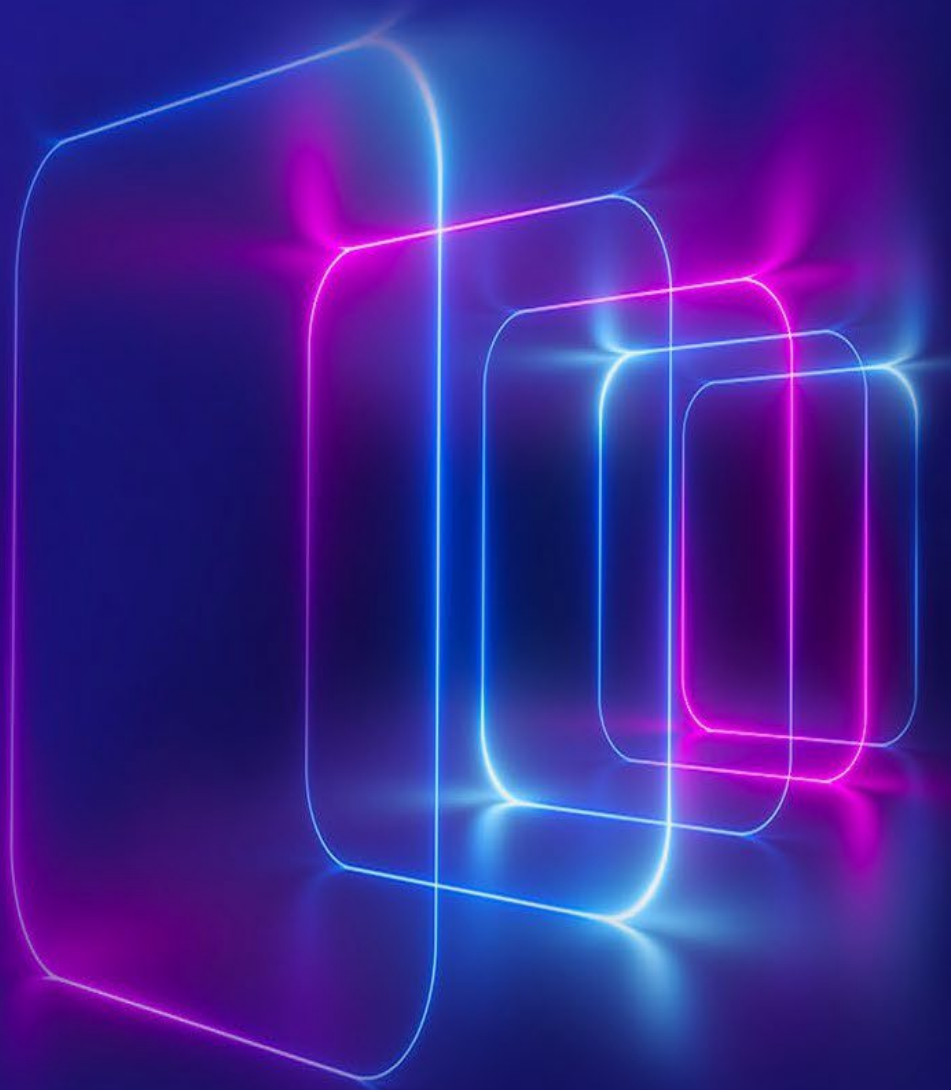
Claves sobre ciberseguridad para 2023

Cómo aportar confianza a través de la ciberseguridad y la privacidad



KPMG España | kpmg.es/ciberseguridad

Índice

Presentación

Cinco pasos cruciales para inspirar confianza mediante la ciberseguridad y la privacidad

Hoy en día, más que nunca, para las empresas, la confianza lo es todo. En un entorno incierto en constante cambio los clientes, los empleados y los inversores buscan organizaciones en las que puedan depositar su confianza. Sin embargo, inspirar y asegurar esta confianza exige que todas las áreas de la organización trabajen conjuntamente para ofrecer una visión coherente y unificada.

En un mundo global y digitalizado cada área de la empresa depende de la equidad, la integridad y la transparencia con la que se recopila y procesa la información. Los sistemas deben ser resilientes, fiables y capaces de responder rápidamente ante una potencial disrupción. No hay duda de que la confianza digital es relevante, tanto si se trata de un comprador o cliente que busca estar seguro al realizar operaciones, como si forma parte de la amplia variedad de grupos de interés de la organización.

La ciberseguridad y la privacidad desempeñan un papel clave en la creación y mantenimiento de esta confianza. En este sentido, las empresas están incrementando la recopilación de datos, ampliando el uso de la Inteligencia Artificial (IA) y las técnicas de aprendizaje automático (ML, por sus siglas en inglés) y adoptando en su agenda aspectos medioambientales, sociales y de buen gobierno (ESG). Todo ello al tiempo que deben cumplir normas regulatorias cada vez más exigentes.

A partir del estudio ‘Claves sobre ciberseguridad para 2023’ realizamos una encuesta a 1.881 ejecutivos. Adicionalmente, mantuvimos una serie de conversaciones con responsables y profesionales de empresas de todo el mundo para explorar en qué medida son conscientes de este reto, cómo lo afrontan y qué pasos necesitan emprender a continuación. Asimismo, exploramos el papel esencial que los responsables de la Seguridad de la información (por sus siglas en inglés, CISO) pueden desempeñar y cómo lograrlo. En consecuencia, se identifican cinco pasos cruciales para inspirar confianza a través de la ciberseguridad: **considerar la ciberseguridad y la privacidad como piedras angulares del negocio; construir alianzas internas; reinventar el papel del CISO; garantizar el apoyo de la Dirección; y llegar a todos los rincones del ecosistema.**

Principales conclusiones

Datos a gran escala

Las empresas están utilizando la extracción de datos a gran escala. Surgen dudas sobre cómo proteger, utilizar y compartir los datos.

La mayoría de encuestados han aumentado la recopilación o análisis de datos de sus clientes.

La inversión en actividades vinculadas con datos está adquiriendo más prioridad para las organizaciones.

Retos de Inteligencia Artificial (IA) y Machine Learning (ML)

Aumentan las dudas de la sociedad y las empresas sobre las implicaciones en materia de ética, seguridad y privacidad que supone adoptar soluciones de IA y ML para análisis de big data.

78% afirma que la IA y el ML suponen retos de ciberseguridad específicos.

3 de 4 manifiestan que la IA y el ML plantean dudas éticas fundamentales.

Valor y confianza

La confianza importa más que nunca, y no es una cuestión únicamente de reputación. Fomentar la confianza genera una ventaja competitiva y mejora los resultados económicos.

Más de 1/3

de las organizaciones es consciente de que una mayor confianza genera un mejor rendimiento.

Pero el 65%

de seguridad de la información están determinados por necesidades de cumplimiento en lugar de por ambiciones estratégicas a largo plazo.

Mayor regulación

Los reguladores están prestando más atención a estas cuestiones, y muchas organizaciones están preocupadas por tener que afrontar un entorno normativo cada vez más complejo.

36% está preocupado por su capacidad para cumplir la legislación ya existente o nueva sobre ciberseguridad cuando se subcontratan actividades a proveedores de servicios digitales.

34% se preocupa por información corporativa relativa a la ciberseguridad.

Comunidades fiables

Se prevé que las alianzas externas también sean cruciales para el éxito en ecosistemas hiperconectados, pero los obstáculos prácticos interrumpen el desarrollo de la colaboración.

