explicar por qué menos de la mitad de las empresas colaboran o intercambian información con socios clave. A pesar de que el 79% afirma que el compromiso constructivo de los proveedores es vital para una ciberseguridad eficaz, sólo el 42% de los encuestados afirma estar colaborando realmente para conseguirlo.

Pero esta reticencia podría causar graves daños. Más de la mitad de las empresas admiten que no saben si sus defensas son lo suficientemente fuertes como para impedir que los atacantes exploten las vulnerabilidades de la cadena de compras y suministro.

Este enfoque más limitado de la colaboración no puede continuar; no ofrece suficiente protección ni a las organizaciones individuales ni a sus ecosistemas, lo que socava la confianza en ambos. A más de la mitad de nuestros encuestados (53%) les preocupa que sus organizaciones no sean lo suficientemente proactivas en sus colaboraciones de ciberseguridad, y puede que tengan razón.

Se necesitan más asociaciones de ciberseguridad en todo el ecosistema

El gráfico muestra el porcentaje de encuestados que seleccionaron todas las opciones aplicables.



Fuente: KPMG Cyber trust insights 2022

Perspectiva de KPMG: El valor de la unidad

La creación de una comunidad efectiva es vital para abordar los retos de la ciberseguridad: las organizaciones individuales deben trabajar juntas. Sin embargo, importantes cuestiones relativas a la gestión de riesgos, la reputación, la legislación y la estrategia pueden seguir impidiendo ese objetivo.

Ninguna organización puede hacer frente a estos retos por sí sola, por lo que es importante combinar recursos y coordinarse eficazmente. Trabajando de forma concertada, tanto las organizaciones públicas como las privadas pueden asegurar una mayor eficiencia, perspectivas y recursos.

Para crear confianza y comunidad, cada parte debe reconocer lo que es posible, dónde están las barreras y cómo superarlas. Por ejemplo, algunas organizaciones están utilizando protocolos existentes, como el marco de ciberseguridad del NIST, para crear un lenguaje y una terminología comunes al asociarse con otras organizaciones. Otras se centran en cómo ayudar a garantizar que la información de propiedad se mantenga dentro de la organización. Los acuerdos de cooperación basados en principios operativos comunes pueden ayudar a las organizaciones a desarrollar relaciones y apoyar la infraestructura digital, manteniendo la privacidad y reforzando la confianza mutua entre los socios.

También es necesario reconocer que el paradigma tradicional de la seguridad es menos relevante en un panorama tan interconectado. En su lugar, tiene más sentido centrarse en el pensamiento resiliente. En lugar de intentar derrotar a los malos actores únicamente aislando y controlando los sistemas, es necesario un enfoque más coordinado y cooperativo.

Prasad Jayaraman
Director, Servicios de Ciberseguridad
KPMG en EE. UU

4

La evolución del CISO

La contribución del CISO en el establecimiento de la confianza

Aparece el CISO

A veces se considera que frenan las iniciativas de innovación y crecimiento, pero los CISO están ahora en posición de desempeñar un papel crucial como facilitadores. Al actuar como uno de los últimos guardianes de la confianza de la organización, pueden ser una fuerza impulsora de su éxito.

