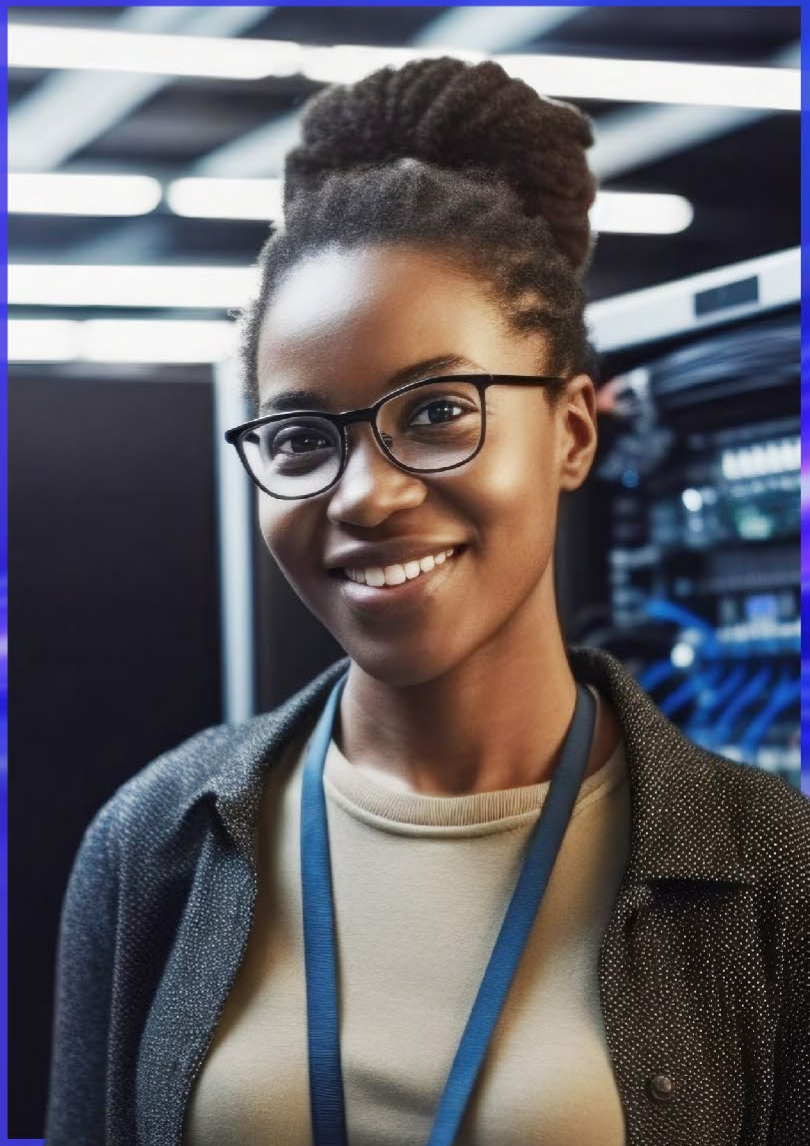
Consideraciones de ciberseguridad 2024

Las innovaciones tecnológicas requieren pragmatismo estratégico.



KPMG International

kpmg.com/cyberconsiderations

Prefacio

A medida que avanza el año 2024, el liderazgo de las organizaciones, desde el CEO y los niveles subsiguientes, se traen mucho entre manos. Deben hacer frente a diversos retos para alcanzar un crecimiento sostenido, navegar las aguas del impacto y los riesgos de la tecnología emergente, y atraer y retener el talento, por nombrar sólo algunos. Por su parte, la directiva de seguridad de la información (CISO, por sus siglas en inglés) es considerada cada vez más como co-responsable proactiva de estos imperativos empresariales en curso, y no simplemente como agentes de rescate de la organización en momentos de crisis.

En nuestro informe anual Consideraciones de ciberseguridad, una muestra representativa de especialistas globales en ciberseguridad de KPMG explora ocho consideraciones a través de las cuales se anima a los CISO y a sus equipos a dar prioridad en el próximo año al respaldo de los objetivos de crecimiento del negocio de la organización, mitigando el impacto de incidentes cibernéticos específicos y reduciendo la exposición general al riesgo cibernético.

Las organizaciones alrededor del mundo se enfrentan a muchos desafíos de ciberseguridad que requieren la implementación de controles para construir e integrar la resiliencia, cumplir con los mandatos reglamentarios y reducir el riesgo general. Sin embargo, la rápida aparición de la inteligencia artificial (IA) como herramienta estratégica tanto para fines legítimos como nefastos está ascendiendo rápidamente en la lista. La democratización de la IA -estas soluciones y modelos tecnológicos avanzados son ahora accesibles en gran medida a cualquier persona con una tarjeta de crédito a través de la nube- ha revelado a la vez nuevas vías de creación de valor y ha expuesto importantes riesgos potenciales.

La IA está demostrando ser un verdadero cambio organizativo, incluso para los equipos de seguridad.

Este panorama de amenazas en evolución requiere que las organizaciones y sus CISO vean la seguridad a través de una lente nueva y más pragmática. Ahora más que nunca, deben equilibrar la seguridad y la privacidad de los datos con los objetivos más amplios de la compañía.

Desde el punto de vista de la ciberseguridad, las repercusiones de los avances sociales, económ|icos, políticos y normativos se dejan sentir hoy en día de forma más sistemática en todo el mundo. La sencilla razón es que el mundo está más conectado. El efecto más crucial del ecosistema empresarial conectado sigue produciéndose en las cadenas de suministro globales: a efectos prácticos, ya no hay prácticamente regiones del mundo que se consideren aisladas.

Sin embargo, sigue habiendo matices locales. Por ejemplo, hay requisitos normativos a los que deben adherirse las empresas que siguen siendo exclusivamente regionales, como el hecho de que determinados mercados sean más sensibles a la protección de los datos personales y las nuevas normas en torno a la IA responsable, las infraestructuras críticas y las cadenas de suministro.

Hay un enfoque global dentro del universo de la ciberseguridad sobre el cumplimiento en general, con un ojo refinado hacia la carga general de la regulación, así como la diversidad de los diversos requisitos de información. Como resultado, las empresas se enfocan más en la integración de la privacidad y la seguridad en la forma en que cumplen con una amplia gama de requisitos y regímenes normativos transfronterizos.

Esto es de especial interés cuando se trata de construir y dirigir sistemas responsables de IA, garantizar la privacidad de los clientes y promulgar directrices en torno a infraestructuras críticas, cadenas de suministro, productos inteligentes y resiliencia.

Al mismo tiempo, es posible que los presupuestos de ciberseguridad tengan que justificarse de forma más objetiva a medida que las organizaciones se enfrentan a la incertidumbre económica. Muchos CISO están presenciando presupuestos planos, no necesariamente reducidos, ya que parte de ese gasto se desvía a la innovación organizativa, en particular soluciones de IA y automatización. Esta notable evolución exige que los equipos de seguridad se dediquen a la racionalización tecnológica y la optimización presupuestaria, es decir, a hacer más con menos.

Si bien los vientos económicos en contra impulsan las presiones presupuestarias, existe una opinión cada vez más extendida de que la ciberseguridad ha madurado hasta el punto de que las organizaciones pueden recortar la inversión. Además, la funcionalidad de la seguridad está ahora integrada en otros presupuestos de TI y transformación, en lugar de ser una dotación presupuestaria central. Además, el cambio a un enfoque de seguridad como servicio basado en la nube integra los costos de seguridad en los gastos operativos más amplios de las empresas de una forma nunca antes vista.

En este entorno, invito a los CISO a perfeccionar su proceso de cuantificación del riesgo cibernético (CRQ), que ayuda a expresar el impacto del riesgo de ciberseguridad en términos financieros utilizando modelos matemáticos para ilustrar el riesgo a través de variables medibles.[1] Si se contempla el riesgo a través de una lente CRQ, se podría demostrar eficazmente el retorno de la inversión y las prioridades de inversión a la gerencia y Junta Directiva, garantizando que la organización entiende la amenaza tanto desde el punto de vista tecnológico como financiero.

Fundamentalmente, este informe explora desde varios ángulos lo que quizás sea la aspiración central de los ejecutivos de toda la empresa: mantener la resiliencia de sus organizaciones. En resumidas cuentas, si se produce una filtración de datos o una brecha en la red, ¿con qué rapidez puede la organización reanudar sus operaciones normales y cómo puede minimizarse el impacto en los clientes?

Esto es emblemático de la agenda de resiliencia que puede verse en muchas de las normativas propuestas más recientemente, en particular las que se centran en sectores de infraestructuras críticas. En muchos casos, ahora se hace hincapié en la respuesta y la recuperación, así como en la mitigación de los daños a los clientes. Se trata de un prisma diferente a través del cual ver la seguridad en relación con la perspectiva tradicional.

La ciberseguridad debe verse como un esfuerzo continuo en constante evolución. Cuanto más acepten las organizaciones que los incidentes cibernéticos son inevitables pero manejables, más posibilidades tendrán de lograr ese equilibrio entre preparación y resiliencia.

Akhilesh Tuteja
Líder Global de Ciberseguridad
KPMG International

[1] Forrester, ***The Cyber Risk Quantification Landscape, Q4 2022***, 29 de noviembre de 2022.

Ocho consideraciones claves de ciberseguridad para 2024

Haga clic en cada consideración para saber más

01

Cumplir con las expectativas del cliente, mejorar el nivel de confianza

A medida que aumentan las amenazas cibernéticas y de privacidad de datos, los CISO deberán intentar trabajar conjuntamente con los grupos de interés en toda la organización para mantener la confianza y así garantizar operaciones resilientes en caso de incidentes de dicha índole.

02

Incorporar la ciberseguridad y la privacidad de una vez y para siempre

La acción de incorporar la seguridad en toda la organización debería considerarse como un ejercicio para impulsar la excelencia operacional.

03

Navegar por fronteras globales difusas

Una consideración central que las organizaciones deben tomar en cuenta es la forma más efectiva de navegar el panorama global de negocios cada vez más complejo para garantizar la resiliencia y la continuidad de negocios

04

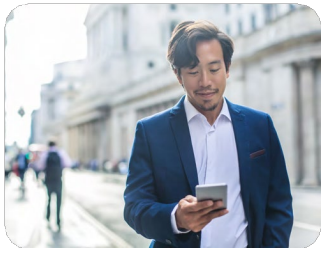
Modernizar la seguridad de la cadena de suministros

A pesar de los desafíos y prioridades de competencia, garantizar que el entorno del proveedor y el socio es seguro no debería considerarse una piedra de tranca, sino más bien un impulsor de negocios.

05

Desbloquear el potencial de la IA — cuidadosamente

Los líderes de seguridad y privacidad deben respaldar los objetivos de negocios que dependen de la IA y deberán determinar la forma de apalancar este tipo de tecnología revolucionaria efectiva y responsablemente.



06

Optimizar la seguridad a través de la automatización

A medida que los modelos operativos se digitalizan, los equipos de seguridad deberían automatizarse y optimizar sus procesos para mantenerse al día.

07

Hacer de la identidad algo individual y no institucional

Impulsados por modelos de negocios en expansión, resulta vital que las organizaciones actualmente consideren la identidad no como un hecho aislado sino desde una perspectiva más amplia.

08

Alinear la ciberseguridad con la resiliencia organizacional

Las organizaciones deberían encontrar la manera de crear una cultura de alto rango de Seguridad resiliente en toda la empresa e intentar garantizar que todos los grupos de interés estén en sincronía.

Consideración 1

Cumplir con las expectativas del cliente, mejorar el nivel de confianza

La fuerza laboral, clientes y proveedores — cada uno de los grupos de interés corporativos — esperan que su negocio busque el crecimiento y las ganancias. Cada vez más, sin embargo, se espera que las compañías sean socialmente responsables al mismo tiempo. Las organizaciones deberían fortalecer la conexión entre la seguridad y la privacidad, y los factores ambientales, sociales y de gobernanza (ESG). Exponencialmente, este vínculo tiene reconocimiento en todo el ámbito de negocios, particularmente por los servicios de calificación de ESG, a medida que buscan una mayor transparencia al momento de medir y comparar organizaciones.

> La optimización de los niveles de confianza debería tener prioridad en la planificación cibernética en lo que respecta a la forma en la que se utilizan los archivos de audio y video en la creación de *deepfakes*, cuyo impacto podría ser grave para la privacidad e incluso para la democracia.