79% manifiesta que la colaboración constructiva con proveedores y clientes es vital, pero solo el 42% reconoce llevarla a cabo.

60% admite que sus cadenas de suministro les sitúan en posición vulnerable a ataques.

Evolución del CISO

¿Reconocen las organizaciones el papel que puede desempeñar el CISO para ayudarles a integrar un enfoque a la confianza digital en todos sus ámbitos?

1/2 de los ejecutivos duda de que la relación entre el consejo y el CISO se caracterice por una "elevada confianza".

1/3 manifiesta que no se considera al CISO un ejecutivo clave y tiene menos influencia de la que necesita para proteger a la organización y a sus datos.

Propósito fiable

¿Han reconocido las empresas la conexión entre la confianza digital y su agenda en materia medioambiental, social y de buen gobierno (ESG)?

Menos de 1 de cada 5 considera que el equipo del CISO es parte del equipo ESG.

50% señala que el equipo del CISO desempeña un papel muy limitado o nulo en el área de ESG.

Fuente: Claves sobre ciberseguridad para 2023

1

Evolución digital

El motivo por el que invertir en confianza

¿A qué nos referimos con confianza?

Una definición clara de confianza puede ayudar a las empresas a asumir un papel activo a la hora de cuantificar, incrementar y acceder a una amplia gama de potenciales ventajas.

En este ámbito, la confianza digital se define como la capacidad de una organización para aprovechar la tecnología digital con vistas a proteger sus intereses y cumplir las expectativas y los valores de la sociedad.

Aunque es probable que cada organización tenga prioridades diferentes y utilice un lenguaje diferente para describir aspectos relacionados con la confianza digital, el concepto suele abarcar:

Seguridad y fiabilidad

Con el objetivo de garantizar que la tecnología y los datos de una organización están bien protegidos, al tiempo que funcionan según lo previsto.

Uso inclusivo, ético y responsable

El propósito es asegurar que una organización diseñe, construya y opere su tecnología y sus datos de forma responsable con las personas, la sociedad en general, su entorno y otros grupos de interés.

Rendición de cuentas y supervisión

La finalidad se centra en garantizar que la organización define claramente las responsabilidades en pro de la credibilidad, al tiempo que las asigna y supervisa.

Por qué es importante: el aumento de la confianza puede impulsar los beneficios y la fidelidad del cliente

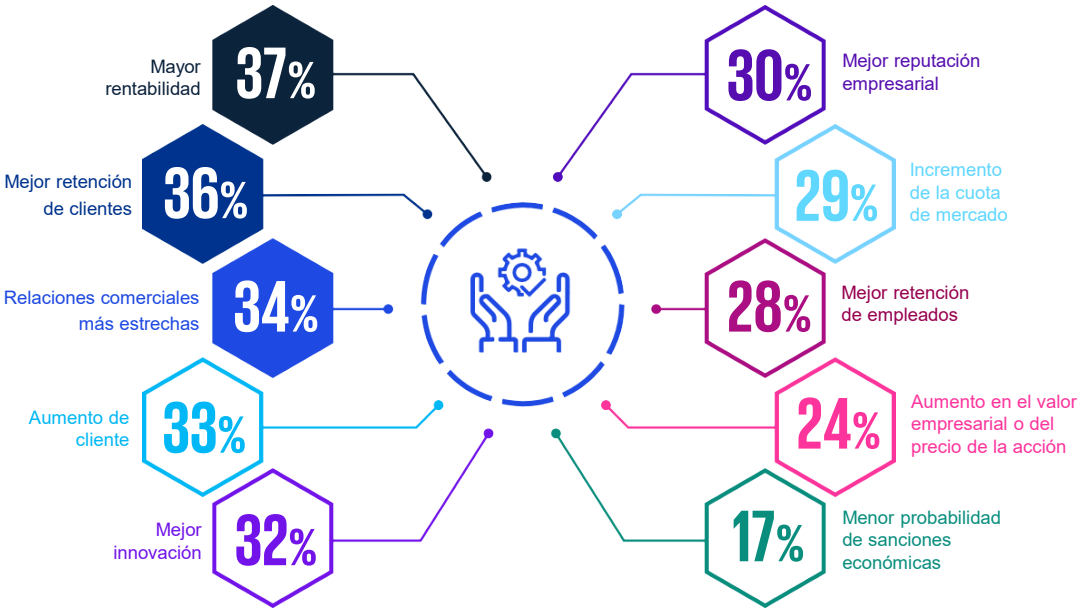
De acuerdo con la opinión de los encuestados, las tres principales ventajas del aumento de la confianza son:

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

Entre otras potenciales ventajas, se encuentra una mayor innovación, una mejor retención de empleados y una mayor cuota de mercado.

Las principales ventajas del aumento de la confianza

El gráfico muestra el porcentaje de encuestados que seleccionan cada opción como una de sus tres preferidas.



Fuente: Claves sobre ciberseguridad para 2023

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

La transformación digital avanza a pasos agigantados: en todos los sectores, las empresas están renovando su tecnología y situando datos avanzados y análisis sofisticados en el núcleo de sus operaciones. En los próximos tres años, las organizaciones prevén realizar una serie de inversiones en herramientas digitales para impulsar su crecimiento, optimizar sus interacciones con compradores y clientes, agilizar las operaciones comerciales y extraer el valor de sus datos. No obstante, cada nueva actividad con datos expone a las empresas a potenciales vulnerabilidades y riesgos para su reputación de los que debe protegerse para mantener la confianza.

Según el Informe Global Tech de KPMG, el 61% de las empresas prevé adoptar nuevas plataformas tecnológicas disruptivas en el plazo de dos años y, durante los próximos tres años, manifiesta que va a incrementar gradualmente su inversión en el Internet de las Cosas (IoT), informática en la periferia *(edge computing)* y 5G, y, en menor medida, realidad virtual (RV) y realidad aumentada (RA).

En el mismo informe de KPMG, la digitalización de canales de cliente se menciona como segundo problema más grave de ciberseguridad para las organizaciones, justo detrás de la adopción de entornos de trabajo híbridos.

En relación con las áreas de experiencia digital sobre las que invierten las empresas, el 37% se centra en el uso de datos de experiencia para personalizar interacciones digitales en tiempo real, mientras que un 36% está invirtiendo en integración multicanal para mejorar la experiencia de cliente.

Al tiempo que estas tendencias adquieren ritmo en diversos sectores, las expectativas de los clientes en cuanto a privacidad también están cambiando. Cada vez con más frecuencia, los usuarios esperan poder personalizar los controles de privacidad en sus dispositivos y canales, demandando así a las organizaciones que incorporen controles flexibles en el diseño de sus futuros productos y servicios.

Principales áreas de inversión en experiencia digital

El gráfico muestra el porcentaje de encuestados que seleccionan cada opción como una de sus tres preferidas.

Fuente: Claves sobre ciberseguridad para 2023

> «Proteger la confianza de los clientes es la prioridad de nuestra inversión en ciberseguridad y privacidad»
>
> **CISO,** Charles Schwab

La ciberseguridad está cambiando y los datos son más importantes que nunca

Ante el entorno actual, las empresas necesitan proteger las áreas más cruciales para garantizar la confianza de los grupos de interés. A este respecto, más del 80% de los encuestados reconoce la importancia de mejorar la ciberseguridad y la protección de los datos, así como la transparencia en el uso de los mismos. En particular, el 51% considera que la protección de activos de TI frente a ataques es extremadamente importante.