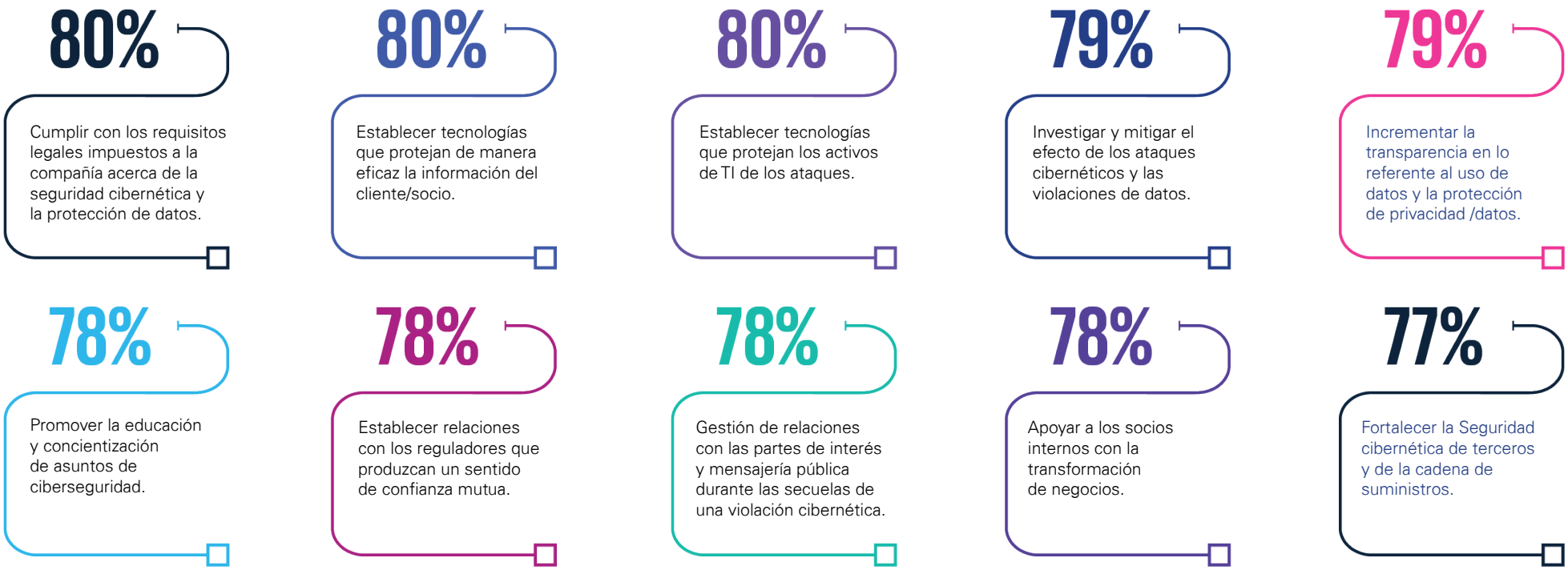
"Los CISO pueden realmente mejorar la confianza, pero a menudo lo que hacen está generalmente impulsado por sus prioridades organizativas", dice Mark Thompson de IAPP. "Existe la necesidad de que empiecen a intervenir en ese espacio: para ayudar a la organización a impulsar y cambiar la dinámica".

Los propios CISO reconocen lo que está en juego. Más de tres cuartas partes de los encuestados (77%) dicen que el aumento de 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% afirma haber visto mejoras en la ciberseguridad en los últimos 12 meses, y más de uno de cada cuatro afirma que lo ha hecho de forma significativa. Esta confianza se combina con una fuerte creencia en la capacidad del CISO para llevar a cabo tareas cruciales.

Pero ¿se sienten los CISO capaces de cumplir con tales expectativas?

Las organizaciones muestran altos niveles de confianza en el CISO
El gráfico muestra el porcentaje de encuestados que califican cada actividad como "eficaz"



Es interesante, entonces, que muchos CISOs estén luchando por conseguir un mandato para perseguir sus objetivos. A menudo puede haber conversaciones difíciles, dice Ann Johnson de Microsoft. "¿Qué datos vamos a compartir? ¿Cómo vamos a almacenarlos? ¿Cómo vamos a utilizarlos desde el punto de vista de la IA-ML? ¿Cómo vamos a protegerlos? El CISO tiene que participar en cada una de estas conversaciones, y no son conversaciones fáciles de mantener", añade Johnson.

Casi dos tercios de los encuestados (65%) afirman que la seguridad de la información es vista por sus organizaciones como una actividad de reducción de riesgos, más que como un factor de negocio. Además, el 57% afirma que los directivos no entienden los beneficios competitivos de la mayor confianza que permite una mejor seguridad de la información. ¿Sugiere esta desconexión que el CISO tiene que hacer más para ofrecer una revisión de la realidad de la ciberseguridad?