Mika Laaksonen
Socio
Líder Global ESG en Ciberseguridad
KPMG en Finlandia

La importancia de ESG y cómo la seguridad y la privacidad encaja en el panorama general

Según la encuesta de KPMG CEO Outlook de 2023, el 69% de los CEO ha integrado los aspectos ESG a su negocio como medio para crear valor, y el 50% prevé obtener beneficios significativos de estos esfuerzos en los próximos tres a cinco años.

Mientras que los aspectos medioambientales de la agenda ESG han acaparado la mayor atención, los elementos de gobernanza, como la ciberseguridad y la privacidad, están menos desarrollados. Con el aumento de las amenazas cibernéticas y la preocupación por la privacidad de datos, los CISO deben trabajar en estrecha colaboración con sus homólogos de ESG para garantizar que, en caso de incidente, las operaciones sean resistentes y los planes de continuidad estén listos para su activación.

Al integrar las consideraciones cibernéticas y de privacidad en los programas de responsabilidad social y proteger los datos de los clientes, las organizaciones pueden aumentar las posibilidades de mantener su reputación y la confianza entre los clientes, incluso en caso de una brecha importante.

Los consumidores que comparten información personal con proveedores de servicios públicos y privados esperan que sus datos estén protegidos y que no se utilicen para fines distintos de aquellos para los que los proporcionaron.

Al mismo tiempo, existe la expectativa de que, en la consecución de sus objetivos empresariales, las organizaciones actúen de manera socialmente responsable para reducir su huella de carbono, apoyar a sus comunidades locales, mejorar las políticas laborales y garantizar la diversidad y la igualdad en el lugar de trabajo, por nombrar sólo algunos puntos.

Abordar la ciberseguridad y la privacidad específicamente y las ESG en general se han convertido en las principales prioridades de las empresas y, por extensión, de los CISO. Existen diferentes normativas para regiones e industrias específicas, y esas directrices deben generar confianza. Esto es importante desde el punto de vista del cumplimiento, pero también es digno de mención porque los clientes B2B y los consumidores B2C tienen expectativas distintas que se ven directamente afectadas por las distintas normas.

Los consumidores individuales pueden adquirir productos o servicios alternativos si no están satisfechos con las acciones del proveedor en relación con sus datos personales, privacidad y respuesta a las violaciones. De hecho, el 82% prefiere que los valores de una marca estén en consonancia con los suyos propios, y el 75% afirma que abandonaría una marca por un conflicto de valores.[2] Dadas las opciones, la mayoría de los consumidores prefiere empresas que den prioridad a la seguridad, la privacidad y la sostenibilidad mediante la adhesión a las normas ESG.

Esto es especialmente cierto en el lado B2B, donde los clientes corporativos valoran salvaguardar sus datos confidenciales y su propiedad intelectual. Cada vez más sectores tienen requisitos reglamentarios en materia de ciberseguridad y privacidad de los datos, y las organizaciones que los cumplen son las preferidas de las partes interesadas.[3] Para muchas organizaciones que operan en sectores B2B, esto es más que un "detalle", ya que las obligaciones reglamentarias fluyen directamente de las empresas de los sectores regulados a sus proveedores, que podrían verse empañados por la asociación si la marca experimenta un evento cibernético significativo.

De hecho, aproximadamente dos tercios de los consumidores pagarían más por productos sostenibles, aunque dos tercios de los ejecutivos del sector minorista se muestran escépticos de que realmente vayan a pagar más.[4] Sin embargo, aunque los consumidores puedan estar de acuerdo con pagar más por la seguridad, la privacidad y la responsabilidad social, estos factores son, por el momento, "apuestas iniciales", el precio de hacer negocios, aunque es probable que afecten a los resultados finales más pronto que tarde.

En los casos relacionados con el capital de inversión o el capital de riesgo, cabe destacar el prisma ético a través del cual estas empresas consideran sus inversiones. Muchas buscan ahora garantías del nivel adecuado de gestión de la ciberseguridad y la privacidad. En última instancia, les preocupa el daño que los incidentes cibernéticos pueden causar a las organizaciones en las que invierten fondos.

> **La cibernética desempeña un papel cada vez más importante en la IA y la ética de los datos. Determinar que los datos utilizados para entrenar algoritmos de IA son precisos, no han sido corrompidos y están libres de sesgos es una tarea titánica y, quizás en última instancia, imposible, pero bien merece la pena el esfuerzo.**

Caroline Rivett
Socia
Líder Global de Ciencias Biológicas en Seguridad Cibernética
KPMG en el Reino Unido

[2] Google Cloud, "New research shows consumers more interested in brands' values than ever," April 27, 2022.

[3] *KPMG, Cybersecurity in ESG*, 2023.

[4] First Insight/Wharton School of the University of Pennsylvania, "The Sustainability Disconnect Between Consumers and Retail Executives," January 2022.

Los beneficios sociales de integrar activamente la ciberseguridad en la agenda ESG

El alcance del diálogo sobre ESG debe ampliarse: en muchas organizaciones, aún no es habitual hablar de ciberseguridad y privacidad en el contexto de ESG.

En el entorno actual, existen graves problemas con el contrato social entre organizaciones, equipos de trabajos y consumidores en relación con la protección de datos. Aumentar la confianza debe ser una prioridad en la agenda cibernética cuando se trata de cómo se utilizan los archivos de vídeo y audio en la creación de deepfakes - imágenes, vídeo o audio con un individuo específico que se sustituye por la cara o la voz de otra persona o se manipula para dar la impresión de que el individuo hizo o dijo algo que no hizo.

Los deepfakes son difíciles de combatir, ya que, en muchos casos, depende del público interpretar si el vídeo o el audio es real o fraudulento. Las organizaciones deben estar atentas para identificar y eliminar estos archivos y deben participar en la educación del público en general sobre el tema.

La cibernética desempeña un papel cada vez más importante en la IA y la ética de los datos. Determinar que los datos utilizados para entrenar los algoritmos de IA son precisos, no han sido corrompidos y están libres de prejuicios es una tarea titánica y, quizás en última instancia, imposible, pero merece la pena el esfuerzo.

La privacidad y la ciberseguridad también desempeñan un papel vital en la protección de la libertad de expresión y la seguridad de los canales de comunicación digital que proliferan hoy en día. Los controles de la privacidad también pueden desempeñar un papel clave a la hora de limitar la explotación y el uso indebido de información personal sin consentimiento o conocimiento. Esto es vital para mantener la confianza del público en las organizaciones.

Muchos programas de descarbonización y reducción de CO_2 se basan en tecnologías digitales y sistemas automatizados para supervisar y gestionar la producción, distribución y consumo de energía. Por muy eficientes que puedan ser estas herramientas, también pueden crear vulnerabilidades imprevistas en materia de ciberseguridad y exigir un alto nivel de protección de los datos. Integrar estratégicamente la ciberseguridad puede ayudar a mitigar las amenazas, reducir el riesgo de filtración de datos y garantizar el cumplimiento de la normativa.

Por último, tanto la ciberseguridad como la privacidad tienen una importante dimensión de responsabilidad social en la que las organizaciones deben trabajar con los clientes B2C y B2B para ayudarles a ser más conscientes de la ciberseguridad. Los bancos lo hacen habitualmente, y los minoristas cada vez más. También existe una conexión con la cadena de suministro y la seguridad del ecosistema, donde es fundamental mejorar la seguridad del ecosistema de proveedores.

¿Realmente le importa a los demás que una empresa tenga un incidente cibernético si se ha logrado manejar?

En teoría, la mayoría de los clientes probablemente diría que no quieren que una empresa cuyos productos o servicios utiliza sufra una filtración de datos. Pero esas mismas personas no quieren pagar más y quieren que los puntos de contacto sean rápidos y sin fricciones. En gran medida, a la gente no le importa hasta que algo malo se materializa, y parece como si quisieran que el trabajo de seguridad ocurra "tras bambalinas".

Una gran parte de la ecuación consiste en demostrar a los clientes que la ciberseguridad es un imperativo de la organización: simplemente es lo que hay que hacer. Las organizaciones deben enfocar esto como si estuvieran formando a sus clientes para que comprendan y se preocupen por las implicaciones de la ciberseguridad y demuestren que lo que están haciendo no es una tarea más, sino un servicio vital.

Formar a personas ajenas a su organización es en sí mismo un ejercicio de mantenimiento de ESG. El Mes de la Concientización sobre Ciberseguridad es un ejemplo de cómo el gobierno y las empresas trabajan juntos para garantizar que los empleados y los consumidores aprecien los fundamentos de la ciberseguridad para evitar los riesgos más obvios.

La seguridad al 100% no existe. A pesar de que se tomen todas las precauciones, los incidentes ocurren. En caso de incidente cibernético, tome rápidamente una decisión sobre si necesita revelar lo sucedido y, en caso afirmativo, cuánta información está dispuesto -u obligado- a compartir.[5] Es vital ser abierto y honesto; una buena comunicación puede hacer que los clientes confíen en una organización incluso más de lo que lo hacían antes del incidente.

[5] KPMG International, "Maintaining cyber vigilance and staying resilient," 2023.

Acciones recomendadas

Conéctese con el equipo ESG de su organización para determinar si el mismo considera la ciberseguridad como un aspecto clave dentro de sus funciones. De no ser así, haga un esfuerzo para sembrar conciencia de cómo y por qué es algo importante para todas las áreas de ESG.

Use la practicidad. La ciberseguridad efectiva no consiste tanto en hacer que los grupos de interés hagan las cosas diferentes, sino de repensar las conversaciones en toda la empresa para inspirar otras áreas de la organización a infundir seguridad en lo que ya hacen.

Mejore su inteligencia reglamentaria global en materia cibernética en general y ESG y privacidad en particular para garantizar el cumplimiento y la presentación de informes oportunos; realice un seguimiento y familiarícese con las regulaciones cada vez más exigentes y sus efectos en sus esfuerzos cibernéticos.

Conozca más

Ciberseguridad en ESG

Es hora de contemplar a los aspectos ESG y a la ciberseguridad a través del mismo lente.

Reporte tecnológico global de KPMG: ESG

Cómo los negocios pueden hacer uso de la tecnología como una oportunidad para afrontar sus ambiciones de ESG.

Camino a la preparación

KPMG ESG Assurance Maturity Index 2023.

Consideración 2

Incorporar la ciberseguridad y la privacidad de una vez y para siempre

La seguridad, desde el CISO hasta todo el equipo que dirige, es una función muy diferente hoy en día. La cibernética está cada vez más integrada en los procesos empresariales centrales. Esa realidad se está reflejando en un alejamiento de una centralización de la ciberseguridad en el rol del CISO hacia un modelo federado, en el que el CISO es el director de la orquesta, establece los marcos, evalúa el riesgo y brinda apoyo para la implementación.

La seguridad es parte integral de todas las funciones de la organización, desde la alta gerencia hasta los procesos administrativos, y muchos líderes ahora reconocen el valor de integrar una mentalidad de seguridad en sus muy diferentes culturas y procesos comerciales.

Los modelos de negocio y la tecnología están cambiando y causando un impacto en la seguridad

Ya sea que se fabrique un widget, se entregue un servicio o se cree información, los modelos operativos se basan cada vez más en la nube, lo que, junto con otras nuevas tecnologías, se utiliza para aumentar la escalabilidad, reducir costos, generar ingresos y ampliar los márgenes de ganancias.

La industria automotriz es un buen ejemplo de transformación de modelos de negocio. Los coches de hoy se han convertido en enormes tabletas sobre ruedas. La gente pide pizza desde la carretera y ni siquiera usa el teléfono. Se ha añadido tanta tecnología a los automóviles propulsados por gasolina, por no hablar de los vehículos eléctricos, que se han convertido posiblemente en el producto más sofisticado disponible para los consumidores minoristas.

La desventaja de la tecnología es que amplía la superficie de ataque, creando nuevas vulnerabilidades potenciales y aumentando la complejidad del ecosistema al que deben enfrentarse los CISO. Al mismo tiempo, el costo de la ciberseguridad se está disparando, lo que lleva a las organizaciones a considerar mejores estrategias para brindar esos servicios.

En este nuevo mundo, las organizaciones no pueden desplegar cientos de personas; los equipos de seguridad deben ser ágiles, particularmente aquellos integrados en líneas de negocios. Las organizaciones deben encontrar la combinación adecuada de personas y tecnología, utilizando la IA en general y el aprendizaje automático en particular para cubrir el terreno que los humanos no pueden de manera eficiente.

Realizar revisiones oportunas de soluciones en miles de aplicaciones es simplemente imposible para los humanos, Las organizaciones deben decidir dónde empezar a incorporar la seguridad dentro de los procesos de desarrollo de aplicaciones y pasar a un monitoreo continuo para comprender el impacto de posibles ataques y vulnerabilidades.