A medida que las organizaciones impulsan su transformación digital, la elaboración de presupuestos para la inversión en ciberseguridad y privacidad debe ser acorde y considerarse cada vez más como parte integral de las iniciativas estratégicas. “El éxito de los servicios de transformación digital dependerá probablemente de la capacidad de las organizaciones para integrar la seguridad y la privacidad en su diseño y ejecución”, señala el CISO de Shell.

Asimismo, añaden: “Nos estamos centrando en lo que denominamos ‘estándares seguros por diseño’ sobre la manera en que integramos la tecnología. Queremos que estos estándares sean transparentes para nuestros clientes, porque mantener y mejorar la confianza es nuestra obligación”.

“Proteger la confianza del cliente es lo que impulsa nuestras inversiones en ciberseguridad y privacidad”, afirma el CISO de Charles Schwab. “Ponemos nuestro máximo empeño en mantener la confianza que tenemos con nuestros clientes tanto mediante mejoras proactivas y continuas de los controles de privacidad como mediante transparencia con relación a cómo protegemos sus datos”.

Perspectiva de KPMG: la confianza se convierte en un elemento fundamental para el éxito de las tecnologías emergentes

Las tecnologías emergentes, como la tecnología de registro distribuido (DLT), la informática cuántica, las redes 5G, IA/ML y la realidad aumentada y virtual se están desarrollando rápidamente y prometen transformar la manera en que operan las empresas.

Sin embargo, el éxito en la implantación de futuras aplicaciones (economía conectada, sistemas inteligentes, NFT, metaverso, etc.) que se basan en dichas tecnologías, dependerá probablemente de la capacidad de la organización para inspirar confianza en múltiples dimensiones. Ello supone integrar controles de seguridad y privacidad con transparencia, fiabilidad e integridad.

Marc Martínez
Socio responsable del departamento de Riesgo Tecnológico y Ciberseguridad de KPMG en España

2

Tendencias de la confianza digital

Comprender los factores que inspiran confianza

Cómo afrontar los retos éticos de la IA

El creciente uso de tecnologías de IA y ML en muchas empresas está creando un conjunto nuevo (y, hasta la fecha, incomprendido) de problemas de confianza. Un estudio de KPMG señala que las empresas están decididas a incorporar la IA y el ML, y esperan ventajas que abarcan desde una mayor eficiencia y productividad hasta un aumento de la capacidad para generar predicciones sobre clientes y mercados.

El problema estriba en que estas tecnologías, si se manejan incorrectamente, suscitan riesgos de ciberseguridad y privacidad que podrían perjudicar la reputación y provocar sanciones regulatorias.

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

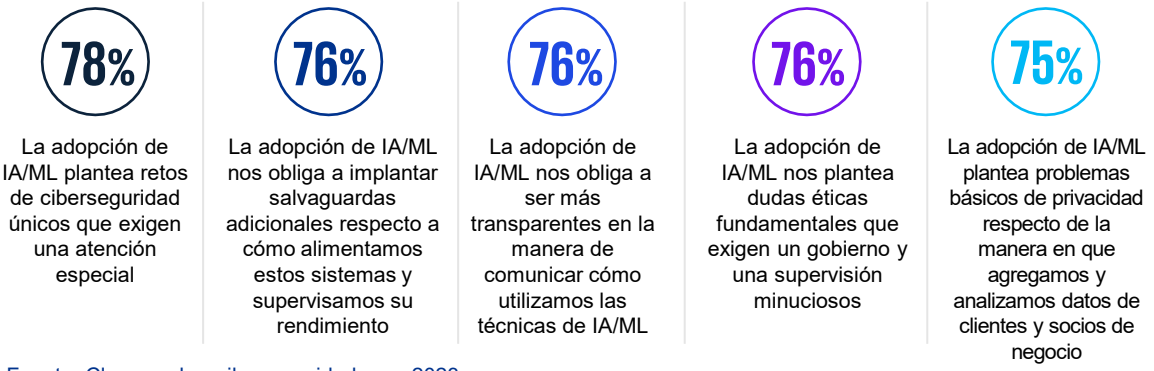
Un porcentaje similar opina que existen dudas éticas fundamentales por resolver cuando adoptan estas tecnologías, y afirma que las organizaciones van a tener que comunicar más abiertamente cómo están gestionando estas cuestiones.

Todo ello subraya el importante papel que los equipos de ciberseguridad y privacidad desempeñan a la hora de ayudar a delimitar el debate ético y gestionar riesgos.

“Estamos trabajando intensamente en Adversarial IA —como, por ejemplo, la intoxicación de datos, *machine drift* o ataques de IA— porque creemos que van a ser la siguiente oleada de ataques”, comenta la vicepresidenta corporativa de Microsoft Security Business Development.

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

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



Fuente: Claves sobre ciberseguridad para 2023

Claves de KPMG: ética de la IA

Las organizaciones son conscientes de que deben empezar a basarse en los datos o arriesgarse a caer en la irrelevancia. Muchas están actualizando el área de IA para automatizar la toma de decisiones basada en datos, pero la IA aporta nuevos riesgos a la marca y la rentabilidad. La tecnología tiene el potencial de generar desigualdad y vulnerar la privacidad, además de limitar la capacidad de tomar decisiones de manera autónoma e individual.

No puede uno limitarse a culpar al sistema de IA de los resultados no deseados. Una IA fiable y ética no es un lujo, sino una necesidad para la empresa. Cada vez más directivos empresariales son conscientes de ello, pero la confianza no se logra sin esfuerzo o retos.

Además, lo que se considera ético y fiable en un sector o región puede no considerarse como tal en otros. No existe una solución universal, y copiar los marcos existentes no resulta eficaz. Únicamente puede alcanzarse una IA fiable con un enfoque holístico, neutro en cuanto a tecnología y con un amplio respaldo a la sensibilización, el gobierno de IA y la gestión de riesgos.

Por ejemplo, las evaluaciones de impacto de la IA deben involucrar a las partes interesadas correctas para identificar riesgos. La IA necesita estar en consonancia con los valores de la organización y las partes interesadas. Las organizaciones deben evaluar cuidadosamente el cumplimiento de las leyes y los reglamentos, así como el rendimiento de la inversión en IA. Las decisiones deben ser rastreables y auditables. Y todas estas protecciones deben introducirse sin obstaculizar la innovación.

Sergi Gil

Socio del departamento de Riesgo Tecnológico y Ciberseguridad de KPMG en España

> «Estamos invirtiendo muchos esfuerzos en Adversarial AI porque creemos que es donde se focalizará la siguiente oleada de ataques»
>
> **Vicepresidenta corporativa,** Microsoft Security Business Development

La perspectiva regulatoria

Al igual que crece la preocupación de la sociedad en torno a la confianza digital, también lo hace el interés de los legisladores y los reguladores, que exigen una mayor transparencia y supervisión. Según la encuesta Claves sobre ciberseguridad para 2023:

36%

de los encuestados siente preocupación por su capacidad para cumplir las normas nuevas o ya existentes sobre ciberseguridad cuando las actividades se externalizan a proveedores de servicios digitales.

34%

reconoce inquietud sobre la revelación de información corporativa relacionada con la ciberseguridad.

31%

se preocupa por las crecientes demandas en torno a infraestructuras críticas, presente cada vez más en normas en Reino Unido, la Unión Europea y Estados Unidos.