Establezca una relación con los altos cargos

Sería poco realista e injusto esperar que los CISO impulsen por sí solos la agenda de la confianza en la ciberseguridad y la privacidad de los datos. Sus interacciones con colegas como el director de datos y el director de privacidad serán probablemente cruciales. Si colaboran eficazmente, este trío puede empezar a realizar cambios prácticos para mejorar la confianza.

La buena noticia es que los líderes más influyentes de las organizaciones creen que los CISO y la función de ciberseguridad más amplia deberían participar en la transformación desde una fase temprana.

El 45% de los encuestados de la alta gerencia ahora ven al CISO como un ejecutivo clave y el perfil del papel del CISO ha crecido rápidamente en los últimos 5 años impulsado por la transformación digital, el crecimiento de la ciberdelincuencia y el aumento de las expectativas reglamentarias.

Una forma de que los CISOs cambien esa perspectiva puede ser desviar el foco de atención de las cuestiones más técnicas - después de todo, más de la mitad de los encuestados de la C-suite dicen que las juntas directivas no los entienden de todos modos. El desafío de entrar en ese papel estratégico sigue siendo para los CISOs. Las empresas exigen que se comprometan a un nivel superior, que se centren en las necesidades de la empresa y que se aseguren de que la cibernética se considera un hilo conductor que atraviesa todos los aspectos de la estrategia, la planificación, la inversión y la ejecución de la empresa.

Los CISO están preparados para dar un paso adelante, pero ¿se les permite hacerlo?

El gráfico muestra el porcentaje de encuestados que están de acuerdo o muy de acuerdo.

Fuente: KPMG Cyber trust insights 2022

Las Juntas Directivas tienen opiniones encontradas sobre la influencia de los CISO

El gráfico muestra el porcentaje de encuestados que indican que las afirmaciones son ciertas.

Fuente: KPMG Cyber trust insights 2022

El reto de cuantificar el riesgo

Muchas organizaciones están haciendo buenos progresos en el modelado y la evaluación de riesgos en un área que se ha resistido notoriamente al análisis. Tres cuartas partes de las organizaciones afirman haber implementado el modelado de riesgos para cuantificar e informar visualmente del riesgo cibernético a la junta directiva, aunque sólo el 58% describe su enfoque para cuantificar los riesgos cibernéticos como "sólido" y está de acuerdo en que sus escenarios de riesgo cibernético se adaptan a las necesidades del negocio.

Más positivamente, más de dos tercios de los encuestados (69%) creen que tienen un enfoque sólido para valorar la confianza digital, en lugar de considerarla sólo un concepto abstracto. Y el 65 por ciento afirma que el modelado de riesgos impulsa la inversión en mejoras de ciberseguridad, con claros vínculos entre los proyectos y la reducción de riesgos.

Por lo tanto, los CISOs necesitan hacer más de lo que hacen hoy, pero también necesitan reconocer la naturaleza evolutiva de su trabajo, ampliando su alcance en áreas donde hay potencial para ayudar a impulsar la confianza en su organización y más allá.

Perspectiva de KPMG: Elogio de la cuantificación del ciberriesgo

Un cuidadoso trabajo de modelización y cuantificación puede ayudar a los responsables de la toma de decisiones a comprender el verdadero nivel de exposición al ciberriesgo de la organización. Esto puede ayudar a la dirección a entender qué controles contribuyen más a reducir determinadas exposiciones cibernéticas y, por tanto, ayuda a garantizar que están centrando sus recursos en las áreas de mayor rendimiento.