La ironía es que no hace falta que el CISO haga eso. Gestionar estos riesgos requiere un cambio cultural en toda la empresa para adoptar la seguridad como parte de los procedimientos operativos estándares de la organización. Los CISO no instalan parches y no administran las operaciones. Los equipos de seguridad deben determinar cómo y dónde integrar ciertas tareas de seguridad en la empresa y monitorear esas tareas para garantizar que se lleven a cabo correctamente. Así es como vemos la evolución de los equipos de seguridad.

Será una cuestión de "contratación interna" para acercar la seguridad al cliente o subcontratación a un proveedor de servicios externo para aprovechar de manera eficiente habilidades especializadas que tal vez no existan dentro de la organización. Muchas organizaciones luchan con la idea de la seguridad como una competencia central, particularmente cuando intentan dominar el gran volumen de nuevas tecnologías.

Trabaje con líderes empresariales para integrar la seguridad de manera efectiva

Se habla mucho de "girar a la izquierda", pero si bien reconocemos la importancia de considerar la seguridad desde el principio, también creemos que las organizaciones deben mirar de un extremo a otro (desde el concepto hasta la construcción e incluir el monitoreo continuo) y abordar la seguridad como un requisito continuo. A lo largo de ese viaje, el elemento número uno de la seguridad es la visibilidad.

Los profesionales de la seguridad se parecen cada vez más a los controladores del tráfico aéreo y las pistas deben mantenerse despejadas. Los CISO deben asegurarse de que el "tráfico", es decir, las aplicaciones, entre y salga de manera eficiente y segura. La seguridad no debería retrasar el lanzamiento de productos y servicios, pero debería haber una visibilidad temprana de los procesos que emplea la empresa.

Integrar la seguridad en un negocio más amplio debe verse como un ejercicio para impulsar la excelencia operativa. Los equipos de seguridad deben describir y demostrar cómo se ve lo "bueno" e inspirar a los profesionales de seguridad integrada de toda la empresa a gestionar esa visión. Es cuestión de establecer barreras de seguridad adecuadas para permitir que se incorpore un enfoque seguro desde el diseño y luego integrar las herramientas y plantillas adecuadas en los entornos de desarrollo.

Los CISO y sus equipos, así como el personal de seguridad integrado en la empresa, deben adoptar un enfoque holístico hacia la excelencia operativa y la responsabilidad compartida. Esto significa dar la misma consideración a las personas, los procesos, la tecnología y los requisitos regulatorios. Al centrarse en la gestión de riesgos, la gestión de incidentes,

> **Hace diez o quince años, la regla 80/20 para los profesionales de seguridad era 80 por ciento de habilidades técnicas y 20 por ciento de habilidades sociales. Si los CISO quieren asegurarse de que no sean percibidos simplemente como personal de apoyo, deben sentirse cómodos con la regla revisada 80/20 según la cual imperativos como la comunicación, la generación de confianza, la resolución de problemas y la gestión de conflictos son tan vitales como garantizar un centro eficiente de operaciones de seguridad.**

Brian Geffert
Director
Servicios de
Ciberseguridad
KPMG en EEUU

la gobernanza y el cumplimiento, las soluciones tecnológicas y la capacitación y concientización de la seguridad sostenible.

Esto es particularmente pertinente a medida que las organizaciones se preparan para las nuevas normas de ciberseguridad de la SEC[6] y la Directiva NIS2 de la UE, que requiere que los estados miembros implementen leyes para proteger a las empresas esenciales de las amenazas cibernéticas para octubre de 2024.[7]

Qué deben hacer los CISO para seguir siendo relevantes

La mayoría de los CISO comprenden las implicaciones de seguridad en torno a los datos, las aplicaciones y la superficie de ataque general, pero realmente pueden diferenciarse en relación con el talento, los presupuestos y las políticas entre organizaciones. Los CISO que entienden cómo trabajar en toda la organización para integrar la seguridad en el negocio mientras mantienen un rol de socio son los que tienen mayor éxito. Los equipos de seguridad deben tener conocimiento de las iniciativas que están planificando las unidades de negocio y de los posibles nuevos vectores de amenazas que pueden revelarse.

Los CISO deberían trabajar para hablar el idioma de sus socios comerciales en lugar de un lenguaje cibernético esotérico. Por ejemplo, no hablemos de vulnerabilidades de día cero, amenazas persistentes avanzadas o estrategias de orquestación, automatización y respuesta de seguridad (SOAR). Esos términos no significan nada para la mayoría de los colegas ajenos a la seguridad. En lugar de eso, diga: "Si este plan no funciona, quedará excluido de tal o cual mercado. Si no podemos proteger con éxito la línea de productos, no se podrán generar suficientes ingresos porque la gente no utilizará los productos".

Los equipos de seguridad no necesitan emplear tácticas de miedo. Más bien, necesitan adoptar un nuevo punto de vista basado en la habilitación empresarial y la reducción de riesgos.

Los CISO deben inspirar a las personas a confiar en que su orientación y visión estratégica son lo mejor para la organización. Su mercancía es la confianza.

Nuevas habilidades y competencias esenciales

Los profesionales de la seguridad deben mejorar sus habilidades interpersonales, incluidas las habilidades interpersonales como las negociaciones, la gestión del tiempo, la capacidad de escucha y la creación de redes. Hace diez o quince años, la regla 80/20 para los profesionales de seguridad era 80 por ciento de habilidades técnicas y 20 por ciento de habilidades sociales.

Hoy en día, esa ecuación ha cambiado. Si los CISO no pueden trabajar con el liderazgo ejecutivo para contar una historia que la organización pueda comprender y posicionar de manera coherente las ideas para influir en las acciones en toda la empresa, simplemente no tendrán éxito.

Además de estas habilidades más interpersonales, los líderes de seguridad deberían considerar aprovechar las metodologías de cuantificación del riesgo cibernético para gestionar de manera más efectiva la exposición general al riesgo. Esto permitirá una mejor comunicación y articulación de los riesgos financieros, así como dónde la organización debe priorizar su inversión en ciberseguridad.

El equipo de seguridad debe reconocer que se comunica principalmente con colegas no técnicos para que comprendan el riesgo y actúen en consecuencia. Si los CISO quieren asegurarse de que no sean percibidos simplemente como personal de apoyo, deben sentirse cómodos con la regla revisada 80/20 según la cual imperativos como la comunicación, la generación de confianza, la resolución de problemas y la gestión de conflictos son tan vitales como garantizar un centro eficiente de operaciones de seguridad.

[6] Comisión de Bolsa y Valores (SEC), "SEC Adopts rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies" 26 de julio de 2023.
[7] Parlamento Europeo, "The NIS2 Directive: A high common level of cybersecurity in the EU", 2 de agosto de 2023.

Acciones recomendadas

Aportar una nueva perspectiva a la junta directiva sobre lo que podría ser un agente disruptor del negocio y qué se debe hacer para gestionar dichos riesgos sin afectar las operaciones y la experiencia del cliente.

Los equipos de seguridad deben determinar cómo y dónde integrar ciertas tareas de seguridad dentro de la empresa en lugar de subcontratarlas a un proveedor de servicios externo y monitorear dichas tareas para garantizar que se lleven a cabo correctamente.

Gestionar el equipo cibernético como una empresa, lo que significa que se debe ceder cierto grado de control sobre lo que hacen otras partes de la organización desde una perspectiva de seguridad.

Conozca más

Encuesta CEO Outlook 2023 de KPMG

Más de 1.300 CEO globales comparten sus visiones sobre geopolítica, regreso a las oficinas, ESG e IA generativa.

Reporte tecnológico global de KPMG 2023

Descubra cómo los líderes están asegurando el valor al navegar un ámbito de incertidumbres con confianza.

El futuro de IT

Descubra las estrategias para avanzar en la función de IT y preparar a las organizaciones para triunfar en la nube y en una era liderada por la IA.

Consideración 3

Navegar por fronteras globales difusas

Los negocios globales operan dentro de un espacio regulatorio cibernético y de privacidad cada vez más complejo. Los intereses nacionales están en juego, lo que lleva a diversos requisitos reglamentarios sobre la soberanía de la información, la seguridad de la cadena de suministro, la transparencia del cumplimiento de los controles cibernéticos, la notificación de incidentes y, por supuesto, la privacidad. Las empresas necesitan calibrar sus informes reglamentarios para un mundo con fronteras cada vez más difusas, pero también mantener controles de seguridad que puedan adaptarse a los requisitos locales. Las organizaciones deben estar preparadas para responder rápidamente ante los cambios geopolíticos y los diversos requisitos de sanciones.

"La gran pregunta para los profesionales de la seguridad es cómo lograr el equilibrio adecuado entre la habilitación empresarial y el valor empresarial, garantizando al mismo tiempo que se mantengan en el lado correcto de los reguladores."

Orson Lucas
Director
Servicios de Ciberseguridad
KPMG en EEUU

Panorama empresarial global: Objetivos cibernéticos y de privacidad comunes, pero divergentes en la práctica

Durante años, el panorama reglamentario global ha estado muy desarticulado. Mientras que algunos mercados dieron prioridad a normativas agresivas en los últimos años, muchos no lo hicieron.
Como resultado, las organizaciones se vieron abocadas a tomar la decisión de implementar sistemas de gobernanza, procesos y controles elevados en función de cada mercado, o bien tratar las normativas emergentes como un indicador de lo que estaba por venir e invertir en programas de privacidad y seguridad proactivos, maduros y automatizados. Mientras que algunos optaron por lo segundo, el presupuesto, los recursos y otras prioridades empresariales en competencia hicieron que muchas organizaciones optaran por lo primero.

Sin embargo, se trata de un escenario que evoluciona lentamente. Mercados como Europa, China y Estados Unidos están marcando la pauta, y muchos otros están siguiendo su ejemplo. Están surgiendo patrones y principios en los ámbitos de la seguridad, la privacidad y la IA. Esto brinda a las principales organizaciones la oportunidad de unirse, a escala local y mundial, en torno a un enfoque basado en principios para proteger y gestionar de forma proactiva la información sensible. Idealmente, esto se manifestará en programas globales únicos de privacidad y seguridad que tengan en cuenta los matices de la normativa y las prácticas locales en mercados específicos. Sin embargo, hay varios retos que las organizaciones verdaderamente globales tendrán que superar para hacer realidad esta visión.

Por ejemplo, las consideraciones relativas a la localización y transferencia de datos requieren una sólida comprensión del inventario y los flujos/transferencias de datos, tanto internamente como con socios comerciales externos y de la cadena de suministro. A menudo, existen múltiples caminos, aunque todos requieren una planificación e intencionalidad significativas para ayudar a garantizar prácticas eficientes, rentables y conformes.

Desde un punto de vista empresarial, las organizaciones seguirán necesitando una audiencia y una huella globales para ampliar sus operaciones, independientemente de la jurisdicción y de dónde tengan su sede. La gran pregunta para los profesionales de la seguridad es cómo lograr el equilibrio adecuado entre la habilitación empresarial y el valor empresarial, garantizando al mismo tiempo que se mantengan en el lado correcto de los reguladores. Es una línea muy fina y un reto claro para los CISO, los CPO y sus equipos.

Las empresas globales se enfrentan a retos para cumplir los cambiantes requisitos normativos

Las organizaciones deben navegar por las aguas reguladoras con cuidado, sabiendo que las normas están en continua evolución. A medida que maduran las herramientas de gestión de las relaciones con los clientes y la tecnología de marketing (MarTech), las organizaciones se dan cuenta del valor de los datos a través de la información y el rendimiento de la inversión que proporcionan a la empresa.

Los reguladores han respondido con normas de privacidad específicas en muchas jurisdicciones de todo el mundo, exigiendo a los CISO, CMO, CDO y CPO que se aseguren de tener una segunda línea de defensa sólida para navegar y cumplir con los requisitos reglamentarios actuales y previstos.
En términos de consecuencias, muchos países y territorios imponen ahora estrictas sanciones económicas -así como suspensiones de licencias comerciales- por infracciones de privacidad.

El aislamiento de la privacidad se está disipando rápidamente. A medida que evoluciona el enfoque de los reguladores, áreas como la compra y venta de datos, el consentimiento y la gestión de preferencias, la ética de los datos y el uso responsable de la IA están aplanando los silos entre las partes interesadas y las funciones empresariales y haciendo que las Juntas Directivas y la gerencia ejecutiva adopten una visión basada en objetivos centrada tanto en el cumplimiento de la normativa como en la confianza del consumidor. Esto último es algo que las organizaciones líderes están utilizando para diferenciarse a medida que buscan construir, mantener y transformar las relaciones con los consumidores.