Y, por si fuera poco, las organizaciones internacionales deben afrontar un contexto cada vez más complejo, diverso y en ocasiones contradictorio relativo a la normativa extraterritorial. “Uno de los retos de los responsables de los sistemas de seguridad es que las partes interesadas de diferentes regiones interpretan de manera diferente las mismas normas”, comenta el CIO de Bechtle, uno de los mayores proveedores de TI de Europa. “Debes tener un concepto claro de lo que puedes y no puedes hacer”.

Perspectiva de KPMG: factores normativos

El crecimiento de la ciberseguridad y la regulación de la privacidad se está acelerando en todo el mundo. Más de 137 países cuentan actualmente con algún régimen de protección de datos y, a menudo, reclaman jurisdicción extraterritorial sobre los servicios ofrecidos en el país o los datos de ciudadanos de dicho país. Algunos regímenes más maduros de privacidad están avanzando hacia una segunda generación de regulación de cara a abordar nuevos retos para la privacidad provocados por la adopción de tecnología. Por ejemplo, en estos momentos los debates sobre la regulación de la IA se están plasmando en borradores legislativos.

Asimismo, los países están introduciendo normas críticas cada vez más estrictas sobre ciberseguridad de las infraestructuras debido a la mayor preocupación por los ataques a sistemas de control industrial. Estas normas están pasando de ser autoevaluaciones a marcos de control más directivos que incluyen informes obligatorios sobre incidentes y auditorías externas.

Los reguladores también están siendo más estrictos en sus marcos de control, además de perseguir el objetivo de reforzar la independencia del CISO y su papel en el establecimiento de normas de control internas. Asimismo, están surgiendo requisitos de resiliencia más holísticos, centrados en la recuperación de la empresa en escenarios extremos, pero plausibles en sectores como, por ejemplo, el financiero.

Los requisitos corporativos de transparencia sobre riesgos de ciberseguridad son objeto de debate, junto con un número creciente de requisitos para la revelación de incidentes de ransomware. Las empresas deben invertir para automatizar la supervisión y la comunicación en materia de cumplimiento, mantener una vigilancia regulatoria y tener en cuenta las tendencias regulatorias sobre privacidad y seguridad a la hora de desarrollar nuevos servicios y productos.

Javier Aznar
Socio del departamento de Riesgo Tecnológico y Ciberseguridad de KPMG en España.

Más allá de la regulación

La confianza digital debe formar parte de la agenda de ESG y, por supuesto, la ciberseguridad y la privacidad probablemente formarán parte de ella. “Los aspectos ESG son esenciales para el negocio en su conjunto pero, naturalmente, el CISO desempeña un papel principal, en particular en lo que respecta a cuestiones sociales y de buen gobierno”, añade el CIO de Bechtle.

Sin embargo, alcanzar este objetivo supone acometer importantes esfuerzos. Menos de una quinta parte de las organizaciones describe la seguridad como parte integrante del equipo de ESG; y la mayoría manifiesta que desempeña un papel muy limitado. Asimismo, las organizaciones han de ser conscientes de las demandas sociales y las expectativas crecientes en torno a estos temas.

En el seno de las organizaciones, las personas responsables del área de ESG deben colaborar con los que se ocupan de la ciberseguridad (a menudo, el CISO) y la privacidad de los datos (a menudo, el DPO).

> **«Los aspectos ESG son esenciales para el negocio en su conjunto, pero, naturalmente, el CISO desempeña un papel principal, en particular en lo que respecta a cuestiones sociales y de buen gobierno»**
>
> **CIO,** Bechtel

Claves de KPMG: ESG y responsabilidad social

Las organizaciones que realmente asuman la agenda de ESG aumentarán la confianza de sus clientes y fortalecerán su marca. En el mundo digital actual, los consejos de administración, los inversores, los reguladores, los clientes y el sociedad en general esperan informes transparentes sobre el posicionamiento de la organización en cuestiones de ciberseguridad y privacidad.

Los grupos de interés necesitan confiar en que los consejeros y los ejecutivos aprecian las implicaciones sociales y se esfuerzan por garantizar la resiliencia y la integridad de sus servicios críticos, al tiempo que protegen la información que se les ha confiado.

Algunas consideraciones clave sobre estos grupos de interés:

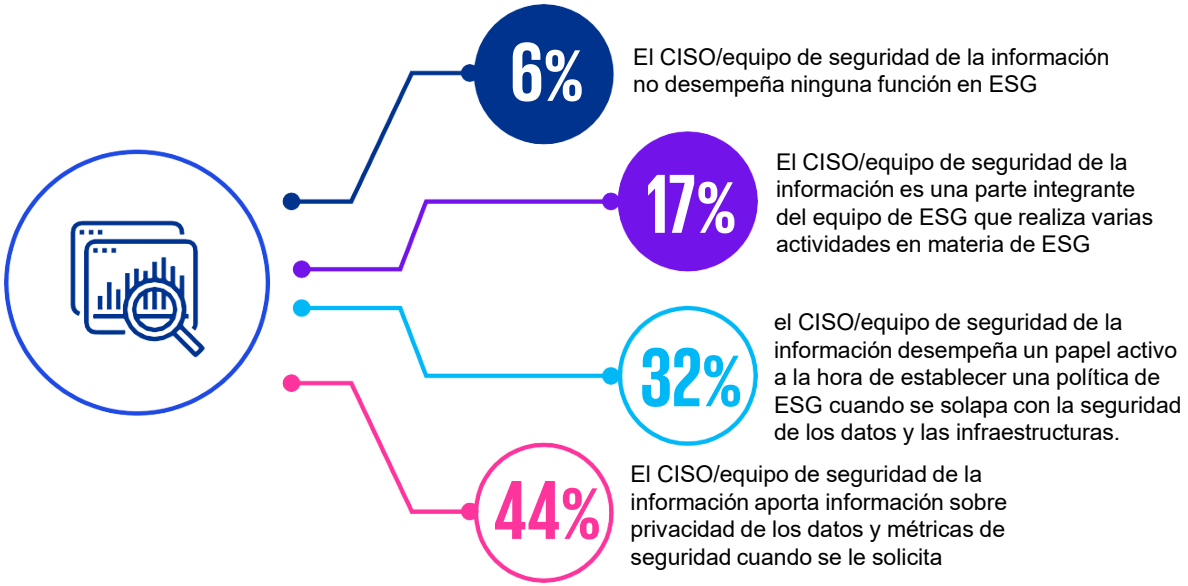
- Supervisión proactiva de activos digitales para garantizar el acceso a contenidos seguros y fiables en una época en la que impera el creciente uso de de fake news y deep fakes.
- Ayudar a proteger a los consumidores, particularmente los que se encuentran bajo el umbral de pobreza cibernética contra fraudes y robos de identidad en el espacio cibernético.
- Velar por la adopción ética de tecnologías como IA y ML, que recopilan y analizan datos de clientes.
- Mantener la fiabilidad, la integridad y la disponibilidad de los servicios digitales en los que como sociedad hemos aprendido a confiar.
- Demostrar un mayor compromiso con la creación de habilidades y capacidades en el ciberespacio, dentro del ecosistema de su proveedor y más allá de estos límites.

Javier Aznar
Socio del departamento de Riesgo Tecnológico y Ciberseguridad de KPMG en España

Sergio Gómez
Socio del departamento de Riesgo Tecnológico y Ciberseguridad de KPMG en España

La mayoría de los CISO solo intervienen pasivamente en las políticas y actividades ESG

El gráfico muestra el porcentaje de encuestados que seleccionaron una opción como una de sus elecciones preferidas.