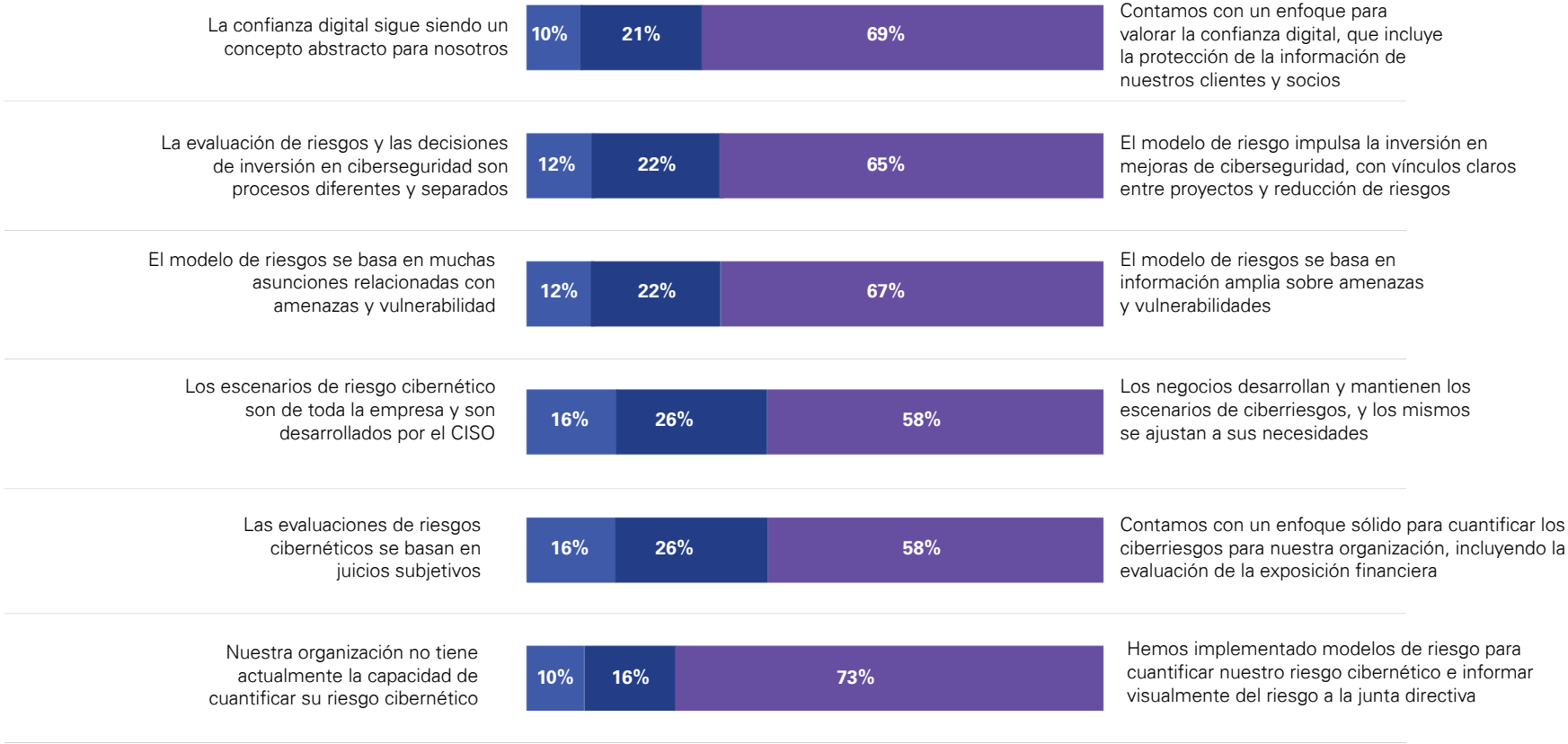
Para conseguirlo, las organizaciones deben seguir cinco principios:

1. Garantizar la alineación del modelo de riesgo con los marcos de riesgo de la organización.
2. Ser coherente en la definición del ciberriesgo como eventos de pérdida potencial para el negocio (los escenarios son una gran manera de hacerlo).
3. Adoptar un enfoque de modelado basado en las amenazas, utilizando un modelo de ruta de ataque para reconstruir cómo pueden materializarse estos riesgos.
4. Utilizar datos del mundo real en los cálculos: las estimaciones de probabilidad e impacto deben basarse en datos empíricos internos y externos (se tiene más de lo que se cree).
5. Comprender las ventajas y limitaciones del modelo y ser transparente al respecto.