> “En el mundo actual, en el que los objetivos y las tácticas de la ciberdelincuencia son cada vez más nefastos y sofisticados, tanto los clientes como las empresas y los organismos reguladores deben adoptar un enfoque mucho más holístico de la gestión de datos y la protección de la información.”

Henry Shek
Socio
Servicios de Ciberseguridad
KPMG en China

Dinámicas geopolíticas cambiantes que influyen en la velocidad de respuesta y la adaptabilidad

Hacer negocios en múltiples regiones es todo un desafío en el entorno actual porque las herramientas y tecnologías que las organizaciones utilizan en un mercado pueden no ser accesibles en otros. Por ejemplo, en algunas partes de China, algunas empresas pueden no tener acceso a ciertas herramientas clave porque la disponibilidad puede estar restringida debido a las decisiones de los proveedores de suministrar en el mercado chino. Se trata de un problema que afecta tanto a la cadena de suministro como a la resiliencia operativa y que puede repercutir gravemente en la productividad de la organización.

Una consideración central que las organizaciones deben examinar es cómo navegar de la manera más eficaz en el cada vez más complejo panorama empresarial global para garantizar la resiliencia y la continuidad del negocio. Intentar navegar por los retos de la privacidad y los datos requiere un plan de gobernanza bien definido que alcance rápidamente un nivel mínimo de madurez cuando la organización opera en jurisdicciones con regímenes de sanciones estrictos.

De hecho, las normativas chinas tienen un enfoque distinto a las de la UE, que son diferentes a las de otras partes del mundo. Tienen ámbitos de aplicación, definiciones de datos personales, limitaciones de recopilación, normas de responsabilidad y marcos jurídicos básicos diferentes. Sin una visión, una estrategia, una gobernanza y un plan táctico sólidos y basados en principios definidos, las organizaciones tendrán cada vez más dificultades para innovar o correrán el riesgo de quedarse rezagadas.

La politización de los negocios y su impacto en la seguridad es otra dinámica a tener en cuenta. En Estados Unidos, por ejemplo, algunas empresas se inclinan políticamente en uno u otro sentido, a veces en función de los valores internos de sus dirigentes, pero a menudo en respuesta a la clientela a la que se dirigen. Esta evolución llegó a un punto álgido con el conflicto de Ucrania, ya que las empresas que siguieron operando

o haciendo negocios con Rusia fueron objeto de sanciones.

Desde el punto de vista de la seguridad e IT, el concepto de segmentación o microsegmentación -por el que las empresas pueden gestionar las cargas de trabajo en un centro de datos o un entorno en la nube con controles de políticas granulares y restringir la propagación de amenazas laterales- es instructivo. Las organizaciones con redes holísticas pueden crear estos segmentos conectados pero separados por cortafuegos. Estamos comprobando que las empresas que cuentan con modelos de segmentación tienen mayor capacidad de aislar eficazmente las operaciones regionales con rapidez en caso de ser necesario.

Las empresas globales deben considerar la jurisdicción nacional a través de diferentes perspectivas. Por ejemplo, ofrecer servicios a ciudadanos de la UE fuera de Europa activa los requisitos del GDPR. En general, las empresas deben tener claro dónde están ubicadas sus operaciones, de quién dependen para realizar negocios (es decir, proveedores),

los mercados en los que ofrecen productos y servicios, y dónde están constituidas como entidad jurídica. La interacción entre estos cuatro conceptos de soberanía da lugar a un complejo panorama normativo en el que se navega con mayor eficacia mediante un enfoque operativo flexible y basado en políticas.

Otra consideración es la redundancia. Por ejemplo, supongamos que una empresa mantiene todo su centro de atención telefónica en una jurisdicción que, por una razón u otra, se ve restringida y debe cerrar todas sus operaciones en ese país. ¿Qué ocurre con el servicio de atención al cliente? Disponer de cierto nivel de negocio, seguridad y redundancia en caso de que la organización necesite apartarse temporalmente del negocio en cierta parte del mundo para sortear los desafíos geopolíticos imperantes puede ayudar a aliviar el riesgo de limitar el negocio más amplio en el proceso.

En definitiva, los CISO y sus equipos deben aplicar siempre una perspectiva de resistencia y preparación. Esto ayuda a las empresas a ir un paso por delante del próximo suceso de cisne negro y a consolidar la capacidad de tomar esas decisiones "disruptivas" con rapidez y confianza, en lugar de verse obligadas a improvisar apresuradamente una estrategia cibernética de hiper-localización.

Acciones recomendadas

- Mantener una comprensión del panorama reglamentario global, específicamente una comprensión de las reglas relevantes a un nivel granular y jurisdiccional.
- Reconocer dónde residen los datos críticos (tanto estructurados como no estructurados) en toda la organización, así como dónde se comparten con socios externos.
- Mejorar la transparencia para generar confianza en las cadenas de suministro globales; en lugar de tratar las relaciones con terceros, cuartos e incluso quintos proveedores únicamente como transaccionales y contractuales (que lo son), acérquelas como una extensión de su ecosistema.

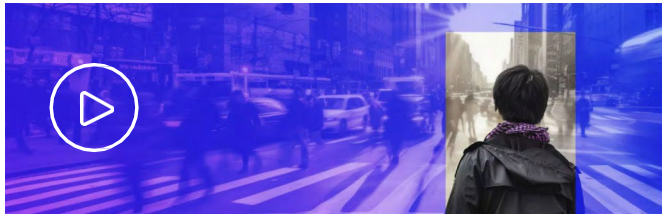
Conozca más

Análisis de riesgo de privacidad 2023

Mantenerse al tanto de los cambiantes desafíos de los riesgos de privacidad.

El hostil centro de atención

El futuro cibernético en la geopolítica.



Global Economic Outlook (Perspectiva económica global)

KPMG International Global Economic Outlook — H2 2023.

Consideración 4

Modernizar la seguridad de la cadena de suministros

El enfoque actual de muchas organizaciones con respecto a la seguridad de terceros y de la cadena de suministro no se ajusta a la realidad del complejo e interdependiente ecosistema actual de organizaciones asociadas. Los modelos tradicionales se basan en el supuesto de que los terceros prestan servicios de forma transaccional. Esa visión no refleja la intrincada red actual de API y procesos vinculados por un complejo conjunto de dependencias de software como servicio. Se recomienda a las organizaciones que establezcan asociaciones más estratégicas con los proveedores centrados en la supervisión y gestión continuas de los perfiles de riesgo cambiantes de estos proveedores para reforzar la resistencia operativa.

"A pesar de los retos y de las prioridades contrapuestas, garantizar la seguridad del ecosistema de terceros no debería ser un obstáculo, sino una herramienta de negocios. Pero no puede haber métodos abreviados. Esto eleva la acuciante necesidad de modernización. ¿Cómo hacerlo de forma más rápida, eficiente y con un mínimo de recursos sin comprometer la calidad? Ahí es donde una mentalidad basada en el riesgo, junto con un enfoque impulsado por los datos y potenciado por la automatización inteligente, puede marcar una diferencia tangible."

Mitushi Pitti
Director General
Servicios de Ciberseguridad
KPMG en EEUU

La evolución del panorama de la cadena de suministro está afectando los modelos de seguridad tradicionales

Históricamente, el modelo de seguridad de terceros se ha centrado en evaluaciones puntuales. La supervisión continua y la realización de inventarios de los componentes de software de proveedores utilizados con frecuencia pueden ayudar a los CISO a comprender mejor la estructura de seguridad de estos proveedores y a identificar posibles riesgos. Con esta dinámica en mente, los CISO deben desarrollar un estándar más moderno para contener la exposición al riesgo en tiempo real.

Para lograr esa postura, vemos tres retos claves para los CISO y sus equipos:

Visibilidad

Un problema de larga data ha sido la incapacidad de las organizaciones para cubrir toda la población de proveedores. Las grandes organizaciones pueden tener miles de proveedores, y a menudo no pueden evaluar con precisión sus actividades con los métodos tradicionales. Se necesitaría un ejército de personal de seguridad para realizar todas las evaluaciones físicas de los puntos finales, lo cual es humanamente imposible. Costaría decenas de millones de dólares, lo que lo hace poco realista desde el punto de vista logístico y presupuestario.

Adaptabilidad

Más allá de comprender el perfil de riesgo de la amplia población de proveedores, la capacidad de ampliación permite a las organizaciones seguir el ritmo de los retos de un panorama en constante expansión y cambio. Desde las nuevas tecnologías y procesos hasta la posibilidad de que un proveedor no siga explícitamente sus protocolos de seguridad, el entorno de terceros es un vector de amenazas en constante movimiento.

El perfil de riesgo en evolución de los socios externos

El antiguo modelo transaccional no contaba con un mecanismo para hacer un seguimiento de cómo está cambiando la relación y cómo eso podría estar creando nuevas vulnerabilidades. Como resultado, dependiendo de la madurez del proveedor, las organizaciones necesitan hacer más (instituir revisiones mensuales) o quizás menos (permitir más autonomía con revisiones trimestrales) para asegurar que estas relaciones operan eficientemente y se adhieren a todos los requisitos de cumplimiento.

Con el rápido ritmo del cambio tecnológico y la realidad de que los clientes son más exigentes, las organizaciones buscan seguir siendo innovadoras. Y, por supuesto, los contratistas y subcontratistas -y los ciberdelincuentes- están haciendo lo propio.

Por ejemplo, muchos proveedores están desplegando la IA para mejorar los procesos y completar las tareas más rápidamente. Pero, por fascinante y poderosa que sea, la IA plantea una serie de nuevos riesgos potenciales, desde cuestiones relacionadas con la integridad de los datos, la validez estadística y la precisión de los modelos hasta problemas de transparencia y confiabilidad. Esta simulación del pensamiento humano por parte de las máquinas debe utilizarse de forma segura y responsable a nivel organizativo y por parte de terceros. Extrapolar estos riesgos a toda la cadena de suministro revela un nuevo panorama de amenazas que los CISO y sus equipos deben vigilar.

A pesar de los desafíos y de las prioridades contrapuestas, garantizar la seguridad del ecosistema de terceros no debería ser un obstáculo, sino una herramienta de negocios. Pero no puede haber métodos abreviados. Esto eleva la acuciante necesidad de modernización. ¿Cómo hacerlo de forma más rápida, eficiente y con un mínimo de recursos sin comprometer la calidad? Ahí es donde una mentalidad basada en el riesgo, junto con un enfoque impulsado por los datos y potenciado por la automatización inteligente, puede marcar una diferencia tangible.

El papel de las organizaciones gubernamentales

Las organizaciones que sufren de regulaciones estrictas, que deben seguir el ritmo del entorno normativo y trabajar con proveedores que no tienen las mismas limitaciones reglamentarias deben encontrar la forma de conseguir que cooperen y empleen los controles de seguridad adecuados. Es una batalla continua a la que se enfrentan las organizaciones. Están buscando la forma de que las normativas ayuden a obligar a terceros a ser más seguros en general.

Las recientes normas de la Comisión de Bolsa y Valores de Estados Unidos (SEC) en torno a la ciberseguridad tienen una posición sobre terceros.

Los reguladores saben que se trata de una preocupación prioritaria y un reto creciente para todas las organizaciones. Un pequeño empujón por parte de los reguladores deberían ayudar a convencer a los proveedores menos maduros para que participen en el programa un poco mejor y ayuden a apuntalar la postura cibernética.

Del mismo modo, la Directiva revisada sobre seguridad de las redes y de la información (NIS-2) de la UE hace hincapié en que las organizaciones deben gestionar de forma proactiva los riesgos introducidos por terceros. Asimismo, la Ley de Resiliencia Operativa Digital (DORA), que facilita la supervisión eficaz de los riesgos planteados por proveedores externos de tecnologías de la información y la comunicación, se centra en controlar mejor la seguridad de la cadena de suministro.

Los reguladores, a través de la DORA, pretenden determinar qué terceros consideran críticos para la resistencia general del amplio ecosistema de proveedores. Puede que estos actores no estén regulados directamente, pero como se consideran de importancia sistémica, las entidades reguladas también les trasladarán sus requisitos.

Intercambio colaborativo de inteligencia: Una estrategia incipiente pero valiosa

En la práctica, el intercambio de información entre empresas y proveedores puede tardar años en llegar, pero es concebible que pueda consolidar las mejores prácticas y, en última instancia, mejorar las relaciones en la cadena de suministro.

Ante el aumento exponencial de la amenaza que representan los actores maliciosos, las organizaciones de diversos sectores, en particular las infraestructuras críticas, deben compartir mucho más la inteligencia sobre amenazas y riesgos, internamente, con el mercado y con los proveedores y socios.