Fuente: Claves sobre ciberseguridad para 2023

Claves de KPMG: Impulsar la confianza ampliando los límites regulatorios mínimos

Las organizaciones más adelantadas están incorporando métricas de privacidad de los datos en los marcos de información sobre aspectos ESG.

De esta manera pueden inspirar confianza al tiempo que velan por que los requisitos regulatorios, como mínimo, se cumplan. A menudo, en el contexto de fomentar una mayor confianza, las organizaciones pretenden ir más allá de los límites de las normas regulatorias mínimas de manera proactiva, de modo que las partes interesadas tengan más confianza en que su información identificativa personal se recopile, utilice o revele apropiadamente; no solo desde una perspectiva legal sino desde una perspectiva que encaje con el mensaje articulado sobre ESG de la organización.

Juanma Zarzuelo
Socio del departamento de Riesgo Tecnológico y Ciberseguridad de KPMG en España

3

Cómo construir una comunidad de confianza

El poder de la colaboración y las alianzas

Las empresas que se encuentran actualmente en proceso de digitalización no operan de manera aislada, sino que son miembros activos de alianzas y colaboraciones más amplias. Esto se suma al reto actual al que se enfrentan los equipos de ciberseguridad: inspirar confianza a través de sus ecosistemas, colaborando con socios para ayudar a garantizar la confianza mutua y en el ecosistema en su conjunto.

La unión hace la fuerza y es que, según refleja la encuesta **'Claves sobre ciberseguridad para 2023',** casi la mitad de los encuestados (44%) declara que la colaboración en ciberseguridad en todo el ecosistema les ayudará, por ejemplo, a prever ataques.

Aunque la colaboración resulta un punto fundamental, no siempre es directa. Más de un tercio de los encuestados (38%) afirma que las preocupaciones sobre privacidad dificultan las alianzas externas en materia de ciberseguridad, y el 36% está preocupado por revelar demasiado acerca de sus medidas de seguridad. Otros problemas incluyen restricciones regulatorias, falta de apoyo del equipo directivo e insuficiencia de recursos.

Fuente: Claves sobre ciberseguridad para 2023

> **« Tener un estándar y afirmar que los parámetros de tu cortafuegos cumplen con dicho estándar es una perspectiva de información completamente diferente que, por lo general, no supone acometer detalles complejos y, a su vez, ayuda a fomentar la confianza. »**
>
> **Responsable de Estrategia,** International Association of Privacy Professionals (IAPP)

La colaboración en materia de ciberseguridad en el conjunto del ecosistema puede ayudar a las organizaciones a prever y recuperarse de los ataques

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

Existen soluciones prácticas, según el responsable de Estrategia de la International Association of Privacy Professionals (IAPP). “Si comunicara los parámetros de mi cortafuegos, existiría el riesgo de que se pudiera apreciar una vulnerabilidad o brecha”, asegura. “Pero tener un estándar y afirmar que los parámetros de tu cortafuegos lo cumplen, es una perspectiva de información completamente diferente que, por lo general, no proporciona detalles complejos y ayuda a fomentar la confianza”.

La falta de madurez de los estándares y las buenas prácticas a la hora de compartir información puede ayudar a explicar por qué menos de la mitad de las empresas están colaborando o intercambiando información con socios clave. Incluso aunque el 79% de los encuestados afirma que una participación constructiva de los proveedores es esencial para que la ciberseguridad sea efectiva, tan solo el 42% manifiesta que están trabajando conjuntamente para lograrlo.

Sin embargo, cabe tener en cuenta que esta actitud puede causar un perjuicio grave. Más de la mitad de las empresas admiten que desconocen si sus defensas son lo suficientemente fuertes como para impedir que los atacantes se aprovechen de las vulnerabilidades en la cadena de compras y suministro.

Este enfoque más limitado con respecto a la colaboración no puede proseguir; no logra ofrecer suficiente protección a organizaciones individuales o sus ecosistemas, socavando la confianza en ambas. A más de la mitad de nuestros encuestados (53%) le preocupa que sus organizaciones no sean lo suficientemente proactivas en sus colaboraciones sobre ciberseguridad; y puede que tengan mucha razón.

Se necesitan más alianzas de ciberseguridad en todo el ecosistema
El gráfico muestra el porcentaje de encuestados que seleccionaron todas las opciones posibles

Fuente: Claves sobre ciberseguridad para 2023

Perspectiva de KPMG: el valor de la unidad

La construcción efectiva de una comunidad es vital para abordar los retos de ciberseguridad y, para ello, las organizaciones deben trabajar codo con codo. Sin embargo, existen cuestiones significativas en relación con la gestión de riesgos, la reputación, la ley y la estrategia que pueden obstaculizar la consecución de esta serie de objetivos.

Ninguna organización puede abordar estos retos por sí misma, por lo que es importante combinar recursos y coordinarse de manera efectiva. Trabajando conjuntamente, las organizaciones tanto públicas como privadas pueden garantizar una mejor eficiencia, perspectivas y recursos.

Para asegurar dicha confianza y construir una comunidad, cada una de las partes debe reconocer lo que es posible, dónde están los obstáculos y cómo superarlos. Por ejemplo, algunas organizaciones están utilizando protocolos existentes, como el marco de ciberseguridad del NIST, a fin de crear un lenguaje y una terminología común cuando interactúan con otras organizaciones. Otras se están centrando en cómo velar para que la información exclusiva no traspase las fronteras de la organización. Los acuerdos de cooperación basados en principios operativos comunes pueden ayudar a las organizaciones a establecer relaciones y sustentar la infraestructura digital, al tiempo que mantienen la privacidad y refuerzan la confianza mutua entre los socios.

Existe también la necesidad de reconocer que el paradigma tradicional de seguridad es menos relevante en este ámbito interconectado. En lugar de ello es más lógico dirigir la atención hacia una mentalidad de resiliencia. Más que intentar derrotar a los agentes malintencionados únicamente aislando y controlando los sistemas, es necesario un enfoque más coordinado y de cooperación.

Marc Martínez
Socio responsable del departamento
de Riesgo Tecnológico y
Ciberseguridad de KPMG en España

4

La evolución del CISO

La contribución del CISO para inspirar confianza

El CISO entra en escena

En ocasiones se ha considerado que los CISO pueden suponer un freno a la innovación y a las iniciativas de crecimiento, sin embargo, los CISO se encuentran actualmente en disposición de desempeñar un papel crucial como facilitadores para cumplir tales objetivos. Al operar como uno de los "guardianes de la confianza" en última instancia de la organización, pueden ser una fuerza que impulse su éxito.