James Hanbury
Director de Servicios de Ciberseguridad de KPMG en el Reino Unido

Muchas organizaciones tienen dificultades para modelar y evaluar el riesgo cibernético

El gráfico muestra el porcentaje de encuestados que indicaron las afirmaciones que más reflejan sus organizaciones.



Fuente: KPMG Cyber trust insights 2022

5

Una misión alcanzable

Cómo las organizaciones pueden impulsar la confianza a través del CISO

Los ejecutivos entienden por qué es importante aumentar la confianza en sus organizaciones y sus ecosistemas, y esperan que el CISO sea uno de sus defensores para lograrlo. La ciberseguridad y la privacidad son elementos clave para impulsar la confianza en las mentes de los clientes, los reguladores y el público a través del imperativo ESG. Los propios CISO reconocen su responsabilidad en la consecución de este objetivo por parte de la empresa, al igual que sus colegas de otras partes de la empresa. Sin embargo, nuestra investigación muestra que muchos están luchando para cumplir con esta responsabilidad - tal vez porque carecen de una visión clara de lo que realmente significa la confianza digital y su parte en el logro de la misma.

No es un trabajo que cualquier CISO pueda hacer solo. Necesitan un mayor apoyo de la alta dirección, más colaboración de otras funciones y una cooperación productiva con socios externos y terceros.

Aun así, el CISO es un defensor vital. Definir explícitamente la confianza puede ser un buen punto de partida, seguido del uso de la ciberseguridad y la privacidad como forma de reforzar la confianza en la organización, con todas las ventajas competitivas que ello conlleva.

¿Cómo deberían hacerlo?

Cinco pasos claves para establecer la confianza a través de la ciberseguridad y privacidad

01

Tratar el ciberespacio y la privacidad como un hilo de oro

Incorpore la ciberseguridad y la privacidad a los procesos empresariales, a la gobernanza y a la cultura de la organización, convirtiéndolas en parte integrante del negocio y no en una sobrecarga impulsada por el cumplimiento.

02

Crear alianzas internas para impulsar la confianza

Trabaje con colegas como el director de datos y el director de privacidad para ayudar a establecer, integrar y mantener la confianza digital.

03

Replantear el papel del CISO

Adoptar una agenda más amplia y reconocer la capacidad de hacer contribuciones de amplio alcance en áreas que van desde ESG hasta la ética de la IA.

04

Asegurar el apoyo del liderazgo para la inversión en confianza

Los CISO que se ganan el apoyo de la alta gerencia y la junta directiva probablemente encontrarán más fácil ayudar a impulsar la agenda de confianza. Esto significa transformar al CISO de un papel técnico limitado a un habilitador estratégico dentro de la organización.

05

Acérquese al ecosistema

Identifique a los socios clave dentro del ecosistema de la organización y colabore estrechamente con ellos para ayudar a mejorar la confianza y la resiliencia.

Metodología y reconocimientos

Acerca de las perspectivas de KPMG *Cyber trust insights* 2022

La encuesta KPMG Cyber trust insights 2022, realizada por KPMG International entre mayo y junio de 2022, encuestó a 1.881 ejecutivos y entrevistó a cinco líderes corporativos de todo el mundo para explorar el papel que juegan la ciberseguridad y la privacidad en la construcción y la gestión de la confianza.