> “la IA plantea una serie de nuevos riesgos potenciales, desde cuestiones relacionadas con la integridad de los datos, la validez estadística y la precisión de los modelos hasta problemas de transparencia y confiabilidad. Esta simulación del pensamiento humano por parte de las máquinas debe utilizarse de forma segura y responsable a nivel organizativo y por parte de terceros. Extrapolar estos riesgos a toda la cadena de suministro revela un nuevo panorama de amenazas que los CISO y sus equipos deben vigilar.”

Elizabeth Huthman
Director
Servicios de Ciberseguridad
KPMG en el Reino Unido

Las organizaciones deben tratar de acabar con la mentalidad de silo y animar a las partes interesadas de la empresa (compras, jurídico, unidades de negocio, riesgos, terceros) a comunicarse y colaborar.

La colaboración y el intercambio de información también ayudan a las organizaciones a gestionar el riesgo de concentración de proveedores. Esta es una consideración importante para las cadenas de suministro ampliadas -terceras, cuartas y quintas partes- en las que varias organizaciones dependen de los mismos proveedores. En estos casos, tiene sentido unir fuerzas manteniendo la confidencialidad en ciertos aspectos del panorama competitivo para garantizar que las terceras partes no sean un eslabón débil en el ecosistema.

Muchas organizaciones se muestran reticentes a esta forma de colaboración. Teniendo en cuenta esta realidad, la Agencia de Ciberseguridad de la Unión Europea (ENISA), a través de los Centros de Análisis e Intercambio de Información (ISAC), y la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) de Estados Unidos, están encabezando una serie de programas centralizados destinados a recopilar y difundir rápidamente información sobre amenazas y vulnerabilidades.

No se trata sólo de si un proveedor puede acceder a datos sensibles para el cliente o la empresa. Supongamos que un proveedor específico es fundamental para mantener la resistencia operativa -lo que significa que afecta a la capacidad de la organización para ensamblar y distribuir productos-, pero no está suficientemente maduro desde el punto de vista de la seguridad. En ese caso, deben tomarse medidas para aumentar la sofisticación de la seguridad del proveedor o puede ser necesario tomar la difícil decisión de cambiar de socio.

Al establecer una cultura corporativa basada en la concienciación sobre el riesgo y la seguridad, ningún individuo o proceso será visto como un eslabón débil o un obstáculo para el negocio. Y esa mentalidad se extenderá a todos los aspectos de la empresa, incluidas las filiales de terceros.

Acciones recomendadas

- Adoptar un enfoque basado en el riesgo para evaluar los procesos de terceros en lugar de un enfoque general para los diferentes proveedores que prestan diversos servicios.
- Aprovechar la automatización inteligente para obtener una mayor visibilidad de los cambiantes perfiles de riesgo de los proveedores y construir un programa de terceros sostenible y escalable con visión de futuro.
- Fomentar el crowdsourcing de inteligencia y compartirla tanto dentro de su organización como con terceros de confianza.

Conozca más

Adelantarse al riesgo cibernético en la cadena de suministro

Con complejas redes globales de proveedores y más vías para que los actores de amenazas encuentren una manera de entrar, comprender y prevenir el riesgo cibernético debe ser una prioridad.

Tendencias de la cadena de suministro 2024: la reestructuración digital

Con las oportunidades digitales arrasando el panorama de la cadena de suministro, la preparación y la línea de visión serán fundamentales para el éxito.

El futuro de la cadena de suministro

Desde ESG hasta los robots y el metaverso, los líderes de la cadena de suministro tienen nuevos desafíos para los que prepararse.

Consideración 5

Desbloquear el potencial de la IA — cuidadosamente

Con una planificación y ejecución cuidadosas, la IA transformará la manera, el momento y las personas que harán el trabajo. Actualmente se habla mucho de la IA generativa, pero muchas otras ramas de la IA, desde la robótica al aprendizaje automático, siguen transformando los negocios. Calibrar la seguridad, la privacidad y las implicaciones éticas inherentes a estas tecnologías es un reto, y las organizaciones buscan establecer marcos que proporcionen tanto gestión de riesgos como gobernanza a la hora de implementar herramientas de IA.

> Los datos son el eje fundamental de la seguridad en general y de la privacidad en particular. El sector necesita que los organismos gubernamentales de todo el mundo armonicen sus legislaciones, ya que la existencia de normativas dispares en las que unos países son más estrictos que otros desincentiva la innovación. El mercado necesita equilibrar esa necesidad de innovación con una orientación y unos límites reguladores eficaces.

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

El camino actual de la IA: Barreras limitadas, abundantes oportunidades

La preocupación por los resultados empresariales y la necesidad de fomentar la confianza entre la fuerza laboral y clientes, en concreto, y entre la sociedad, en general, ha suscitado un amplio debate ético sobre cómo controlar y desplegar la IA de forma responsable, transparente e íntegra.

Para ello, se están intensificando las normativas en este ámbito. Los sectores públicos y privados deben colaborar para ofrecer soluciones prácticas de apoyo a la innovación y el desarrollo que garanticen la seguridad y la privacidad desde el principio.

Existe cierta inquietud en el mercado por innovar debido a los titulares cautelosos, la falta de barreras normativas y la ausencia de un enfoque global estandarizado y universal de la IA. Pero esa inquietud se enfrenta a una pasión equivalente por el potencial de la IA para estimular la innovación.

Incluso los enfoques locales sobre cómo deben gestionarse, desplegarse y legislarse los modelos y algoritmos de IA son confusos. Algunos países y regiones están más avanzados que otros. Las organizaciones deben ser conscientes de los elementos fundamentales necesarios para establecer y mantener la confianza y, al mismo tiempo, ser conscientes de la dirección en la que avanza la normativa. Esto contribuirá en gran medida a minimizar el trabajo necesario para garantizar el cumplimiento de estos regímenes en el futuro.

Aunque animamos a las organizaciones a que sigan adelante con la apasionante y vital labor que están realizando con la IA, al mismo tiempo deben asegurarse de que comprenden a fondo las complejidades que involucra y cómo reducir el riesgo de sus modelos de forma eficaz.

A medida que se desarrolla el mercado, es importante dar tiempo a los reguladores y legisladores mundiales para que establezcan directrices significativas para el desarrollo de la IA. La Ley de IA de la UE es un ejemplo destacado. Esta legislación histórica está a punto de hacer por la IA lo que el Reglamento General de Protección de Datos (RGPD) de la UE ha hecho por la privacidad, allanando el camino para avances interesantes y responsables en este campo.

Aunque la ausencia de legislación es un claro obstáculo, la buena noticia es que la legislación existente sobre privacidad tiene principios similares que pueden y deben aplicarse a los nuevos algoritmos de IA. Factores de privacidad como la notificación, el consentimiento, la capacidad de explicación, la transparencia y el riesgo de daño están codificados en la legislación vigente.

Para seguir siendo competitivos en el mercado, los CISO deben asociarse con los directores de datos y los responsables de su protección para apoyar los objetivos empresariales que dependen de la IA y determinar cómo aprovechar esta tecnología que cambia el juego de forma eficaz y responsable. Al mismo tiempo, deben dotar de gobernanza y controles suficientes a los procesos que pueden haber funcionado en gran medida sin supervisión durante algún tiempo. En esta armonía entre habilitación y gobernanza radica el éxito de la adopción.

Principales desafíos para equilibrar la innovación en IA con los intereses sobre seguridad y privacidad

Para facilitar la adopción de la IA, las organizaciones deben tomar decisiones cruciales que darán forma a su enfoque, como determinar si crear modelos internos o confiar en terceros. Aunque pueda parecer que una opción es menos incierta, lo cierto es que ambas conllevan riesgos inherentes que las organizaciones deben reconocer y gestionar eficazmente.

> **Los CISO, líderes senior y sus equipos deben respaldar los objetivos comerciales que dependen de la IA y determinar cómo para aprovechar esta tecnología innovadora de manera eficaz y responsable. Al mismo tiempo, necesitan dotar de suficiente gobernanza y controles a procesos que pueden haber operado en gran medida sin supervisión durante algún tiempo.**
>
> **Esta armonía entre habilitación y gobernanza es donde radica la adopción exitosa.**
>
> **Katie Boswell**
> Director General
> Servicios de Seguridad
> Cibernética
> KPMG en EEUU

Las organizaciones deben informarse sobre las garantías de transparencia, responsabilidad, imparcialidad, privacidad y seguridad para poder innovar e implantarse con confianza. Por ejemplo, hay que fijarse en las grandes empresas tecnológicas y en las jurisdicciones que están más avanzadas en su camino hacia la IA para obtener orientación sobre el desarrollo responsable.

Desde el punto de vista de la privacidad y la seguridad, muchas organizaciones se están viendo forzadas en cierto sentido. Con tantas unidades de negocio avanzando a toda máquina con la IA,

los CISO y directores de producto (CPO) deben seguirles la pista y asegurarse de que se instalan los controles necesarios. Establecer y mantener la confianza en esas soluciones de IA desde el principio son fundamental, para la marca y la capacidad de cumplir sus objetivos empresariales.

Ello requiere una cooperación interfuncional, especialmente desde el punto de vista de la financiación. Pero para aprovechar y perseguir a fondo las oportunidades de innovación, las organizaciones deben acordar una estrategia unificada de seguridad, privacidad, ciencia de datos y de índole jurídica. Siguiendo el ejemplo de la Ley de Inteligencia Artificial de la UE, el gobierno de EE.UU. ha dejado claro recientemente su compromiso con este imperativo colectivo mediante la publicación de una amplia Orden Ejecutiva sobre Inteligencia Artificial Segura y Confiable que codifica la seguridad, la privacidad, la equidad y los derechos civiles, así como la innovación y la competencia en relación con la IA.[8]

Lograr un equilibrio entre la rápida innovación en IA y la aplicación de sólidas medidas de privacidad y seguridad

Los datos son el eje fundamental de la seguridad en general y de la privacidad en particular. El sector necesita que los organismos gubernamentales de todo el mundo armonicen sus normativas, ya que la existencia de legislaciones dispares en las que unos países son más estrictos que otros desincentiva la innovación. El mercado necesita equilibrar esa necesidad de innovación con una orientación y unos límites reglamentarios eficaces.

Se trata de un cambio de mentalidad tanto cultural como tecnológico, en el que la gestión del cambio es un factor crítico para el éxito. Para integrar la privacidad y la seguridad desde el diseño con la IA y otras tecnologías emergentes, los profesionales que las gestionan no solo las tecnologías- deben dar prioridad a la privacidad y la seguridad. Si la organización tiene en cuenta la privacidad y la seguridad desde el principio, se convertirán en componentes naturales del modelo operativo.

Si el mundo mantiene el rumbo en la adopción de la IA para satisfacer las necesidades de innovación, acabará siendo algo habitual, como ocurre con la adopción de la nube.

Hubo un tiempo, no hace mucho, en que pasarse a la nube era una empresa monumental. Ahora, forma parte de la práctica empresarial habitual: no hay ningún aspecto de la seguridad que no tenga un elemento en la nube. Creemos que esa será también la progresión probable de la IA. No habrá "seguridad de la IA" porque formará parte de la seguridad general.

[8] Whitehouse.gov, Sala de Información, Acciones Presidenciales, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," 30 de octubre de 2023.

Acciones recomendadas

Alinear el marco de IA con los estándares actuales y desarrollar una sólida gobernanza de la IA alineando las prioridades de los distintos líderes empresariales de la organización y obteniendo el apoyo interfuncional de aquellos con un interés personal en el éxito de la IA.

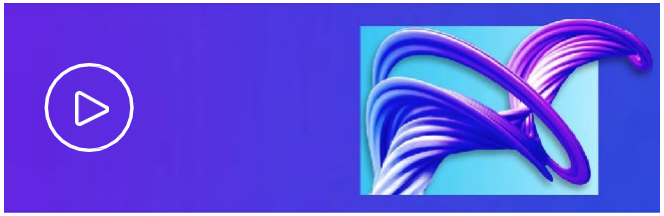
Garantizar que la finalidad de los algoritmos de IA, ya sean desarrollados interna o externamente, esté claramente definida y documentada y que los datos de entrenamiento sean pertinentes, adecuados para el objetivo empresarial y que cuenten con el consentimiento seguro.

Familiarizarse con las estipulaciones de la Ley de IA de la UE y la Orden Ejecutiva emitida por el gobierno de Biden sobre Inteligencia Artificial Segura y de Confianza.