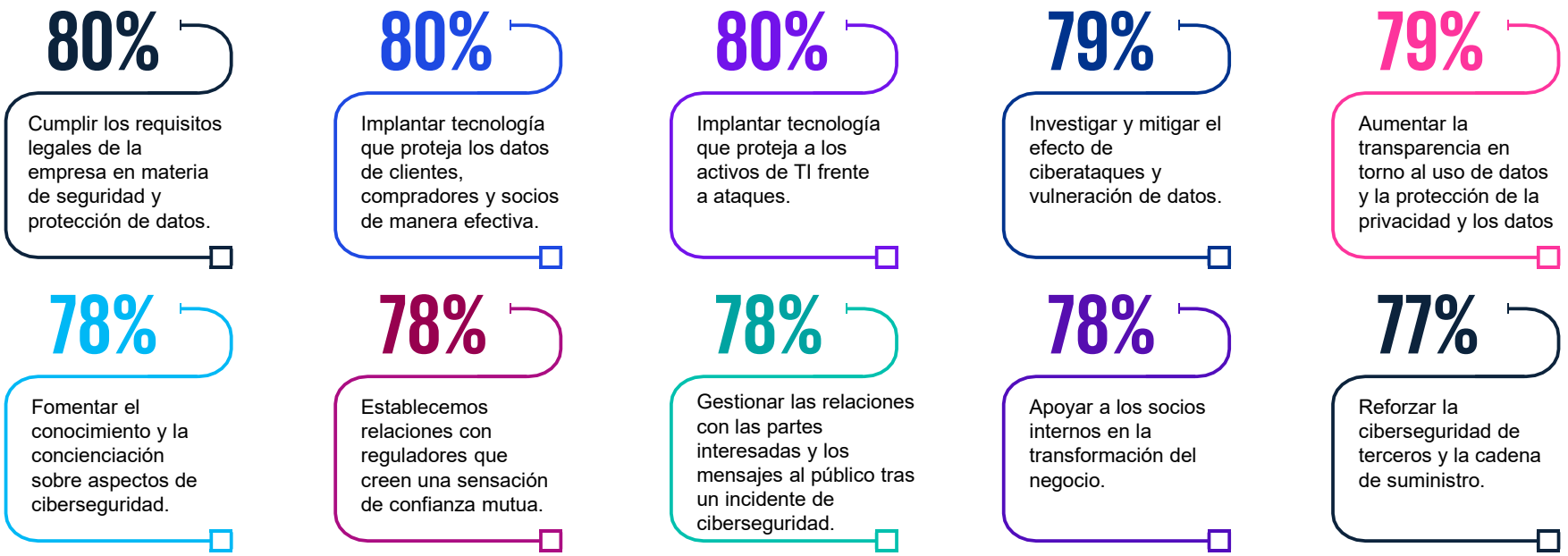
"Los CISO pueden potenciar y mejorar la confianza, pero a menudo lo que hacen está condicionado en general por las prioridades de su organización", comenta el responsable de Estrategia de la IAPP. "Es necesario que empiecen a explorar ese espacio para ayudar a la organización a avanzar y cambiar la dinámica".

Los propios CISO son conscientes de lo que está en juego. Más de tres cuartas partes de los encuestados (77%) señalan que el aumento de la confianza es un objetivo clave de sus programas de ciberriesgo.

Y las organizaciones muestran elevados niveles de confianza en sus capacidades de ciberseguridad: El 74% afirma que ha apreciado mejoras en ciberseguridad durante los últimos 12 meses; y más de una cuarta parte de ellos las considera significativas. Esta confianza se suma a la firme creencia en la capacidad del CISO para llevar a cabo con éxito tareas cruciales.

¿Pero se sienten capaces los CISO de cumplir estas expectativas?

Las organizaciones muestran elevados niveles de confianza en el CISO
El gráfico muestra el porcentaje de encuestados que califican cada actividad como 'efectiva'.



Fuente: Claves sobre ciberseguridad para 2023

Es interesante, por tanto, que el público y los CISO se esfuercen por adoptar un compromiso para alcanzar sus objetivos. A menudo pueden presentarse conversaciones difíciles, afirma la vicepresidenta corporativa de Microsoft. "¿Qué datos vamos a compartir? ¿Cómo los vamos a almacenar? ¿Cómo vamos a utilizarlos desde un planteamiento de IA-ML? ¿Cómo vamos a protegerlos?"

El CISO debe intervenir en cada una de estas conversaciones, "y no son fáciles de mantener", añade.

Casi dos tercios de los encuestados (65%) declara que las organizaciones consideran que la seguridad de la información es una actividad que reduce riesgos, más que impulsar el negocio. Además, el 57% comenta que los máximos responsables no entienden las ventajas competitivas de una mejora de la confianza gracias a una mejor seguridad de la información.

¿Sugiere esta desconexión que el CISO necesita esforzarse más para ofrecer una visión realista de la ciberseguridad?

Establecer una relación con responsables sénior

Sería poco realista e injusto que los CISO fueran los únicos en impulsar la agenda de ciberseguridad y privacidad de los datos. Sus interacciones con homólogos, como el responsable de datos y el responsable de privacidad, podrían ser cruciales. Si colaboran de manera efectiva, pueden conjuntamente empezar a introducir cambios prácticos para mejorar la confianza.

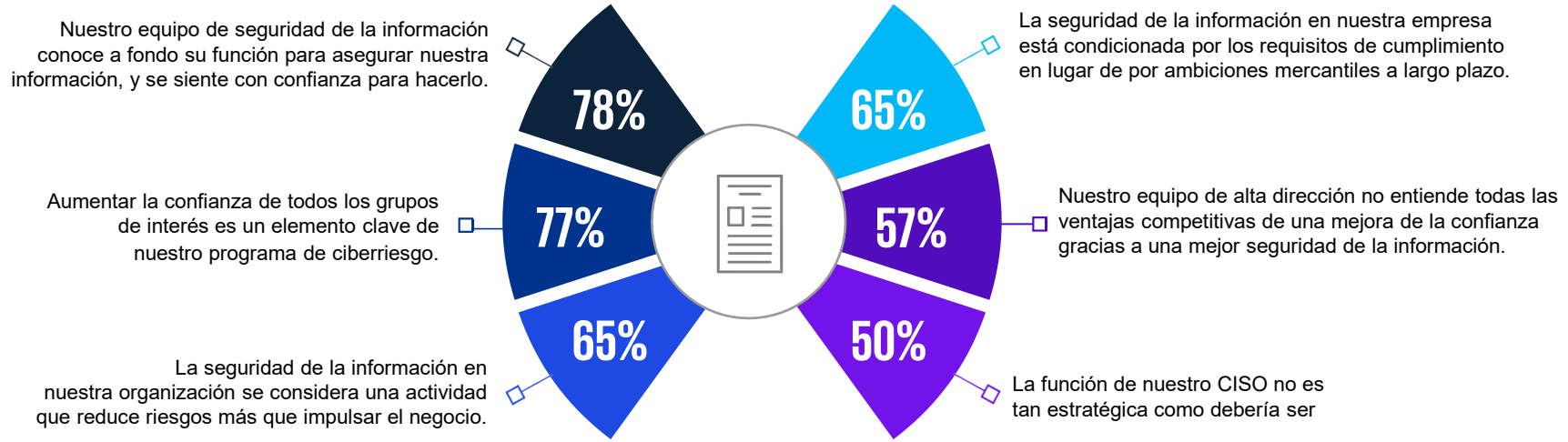
La buena noticia es que los líderes más influyentes de las organizaciones creen que los CISO y la función de ciberseguridad en su conjunto deben participar en la transformación desde las primeras etapas.

El 44% por ciento de los encuestados del equipo de alta dirección considera ahora al CISO como un ejecutivo clave, y el perfil de su función ha aumentado rápidamente en los últimos cinco años debido a la transformación digital, el aumento de las ciberamenazas y el incremento de las expectativas de los reguladores.

Una manera de que los CISO cambien esa perspectiva podría consistir en desviar el foco de atención de las cuestiones más técnicas, dado que más de la mitad de los altos directivos encuestados se quejan de que los consejeros no las entienden. Por tanto, queda pendiente que los CISO asuman este papel estratégico. Las empresas están reclamando una implicación a nivel sénior, un foco de atención en las necesidades del negocio y un intento por garantizar que la ciberseguridad se considere la piedra angular en cada aspecto de la estrategia, la planificación, la inversión y la ejecución del negocio.