Una proporción significativa de la muestra encuestada está compuesta por altos directivos: El 42% son miembros de la junta directiva. Entre los encuestados hay líderes de 31 mercados (24% de ASPAC, 50% de EMA, 16% de Norteamérica y 10% de Sudamérica) y seis sectores industriales clave (energía y recursos naturales, servicios financieros, ciencias de la vida y farmacéutica, medios de comunicación, entretenimiento y tecnología, sector público y telecomunicaciones).

Todos los encuestados tienen ingresos anuales superiores a 100 millones de dólares, el 45% tiene ingresos anuales superiores a 500 millones de dólares, el 23% tiene ingresos superiores a 1.000 millones de dólares y el 7% tiene ingresos superiores a 5.000 millones de dólares.

KPMG desea agradecer a las siguientes personas por sus contribuciones:

— Bashar Abouseido, SVP y CISO, Charles Schwab
— Ulrich Baisch, CIO, Bechtle
— Allan Cockriel, CISO, Shell
— Ann Johnson, Vicepresidenta Corporativa, Desarrollo de Negocios de Seguridad de Microsoft
— Mark Thompson, Director de Estrategia, Asociación Internacional de Profesionales de la Privacidad (IAPP)

Acerca de KPMG

Las firmas de KPMG pueden ayudarle a crear un mundo digital resistente y de confianza, incluso ante la evolución de las amenazas. Los profesionales de la ciberseguridad de KPMG pueden ofrecer una visión multidisciplinar del riesgo, permitiéndole llevar la seguridad a toda su organización, para que pueda anticiparse al mañana, moverse más rápido y obtener una ventaja con una tecnología segura y de confianza.

No importa en qué punto de su trayectoria de ciberseguridad se encuentre, las firmas de KPMG tienen experiencia en todo el proceso, desde la sala de juntas hasta el centro de datos. Además de evaluar su ciberseguridad y alinearla con los profesionales de su negocio, podemos ayudarle a desarrollar soluciones avanzadas, asistirle en su implementación, asesorarle en el seguimiento de los riesgos en curso y ayudarle a responder eficazmente a los incidentes cibernéticos.

Los profesionales de KPMG aprovechan las tecnologías en constante evolución que pueden conectar e impulsar a las empresas, generando confianza y creando y protegiendo el valor, al tiempo que tienden un puente entre el pasado y el futuro.

Creemos juntos un mundo digital de confianza.

Autor y colaboradores

Akhilesh Tuteja
Global Cyber Security Leader
KPMG International and
Partner KPMG in India
atuteja@kpmg.com

Como apasionado líder de la práctica de Ciberseguridad Global, Akhilesh se compromete a ayudar a las organizaciones a utilizar la ciberseguridad para crear confianza y proteger su futuro. Ha asesorado a numerosos clientes en materia de ciberseguridad, estrategia de TI y selección de tecnología, ayudándoles a obtener los beneficios empresariales de la tecnología

Akhilesh ha desempeñado un papel decisivo en el apoyo al sector y es ampliamente reconocido por su sólida combinación de conocimientos empresariales y técnicos. Es un colaborador habitual de publicaciones empresariales y tecnológicas y es un notable conferenciante sobre ciberseguridad y su impacto en las empresas.

Siddharth Durbha
Director, Digital Trust
KPMG in India

Prasad Jayaraman
Principal, Cyber Security Services
KPMG in the US

David Ferbrache
Global Head of Cyber Futures
KPMG International

Sylvia Klasovec Kingsmill
Global Privacy Leader
KPMG International and Partner
KPMG in Canadá

Atul Gupta
Partner and Head of Digital Trust
and Cyber Security Services
KPMG in India

Sander Klous
Partner, D&A Business Development
KPMG in the Netherlands

James Hanbury
Director, Cyber Security Services
KPMG in the UK

Srinivas Potharaju
Partner, Digital Trust
KPMG in India

Contactos

Mónica Barrios
Socia de *Consulting*
y *Cyber Security*
KPMG en Venezuela
E: mbarrios@kpmg.com

kpmg.com/ve