Conozca más

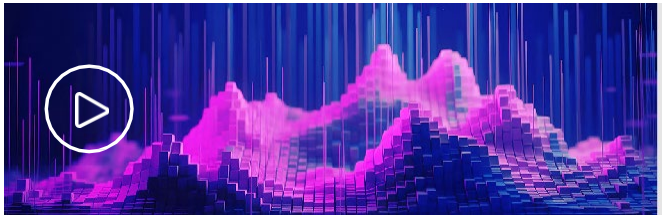
Privacidad en el nuevo mundo de la IA

Como establecer la confianza en la IA a través de la privacidad.



Modelos de IA generativa: riesgos y posibles recompensas en los negocios

¿Qué podría significar el auge de ChatGPT, DALL•E 2, Bard y otros para su organización?



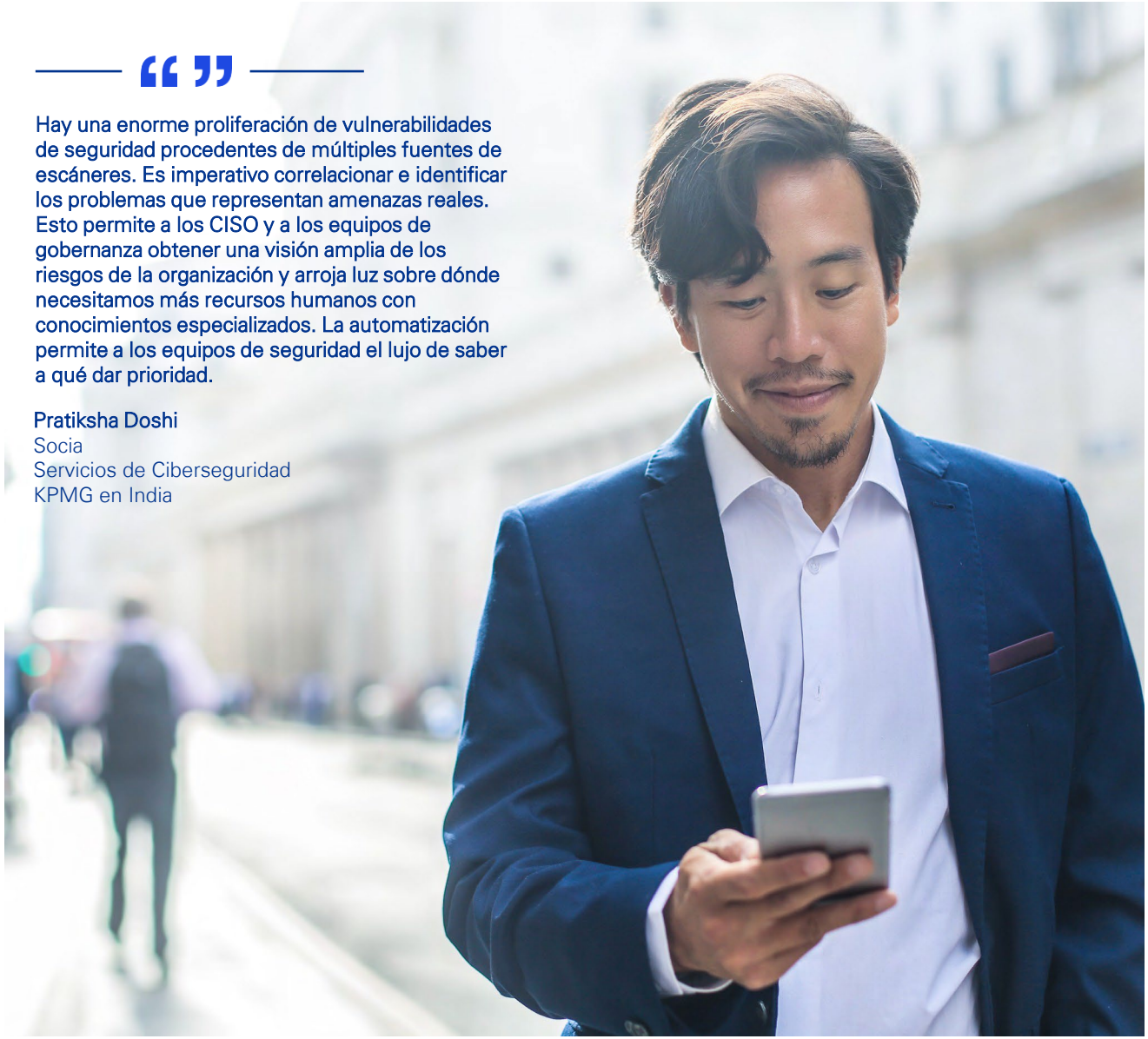
Informe de la encuesta de IA generativa de KPMG: Ciberseguridad

Una encuesta exclusiva de KPMG examina cuatro áreas en las que esta notable tecnología se muestra muy prometedora.

Consideración 6

Optimizar la seguridad a través de la automatización

Los negocios trasladan cada vez más sistemas a la nube, el volumen de datos que necesitan protección se dispara y cada vez más personas trabajan a distancia y acceden a las redes corporativas con sus propios dispositivos. Como resultado, la superficie de ciberataque se está expandiendo, creando más alertas, falsos positivos y protocolos de intervención que los CISO deben gestionar. Hay mucho ruido en los centros de operaciones de seguridad (SOC), y no hay suficientes cristales ni humanos para hacer frente al volumen. ¿Cómo pueden los CISO seguir detectando una amenaza tras otra y tener la sensación de que no se les escapa nada? Necesitan recopilar, correlacionar y escalar las señales que requieren una respuesta, y deben hacerlo rápidamente. La única forma de hacerlo es mediante la automatización.



> Hay una enorme proliferación de vulnerabilidades de seguridad procedentes de múltiples fuentes de escáneres. Es imperativo correlacionar e identificar los problemas que representan amenazas reales. Esto permite a los CISO y a los equipos de gobernanza obtener una visión amplia de los riesgos de la organización y arroja luz sobre dónde necesitamos más recursos humanos con conocimientos especializados. La automatización permite a los equipos de seguridad el lujo de saber a qué dar prioridad.

Pratiksha Doshi
Socia
Servicios de Ciberseguridad
KPMG en India

¿Por qué se debería automatizar la seguridad en este momento?

Las agendas digitales proliferan a gran velocidad. Al mismo tiempo, muchas organizaciones se ven a sí mismas como empresas tecnológicas, independientemente de su actividad principal, debido a la explosión de nuevas tecnologías digitales que muchas de ellas deben adoptar y dominar. Por ejemplo, las instituciones financieras son ahora casi completamente digitales en términos de interacción con el cliente, y muchos proveedores de servicios de salud están utilizando la telemedicina, dispositivos médicos impulsados por IA y el mantenimiento de registros basado en *blockchain*.

A medida que los modelos operativos se digitalizan, los equipos de seguridad necesitan automatizar y actualizar sus procesos para seguir el ritmo. De hecho, los atacantes también utilizan nuevas tecnologías y cada semana parecen más sofisticados. Y no se limitan a intentar acceder al entorno, sino que también utilizan la IA para cometer fraudes una vez allí. Los ciberdelincuentes están utilizando *deepfakes* - archivos multimedia sintéticos manipulados para imitar la apariencia, la voz o las acciones de otra persona- para ponerse en contacto con centros de llamadas e iniciar campañas de *phishing* más creíbles.

Los CISO deben ser tan sofisticados como los posibles atacantes para abrirse paso entre el parloteo e identificar rápidamente los incidentes legítimos; la forma más eficiente de hacerlo es adoptar la automatización y la IA en el SOC. La automatización de funciones de seguridad sencillas, como la gestión de registros, el análisis de amenazas y los controles de acceso, permitirá a los equipos de seguridad perseguir tiempos de respuesta más ágiles y eficientes.

Muchas organizaciones de numerosos sectores están automatizando con éxito la función de seguridad y liberando recursos humanos mediante la automatización de tareas rutinarias y repetitivas, empero vitales.

El trabajo que antes realizaban profesionales altamente calificados, como la exploración de vulnerabilidades, el análisis de registros y el cumplimiento de normativas puede estandarizarse y ejecutarse automáticamente.

La automatización está transformando el amplio panorama de la seguridad

La automatización de la seguridad se está convirtiendo en una herramienta fundamental en todas las funciones de ciberseguridad, la primera de las cuales es la prevención. La automatización de los procedimientos y actualizaciones programados puede desempeñar un papel clave a la hora de garantizar que las defensas corporativas y soberanas sean resistentes y fiables a medida que los actores maliciosos organizados y deshonestos amplían su escala y aceleran sus ataques. La automatización también puede ayudar a proteger el ecosistema de terceros, evaluando las vulnerabilidades y poniendo al descubierto los puntos débiles de los ecosistemas de vendedores y proveedores.

En cuanto a la detección y respuesta, la automatización puede ser valiosa para ayudar a los CISO a crear un nivel de seguridad de autoservicio que puede ser decisivo para completar las evaluaciones y pruebas e implantar los resultados en la red de producción. Esto reduce significativamente la mano de obra que de otro modo sería necesaria. Además, si las direcciones IP específicas ya están en la lista negra, no hay necesidad de intervención humana y el análisis de tickets puede automatizarse

Los malos actores utilizan la automatización para escalar y aumentar la velocidad de sus ataques. La forma más eficaz de defenderse contra un ataque automatizado es la detección y respuesta automatizadas. En caso de infracción, los procesos de supervisión automatizados pueden identificar incidentes de seguridad casi en tiempo real y comenzar la corrección alterando las reglas de las políticas de acceso o poniendo en cuarentena los dispositivos o usuarios dudosos.

> Los CISO y sus organizaciones de seguridad implementan la automatización para validar los controles mediante la recopilación de pruebas en el mundo real y demostrar que los controles funcionan según lo prescrito. Esto agiliza la gestión de riesgos y la gobernanza para la primera, segunda y tercera líneas de defensa.

Angela Leggett
Director General
Servicios de Ciberseguridad
KPMG en EEUU

Algunas organizaciones de seguridad implementan la automatización para recopilar pruebas forenses digitales y validar que los controles funcionan según lo prescrito. Esto agiliza la gestión de riesgos y la gobernanza para la primera, segunda y tercera líneas de defensa.

El cumplimiento de la normativa es otro excelente ejemplo del valor de la automatización. Por ejemplo, en julio de 2023, la SEC adoptó normas para las empresas públicas sobre gestión de riesgos de ciberseguridad estrategia y gobernanza. Según estas normas, los incidentes de seguridad importantes deben notificarse en un plazo de cuatro días laborables. Para cumplir con dicho requisito, las empresas deben detectar el incidente, evaluar su importancia y, a continuación, presentar el informe. Establecer un flujo de trabajo que genere y envíe automáticamente el formulario 6-K requerido puede ser una forma especialmente útil de apoyar los esfuerzos de cumplimiento.[9]

[9] SEC.gov, *SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*, 26 de julio de 2023.

Para las organizaciones globales, esto va incluso más allá de la presentación del 6-K. Se debe cumplir con una serie de requisitos de información reglamentaria en diferentes formatos y plazos, a veces medidos en horas. La automatización de estos procesos podría marcar la diferencia entre el cumplimiento y las infracciones.

La automatización afecta a los equipos de seguridad y a la empresa desde el punto de vista de las personas y las competencias

La automatización aumenta los procesos de seguridad y permite a los CISO dar prioridad al lugar más idóneo para desplegar al talento humano. Parece haber una enorme proliferación de vulnerabilidades de seguridad procedentes de múltiples fuentes de escáneres. Es imperativo correlacionar e identificar los problemas que representan amenazas reales. Esto permite a los CISO y a los equipos de gobernanza obtener una visión amplia de los riesgos de la organización y arroja luz sobre dónde necesitamos más recursos humanos con conocimientos especializados. La automatización permite a los equipos de seguridad el lujo de saber a qué dar prioridad.

Está claro que habrá cambios en el trabajo que realizan los equipos de seguridad. Cada vez más, los humanos se centrarán en cuestiones más estratégicas relacionadas con la evaluación de amenazas, la formación de concientización y la alineación empresarial, por nombrar solo algunas, en lugar de realizar el tipo de tareas repetitivas que pueden hacer la IA o los motores de análisis predictivo.

Y este trabajo requerirá nuevos conjuntos de habilidades. Por ejemplo, los CISO y sus equipos deben empezar a entender cómo funcionan los grandes modelos lingüísticos, cómo se pueden entrenar, cómo programarlos, etc. También es necesario crear conciencia y dominio de los conceptos de seguridad en relación con la nube, el Internet de las cosas y la IA.