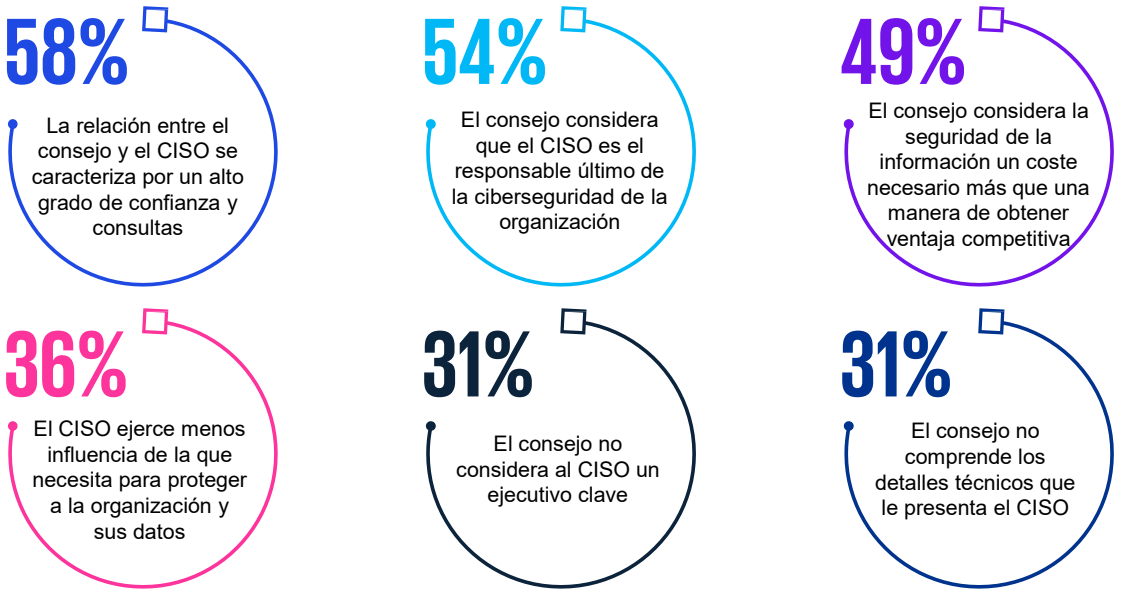
Los CISO están preparados para dar un paso al frente, pero ¿se les permite hacerlo?

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



Fuente: Claves sobre ciberseguridad para 2023

Los consejos tienen opiniones diversas sobre la influencia del CISO
El gráfico muestra el porcentaje de encuestados que indicaron que las afirmaciones son ciertas



Fuente: Claves sobre ciberseguridad para 2023

El reto de cuantificar el riesgo

Muchas organizaciones están realizando grandes avances en la modelización y evaluación de riesgos en un área que se ha resistido notablemente al análisis. Tres cuartas partes de las organizaciones afirman que han implantado la modelización de riesgos para cuantificar y comunicar visualmente el ciberriesgo al consejo, pero solo el 58% describe su enfoque a la hora de cuantificar los ciberriesgos como 'sólido' y manifiesta que sus escenarios de ciberriesgo están adaptados a las necesidades del negocio.

Desde una perspectiva más positiva, más de dos tercios de los encuestados (69%) creen que tienen un enfoque sólido en la valoración de la confianza digital, en lugar de considerarla un concepto abstracto. Y un 65% dice que la modelización de riesgos impulsa la inversión en mejoras en la ciberseguridad, con vínculos claros entre proyectos y reducción de riesgos. Así pues, los CISO necesitan hacer más de lo que hacen hoy en día, así como reconocer la naturaleza evolutiva de su puesto, ampliando su alcance hasta áreas donde existe potencial para impulsar la confianza en su organización más allá de sus límites.

Perspectiva de KPMG: a favor de la cuantificación del ciberriesgo

Un trabajo minucioso de modelización y cuantificación puede ayudar a los responsables de la toma de decisiones a conocer el verdadero nivel de exposición al ciberriesgo de la organización. Ello puede ayudar a la dirección a comprender qué controles son los que más contribuyen a reducir determinadas exposiciones al ciberriesgo y, por tanto, que ayudan a dirigir sus recursos hacia las áreas más ventajosas.

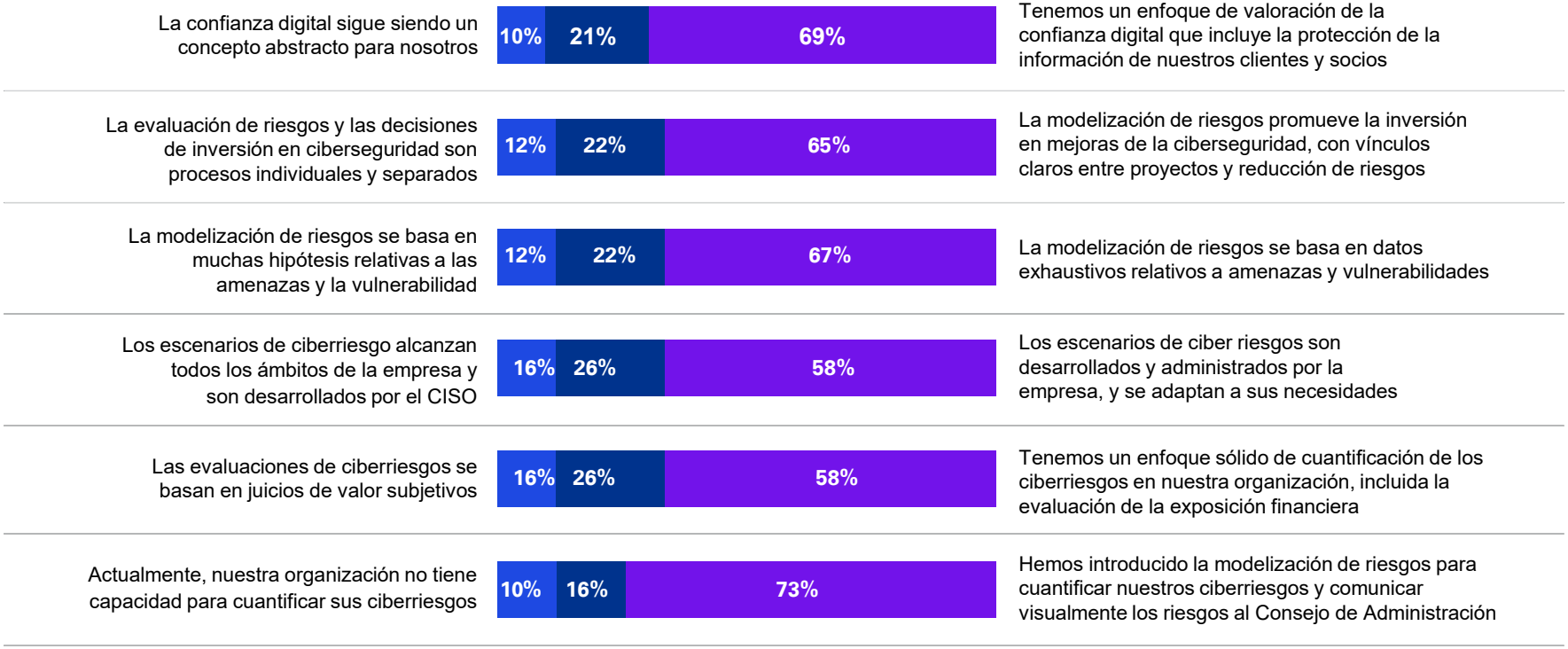
Para conseguirlo, las organizaciones deben atenerse a cinco principios:

1. Velar por la alineación del modelo de riesgo con sus marcos de riesgo.
2. Ser coherentes en la definición del ciberriesgo como sucesos de pérdida potencial para el negocio (los escenarios constituyen un método excelente para ello).
3. Adoptar un enfoque basado en las amenazas a la modelización, utilizando modelización de ruta de ataque para deconstruir la manera en que pueden materializarse dichos riesgos.
4. Utilizar datos reales en los cálculos; las estimaciones de probabilidad e impacto deben estar justificadas con datos empíricos internos y externos (disponen de más de ellos de lo que piensan).
5. Conocer a fondo las ventajas y las limitaciones del modelo y ser transparentes a este respecto.