Acciones recomendadas

Definir su visión y estrategia iniciales para la automatización. Considerar los objetivos de seguridad a corto y largo plazo, garantizar la alineación de esos objetivos con las prioridades empresariales de la organización y determine el tipo de protecciones que requieren esos objetivos compartidos.

Identificar cuáles son los datos accesibles de los que dispone organización de forma centralizada y definir un plan automatizado de supervisión de controles continuos para impulsar la eficiencia en las tres líneas de defensa.

Determinar qué herramientas crear en lugar de adquirir y comprender cómo se automatizan los socios de la cadena de suministro para reforzar la confianza entre las organizaciones y aprovechar ese aprendizaje cuando proceda.

Empoderamiento de la seguridad

Orquestación de seguridad y respuesta automatizada para ayudar a garantizar el futuro.

Generar confianza en entornos de nube

Encuesta sobre transformación de la nube de KPMG 2023

Dominar un entorno multi-nube

La evolución de las capacidades de la nube.

Consideración 7

Hacer de la identidad algo individual y no institucional

Cada organización con la que interactúan los consumidores les asigna una identidad digital única, y al igual que los nombres de usuario y las contraseñas varían, los métodos de autenticación también lo hacen. Desde el punto de vista de la ciberseguridad, el modelo de identidad está evolucionando. La mayoría de los modelos de gestión de identidades y accesos (IAM) fueron concebidos originalmente para gestionar identidades digitales y accesos de usuarios para organizaciones individuales. Muchos se están reconceptualizando ahora para abarcar un nivel de resiliencia adecuado para entornos informáticos federados, privados, públicos o multi-nube. Esto debería eliminar la necesidad de que los individuos garanticen el exhaustivo, largo e intrusivo proceso de comprobación de identidad cada vez que interactúan con una nueva institución, ya sea como cliente o empleado.

Los modelos de identidad tradicionales adoptan un enfoque federado

En el entorno actual, tener confianza en la identidad de las personas con las que interactúan las empresas es una de las principales preocupaciones de los responsables de seguridad, y un objetivo muy cambiante. En los últimos 10 o 20 años, la mayoría de las organizaciones diseñaron e implementaron sus programas de gestión de identidades. Los profesionales de la seguridad pensaban: "Si lo implemento yo, tendré todo el control". A pesar de ello, este enfoque creaba un punto de vista muy aislado y aumentaba el número de identidades únicas que había que gestionar. Desde la perspectiva del cliente, acabábamos teniendo decenas o centenares de identidades, una por cada empresa con la que nos conectábamos.

Hoy en día, la línea entre la seguridad de empresa a consumidor (B2C) y de empresa a empresa (B2B) se ha difuminado considerablemente. Dejando a un lado el hecho de que los usuarios B2B suelen tener un acceso más profundo a los recursos de la red que los usuarios B2C, ambos son usuarios externos, lo que ha llevado a las organizaciones, en muchos casos, a fusionar en gran medida a los dos en términos de sus enfoques de gestión de identidades.

Impulsadas por la expansión de los modelos de negocio, es vital que las organizaciones vean ahora la identidad no de forma aislada, sino desde una perspectiva holística. Este es un motor importante hacia un modelo de identidad en el que proveedores y clientes finales puedan interactuar ágilmente con múltiples organizaciones sin verse obligados a pasar cada vez por un complicado proceso de comprobación de identidad.

Los consumidores deben controlar sus identidades digitales, que deben ser transferibles entre sus personas consumidoras y empleadas. En los últimos años se ha producido una mejora en el nivel de ciberseguridad

> A medida que aumentan los niveles de confianza asociados a esas identidades, empezamos a ver una tendencia hacia un modelo de identidad federada, es decir, menos identificaciones digitales distintas que puedan aprovecharse de forma segura en distintos dominios.

Marko Vogel
Socio
Servicios de Ciberseguridad
KPMG en Alemania

que ofrecen muchos de los principales actores tecnológicos y sociales, y las identidades se utilizan en todo el ecosistema del comercio digital. A medida que aumentan los niveles de confianza asociados a esas identidades, empezamos a ver una tendencia hacia un modelo de identidad federada, es decir, menos identificaciones digitales distintas que puedan aprovecharse de forma segura en distintos dominios.

La evolución hacia un modelo en el que las identidades digitales con altos niveles de seguridad sean la norma permitirá a las empresas recopilar, almacenar y procesar menos información personal identificable (IPI), lo que sería un resultado decididamente positivo para los consumidores.

Cabe mencionar aquí el valor de *blockchain* en la gestión de identidades. Los sistemas de libro mayor distribuido se utilizan cada vez más para desarrollar modelos eficaces de identidad federada. La integración de la infraestructura de seguridad con la tecnología *blockchain* proporciona confianza a través de la visibilidad, el consentimiento verificable, el cifrado y las pistas de auditoría. Esto ayuda a las organizaciones a abordar los problemas de privacidad y fraude al delegar la gestión de derechos de datos y el control de acceso al sujeto en lugar de a un tercero centralizado.

Cuanto mayor sea el nivel de garantía de una identidad digital, más portátil será. Y cuando las identidades sean portátiles, podemos esperar ver una tendencia hacia menos inicios de sesión de los consumidores en general, es decir, menos identidades digitales. En última instancia, no solo tenemos que hacer que las identidades sean portátiles -de hecho, se espera que el uso de monederos digitales supere los cinco mil millones de usuarios en todo el mundo en 2026, un aumento de más del 50 por ciento desde los 3,4 mil millones en 2022[10] — sino que sean sistemáticamente a prueba de manipulaciones y verificables. Aquí es donde puede entrar en juego la biometría, que utiliza identificadores biológicos, físicos y de comportamiento únicos.

Una consideración relacionada es cuándo, o si, las organizaciones pueden deshacerse de las contraseñas, uno de los principales puntos de fallo de todos los sistemas de identidad. Parece productivo alejarse del modelo de contraseñas y ampliar el uso de múltiples factores de autenticación (dispositivo, ubicación, biometría, comportamiento) para la validación segura de la identidad, especialmente en todo el ecosistema empresarial. ¿Desaparecerán realmente las contraseñas? Es probable que aún falten años, pero parece que avanzamos en esa dirección.

La tecnología *deepfake* está cambiando el juego de la identidad

La amenaza que suponen los *deepfakes* -archivos de imagen, vídeo o audio sintéticos en los que se manipula y sustituye la apariencia, la voz o las acciones de una persona- es muy real, al igual que las implicaciones financieras, de reputación y de servicio que conlleva.

Los CISO deben acelerar la innovación en seguridad para seguir el ritmo.

Con la vertiginosa evolución tecnológica, las preocupaciones relacionadas con *deepfake* se están ampliando más rápidamente de lo que lo hicieron en relación con el *phishing* hace 25 años. Hoy en día, los ciberdelincuentes buscan objetivos más ambiciosos que los consumidores individuales o los personajes públicos. Ciberdelincuentes creativos y ambiciosos con acceso a la tecnología más avanzada han puesto sus miras en objetivos más rentables -empresas, instituciones y gobiernos-, muchos de los cuales están mal preparados para defenderse de esta amenaza.

La cuestión clave es qué se necesitará para entrenar a la tecnología en la creación de falsificaciones de audio y vídeo que puedan derrotar sistemáticamente la autenticación basada en la biometría.

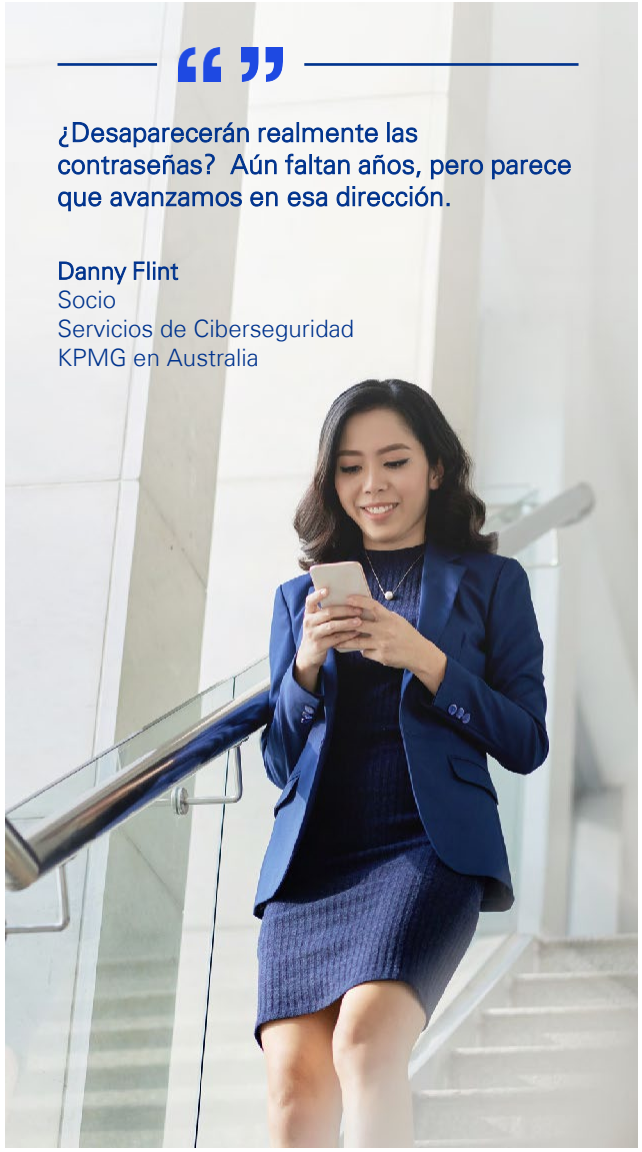
> **La evolución hacia un modelo en el que la identidad digital con un alto nivel de seguridad sea una realidad permitirá a las empresas recopilar, almacenar y procesar menos información de identificación personal, lo que es un resultado decididamente positivo para los consumidores.**

Jim Wilhelm
Director
Servicios de Ciberseguridad
KPMG en EEUU

Las consideraciones de costos por sí solas sugieren que se necesitarán atacantes cada vez más sofisticados, pero a medida que se amplíe el acceso a la tecnología, será menos costosa, lo que facilitará a los malos actores emplear las *deepfakes* como táctica fraudulenta.

Una preocupación clave en relación con las falsificaciones profundas es la financiación necesaria para la detección, desde el mantenimiento de la potencia informática adecuada, los algoritmos forenses y los procesos de auditoría hasta el talento necesario para emplear estas herramientas. Se anima a los CISO a entablar conversaciones con los altos responsables de la toma de decisiones para garantizar que los presupuestos se ajustan a las amenazas emergentes y mantienen la tecnología al día, asegurándose de que las actualizaciones de software se instalan tan pronto como se publican.[11]

[10] Juniper Research, *Digital Wallets: Market Forecasts, Key Opportunities and Vendor Analysis 2022–2026*. August 2022
[11] KPMG in the US, "Deepfakes: Real threat," 2023.



¿Desaparecerán realmente las contraseñas? Aún faltan años, pero parece que avanzamos en esa dirección.

Danny Flint
Socio
Servicios de Ciberseguridad
KPMG en Australia

El papel del Gobierno en el nuevo ecosistema de la identidad

Los sectores público y privado parecen estar acercándose en el tema de la identidad. Por ejemplo, un gobierno está introduciendo el Marco de Identidad Digital Confiable (TDIF). Este régimen especifica los requisitos mínimos que deben cumplir los proveedores de servicios de identidad para lograr y mantener la acreditación TDIF que permite a sus clientes acceder a los servicios digitales del gobierno.

El objetivo último es mantener una plataforma de fácil uso que facilite identidades digitales accesibles, seguras y privadas. Es importante destacar que los particulares podrán utilizar varios proveedores de servicios de identidad para mantener identidades digitales personales y empresariales distintas o combinadas.

El TDIF permite a las personas elegir qué identidad digital utilizar, para qué fines y durante cuánto tiempo, y tener garantías en torno a ella. Las administraciones públicas no pueden hacerlo solas, no es rentable. Además, es probable que en el entorno actual se confíe más en las empresas que en las administraciones públicas.

En algunos países, el telón de fondo se encuentra más fragmentado porque la actividad reguladora se desarrolla principalmente territorio por territorio. Pero eso no es más que la punta del iceberg, ya que la identidad digital devela un nuevo conjunto de consideraciones en torno a la aceptación. La gente viaja habitualmente a través de las fronteras para hacer negocios. ¿Sus credenciales digitales serán aceptadas por los funcionarios más allá de las fronteras territoriales? Pensando en el aspecto de la colaboración público-privada, si una persona tiene una identificación digital conectada a una institución financiera, así como una credencial digital emitida por el gobierno, ¿cuál de ellas utilizará en diferentes circunstancias?