Guillermo González
Director del departamento de Riesgo Tecnológico y Ciberseguridad de KPMG en España

Muchas organizaciones están teniendo dificultades para modelar y valorar el ciberriesgo

El gráfico muestra el porcentaje de encuestados que indicaron que las afirmaciones reflejaban más exactamente la situación en sus organizaciones.



Fuente: Claves sobre ciberseguridad para 2023

5

Misión posible

Cómo el CISO contribuye a la confianza en las organizaciones

Los ejecutivos entienden la importancia de impulsar la confianza en sus organizaciones y ecosistemas, y centran su mirada en el CISO para que sea uno de los líderes en esta tarea. La ciberseguridad y la privacidad son elementos clave para impulsar la confianza de clientes, reguladores y el público a través del imperativo ESG.

En consecuencia, los propios CISO son conscientes de su responsabilidad para la consecución de esa meta, al igual que sus homólogos en otras partes del negocio. Sin embargo, este estudio señala que muchos de ellos tienen dificultades para alcanzar esta responsabilidad. Quizás por la falta de una visión clara de lo que realmente significa la confianza digital y la manera de lograrla.

No es una tarea que un CISO pueda hacer por sí solo. Necesita un apoyo más firme de la alta dirección, más colaboración de otras funciones y cooperación productiva con socios externos y terceros.

Aun así, el CISO es un actor esencial. Una definición explícita de la confianza puede ser un buen punto de partida, además del uso de la ciberseguridad y la privacidad como un medio para reforzar la confianza en la organización, con todas las ventajas competitivas que conllevan.

¿Cómo deberían abordarlo?

Cinco pasos cruciales para inspirar confianza mediante la ciberseguridad y la privacidad

01

Considerar la ciberseguridad y la privacidad como una piedra angular

Implantar la ciberseguridad y la privacidad en los procesos de negocio, el buen gobierno y la cultura de la organización, convirtiéndolas en parte integrante del negocio en lugar de una sobrecarga derivada del cumplimiento normativo.

02

Establecer alianzas internas para impulsar la confianza

Trabajar con homólogos, como el responsable de datos y el responsable de privacidad para ayudar a establecer, integrar y mantener la confianza digital.

03

Reinventar la función del CISO

Asumir una agenda más amplia y ser consciente de la capacidad para realizar aportaciones de mayor alcance en áreas que abarcan desde los aspectos ESG hasta la ética de la IA.

04

Obtener el apoyo de la dirección para invertir en confianza

Los CISO que cuentan con el apoyo de la alta dirección y el consejo probablemente tendrán más fácil ayudar a impulsar esta confianza. Para ello, es fundamental transformar el papel del CISO desde una función técnica hacia un intermediario estratégico en el ámbito de la organización.

05

Llegar a todos los rincones del ecosistema

Identificar socios clave dentro del ecosistema de la organización y colaborar estrechamente con ellos ayuda a mejorar la confianza y la resiliencia.

Metodología y reconocimientos

Acerca de 'Claves sobre ciberseguridad para 2023'

El estudio 'Claves sobre ciberseguridad para 2023', realizado por KPMG International entre mayo y junio de 2022, encuestó a 1.881 ejecutivos y entrevistó a cinco líderes empresariales del panorama internacional para explorar el papel que desempeñan la ciberseguridad y la privacidad en la creación y el mantenimiento de la confianza.

Una proporción significativa de la población participante estaba compuesta de responsables de nivel sénior: El 42% son miembros del consejo o del equipo de alta dirección. Entre los encuestados, había responsables de 31 mercados (24% de ASPAC, 50% de EMA, 16% de Norteamérica y 10% de Sudamérica) y seis sectores clave (energía y recursos naturales, servicios financieros, ciencias de la vida y farmacéutico, medios de comunicación, entretenimiento y tecnología, sector público y telecomunicaciones).

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

KPMG agradece su aportación a las siguientes personas, compañías y entidades:

- Charles Schwab
- Bechtle
- Shell
- Microsoft
- International Association of Privacy Professionals (IAPP)

Acerca de KPMG

Las firmas de KPMG pueden ayudarle a crear un entorno digital resiliente y fiable, incluso en un contexto de evolución de las amenazas. Los profesionales de KPMG pueden ofrecer una visión multidisciplinar del riesgo, de modo que ustedes puedan implantar la seguridad en todos los ámbitos de su organización y puedan anticiparse al día de mañana, avanzar más rápido y conseguir margen con tecnología segura y fiable.

No importa en qué punto se encuentra de su itinerario de ciberseguridad, las firmas de KPMG tienen conocimientos especializados en todo su recorrido; desde el Consejo de Administración hasta el centro de datos. Además de evaluar su ciberseguridad y alinearla con las prioridades de su empresa, podemos ayudarle a desarrollar soluciones avanzadas, asistirle en su implantación, asesorarle en la supervisión de riesgos constantes y ayudarle a responder de manera efectiva ante incidentes cibernéticos.

Los profesionales de KPMG recurren a tecnologías en constante evolución que pueden conectar e impulsar las empresas de cara al futuro, inspirando confianza y creando y protegiendo el valor, al tiempo que se reduce la brecha entre el pasado y el futuro.

Creemos juntos un mundo digital fiable.

Contactos

Marc Martínez
Socio responsable del departamento de Riesgo Tecnológico y Ciberseguridad de KPMG en España
E: marcmartinez@kpmg.es

Javier Aznar
Socio del departamento de Riesgo Tecnológico y Ciberseguridad de KPMG en España
E: jaznar@kpmg.es

Juanma Zarzuelo
Socio del departamento de Riesgo Tecnológico y Ciberseguridad de KPMG en España
E: jzarzuelo@kpmg.es

Sergi Gil
Socio del departamento de Riesgo Tecnológico y Ciberseguridad de KPMG en España
E: sergigil@kpmg.es

Sergio Gómez
Socio del departamento de Riesgo Tecnológico y Ciberseguridad de KPMG en España
E: sergiogomezrodriguez@kpmg.es

Guillermo González
Director del departamento de Riesgo Tecnológico y Ciberseguridad de KPMG en España
E: ggonzalezgonzalez@kpmg.es

Es posible que la totalidad o algunos de los servicios descritos aquí no puedan prestarse cuando se trate de clientes de auditoría de KPMG y de sus entidades afiliadas o vinculadas.

home.kpmg/socialmedia

Diseñado por Evalueserve.

Nombre original de la publicación: KPMG cyber trust insights 2023 | Número de publicación: 138298-G | Fecha de publicación: Octubre de 2022