Además, cuando las personas presentan una identificación digital emitida por el gobierno, ¿deberían estar obligadas a compartirla toda? Hay ciertos datos que las autoridades financieras, sanitarias o policiales quieren o necesitan ver. Aun así, las personas deben poder mantener un control total sobre lo que revelan sobre sí mismas. Por ejemplo, las personas deberían tener autonomía para revelar su nacionalidad, títulos universitarios, cualificaciones profesionales, etc., pero no deberían estar obligadas a ofrecer los datos personales subyacentes.

Otra cuestión fundamental para los profesionales de la seguridad es: ¿a quién pertenece el riesgo? Si la identidad digital de alguien se ve comprometida y se utiliza con fines fraudulentos, ¿es responsable el emisor o el titular? Dependiendo del uso previsto de una identidad digital, deberían imponerse a las empresas normas estrictas pero manejables.

Esta es una cuestión sobre la que debe haber normativas y reglamentos generalmente aceptadas para garantizar que los proveedores de identidades digitales puedan operar de forma colaborativa y segura.

Uno de los principios fundamentales del Reglamento General de Protección de Datos (RGPD) de la UE es que las personas deben dar su consentimiento para que las organizaciones utilicen sus datos personales en contextos específicos y para transacciones concretas.

Pero si una empresa quiere utilizar información personal identificable (IPI) para otro fin o venderla, debe volver a obtener el consentimiento. Ese imperativo básico debería ser una norma global.

Del mismo modo, la identidad digital de la UE -un monedero digital personal para ciudadanos y residentes de la UE- pronto permitirá a las personas identificarse o confirmar determinada información personal. Esta identidad electrónica podrá utilizarse tanto en línea como fuera de línea para servicios públicos y privados en toda la UE.[13]

La normativa global en materia de identidad es fragmentaria e incoherente. Hasta cierto punto, el mercado se ha insensibilizado ante el ritmo constante de las violaciones de datos. Los clientes particulares e institucionales deben estar atentos a los datos sensibles que revelan y a dónde los revelan. Los CISO y sus equipos deben mantener las demandas de los clientes sobre el uso responsable y el control de los datos como un factor central en el desarrollo de políticas y estrategias de gestión de identidades.

[13] Comisión Europea, "Digital Identity for all Europeans," 2021.

Acciones recomendadas

Mantener el enfoque de la identidad flexible para cumplir con el entorno normativo en evolución y garantizar que la arquitectura establecida pueda integrar las tecnologías emergentes en el proceso de seguridad mucho más rápido que los trayectos de dos, tres o cuatro años que vemos hoy en día.

Explorar sistemas de identidad más ágiles e interoperables para facilitar un ecosistema de identidad federada.

Considerar su papel, ahora y en el futuro, como emisor de identidades/credenciales, parte de confianza, proveedor de monederos digitales o las tres cosas a la vez en este ecosistema de identidad en evolución.

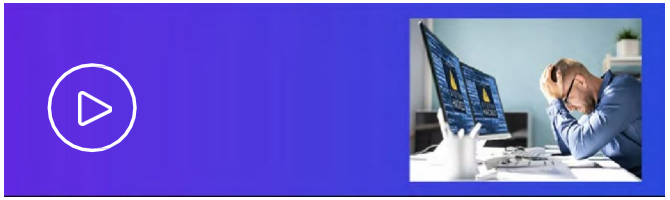
Conozca más

Los *Deepfakes* reescriben las reglas de la ciberseguridad

Las falsificaciones ya no son sólo una broma para el Día de los Inocentes. Están acercándose a las Juntas Directivas de su jurisdicción, y tienen el potencial de desestabilizar sus negocios.

El contenido falso se está convirtiendo en un problema real

La disponibilidad generalizada de sofisticadas tecnologías informáticas y de IA permite que prácticamente cualquiera pueda crear contenidos falsos de gran realismo.



Cómo la gestión de identidades y accesos puede mejorar la resistencia y el cumplimiento de la normativa DORA

Con las nuevas normativas de la UE exigiendo vigilancia en torno a la seguridad, un marco sólido de identidad y acceso es una herramienta vital en el kit.

Consideración 8

Alinear la ciberseguridad con la resiliencia organizacional

Durante un incidente cibernético, las organizaciones necesitan una respuesta que se mida en minutos y horas, no en días y semanas. En el entorno volátil actual, la resiliencia se ha convertido en un tema común para las organizaciones de sectores de infraestructuras críticas como la energía, las comunicaciones y el transporte, con la gerencia centrada en la recuperación si fallan los controles preventivos. La resistencia debe alinearse perfectamente con la ciberseguridad, haciendo hincapié en la protección, la detección y la respuesta y recuperación rápidas. La resistencia cibernética es vital para mantener las capacidades operativas de las empresas, salvaguardar la confianza de los clientes y reducir el impacto de futuros ataques. Estas disciplinas deben trabajar conjuntamente para ayudar a las organizaciones a gestionar el riesgo.

> Resiliencia significa estar mejor equipado para gestionar incidentes de forma rápida, exhaustiva y con menor impacto en el negocio. Esto no significa que nunca vaya a producirse otro incidente. Los CISO no pueden controlar las amenazas externas, pero sí la preparación de la organización.

Dani Michaux
Líder de Ciberseguridad
y Socia de la Región EMA
KPMG en Irlanda

Recuperar la confianza es clave después de un incidente

Cuando se produce una filtración de datos o un ataque de *ransomware*, la confianza es el primer activo que se ve afectado. Y la confianza es un activo corporativo en su totalidad. El grado de preparación de las organizaciones y la rapidez con la que pueden responder y recuperarse son factores determinantes para restablecer la confianza de los clientes y, en el caso de las empresas públicas, de los inversionistas.

Cuando las organizaciones se comprometen a ganarse -y volver a ganarse- la confianza de estas partes interesadas fundamentales, se sitúan firmemente en la senda de la resiliencia operativa. En algunos casos, la recuperación de la confianza pasa por una rápida recuperación técnica; en otros, por identificar formas alternativas de prestar servicios. En todos los casos, se trata de identificar a las partes interesadas vulnerables o afectadas, atender rápidamente sus necesidades y minimizar las interrupciones.

Los reguladores de todas las regiones están haciendo mayor hincapié en la resiliencia y la confianza. Por ejemplo, las normas adoptadas en 2021 por la Autoridad de Conducta Financiera del Reino Unido tienen como propósito garantizar que los servicios empresariales importantes en el sector de los servicios financieros del Reino Unido funcionen con suficiente resiliencia en caso de interrupciones operativas.

Se exige a las empresas que demuestren que adoptan un enfoque de resiliencia por diseño. Este marco se basa en la noción de evitar "daños de gran alcance a los consumidores y riesgos para la integridad del mercado" como resultado de un evento cibernético.[14]

Misión crítica: Centrarse en lo importante con una planificación anticipada

Cada organización es única en lo que hace y en cómo lo hace, pero desde el punto de vista de la seguridad, es universalmente instructivo llevar a cabo ejercicios de simulación estructurados y basados en escenarios antes de un incidente cibernético para asegurarse de que las personas, los procesos y la tecnología están alineados.

La planificación de escenarios no debe ser simplemente una casilla que se marca. Estos ejercicios revelan las opciones estratégicas en torno a cómo las organizaciones se enfrentan a un evento disruptor importante como un ataque de *ransomware* y crean confianza en que el liderazgo está preparado para coordinar los esfuerzos de respuesta y gestionar y, en última instancia, reducir el impacto en los clientes. También es imperativo que las organizaciones determinen de antemano qué procesos de negocio son realmente críticos para la misión y necesitan volver a estar en línea lo antes posible.

> **La evaluación continua de la ciber-resiliencia de la organización como pilar fundamental de su preparación general y la realización de ejercicios de priorización es fundamental para mantener un plan de ciberseguridad que sea adecuado tanto para el propósito como para el momento. Proporciona una hoja de ruta de respuesta.**
>
> **Jason Hawrard-Gau**
> Líder Global de Servicios de Recuperación cibernéticos
> KPMG International y Principal KPMG en EEUU

La resiliencia cibernética, la capacidad de adaptarse y enfrentar un incidente cibernético, difiere de la continuidad del negocio, los procedimientos que sigue una organización para operar durante un incidente. La resiliencia es estratégica, mientras que la continuidad está orientada a los procesos. En ese sentido, es mucho menos estresante llevar a cabo un ejercicio de resistencia antes de una situación de recuperación que en un punto medio, cuando múltiples áreas de negocio pueden entrar en pánico.

La evaluación continua de la ciber-resiliencia de la organización como pilar fundamental de su preparación general y la realización de ejercicios de priorización es fundamental para mantener un plan de ciberseguridad que sea adecuado tanto para el propósito como para el momento. Proporciona una hoja de ruta de respuesta y recuperación.

Cada día, los actores de amenazas persistentes avanzadas aprovechan diferentes vectores de ataque de nuevas formas. Esta evolución es una realidad que los CISO deben tener en cuenta. Disponer de un plan de resistencia escrito y verificado como trampolín para una acción tangible es mucho más eficaz que una lluvia de ideas durante un ataque.

Evitar la complacencia en un panorama de amenazas cambiante

La seguridad básica de las organizaciones está mejorando. Al mismo tiempo, el panorama empresarial y de la cadena de suministro está evolucionando, con una mayor dependencia de una red de proveedores de TI, software y otros servicios, y organizaciones que experimentan con nuevas tecnologías como la IA, la Web 3.0 y los productos inteligentes.

En respuesta, los atacantes -organizados/apoyados por el Estado y actores en solitario- se están volviendo más sofisticados, explorando nuevos vectores y manipulando la realidad a través de la suplantación de identidades y *deepfakes*. Los ataques actuales han pasado a incluir ataques a la cadena de suministro y *ransomware* de doble o triple extorsión respaldado por un complejo ecosistema de "delincuencia como servicio". [15]

[14] Autoridad de Conducta Financiera, Declaración de Política PS21/3, "Building operational resilience," marzo 2021.

[15] KPMG International, "Maintaining cyber vigilance and staying resilient," 2023.

En resumen, las organizaciones deben adoptar un enfoque dinámico de la resistencia. No pueden dormirse en los laureles, porque no sólo cambian las amenazas, sino también la forma en que los delincuentes intentan perturbar los procesos internos y las cadenas de suministro.

Las organizaciones deben mejorar y adaptarse continuamente. Resiliencia significa estar mejor equipado para hacer frente a un incidente de forma rápida, exhaustiva y con un impacto mínimo en el negocio.

Esto no significa que nunca vaya a producirse otro incidente. Los CISO no pueden controlar las amenazas externas, pero sí la preparación de la organización.

Las inversiones de tiempo, personal y presupuesto no deben centrarse únicamente en evitar incidentes, sino en cultivar un estado duradero de resiliencia que se convierta en un componente integral e integrado del plan general de ciberseguridad.

Existe una carrera armamentista continua entre las organizaciones y los malos actores, y estos últimos evolucionan constantemente e innovan más rápido, porque es en lo único que piensan. Si los CISO comprenden y gestionan la deriva de la seguridad de la organización, pueden reducir la capacidad de los atacantes para identificar y explotar las vulnerabilidades.

A medida que las organizaciones navegan por el cambiante y volátil panorama actual de la ciberseguridad, la resiliencia no debe verse como una serie de proyectos puntuales o intermitentes. Por el contrario, debe ser una estrategia adaptable que complemente la agenda de ciberseguridad de la organización, proteja los intereses del cliente, se alinee con los objetivos de la empresa y se centre en ofrecer valor a largo plazo.

Acciones recomendadas

Evaluar cómo la organización puede responder mejor y más rápido si vuelve a ser atacada la próxima semana y el próximo mes/año para identificar "ganancias rápidas", como agilizar los pagos, garantizar la liquidez, mejorar la comunicación y aumentar la velocidad de respuesta.

Fomentar comportamientos en toda la organización y la alineación cultural para dar prioridad a lo que realmente importa a la organización en términos de datos, servicios e infraestructura.

Actualizar periódicamente los planes y guías de actuación para adaptarlos a la evolución del panorama de amenazas y a los cambios en la dependencia de las TI y la cadena de suministro.

Conozca más

Mantener la ciber-vigilancia y la capacidad de recuperación

Cómo recuperarse de un ciberataque, reconstruir eficazmente y evitar la complacencia.

Resiliencia operativa cibernética y digital

Centrarse en la resiliencia estratégica.

Mercado intermedio: un enfoque holístico para impulsar la resiliencia cibernética

Un mundo más conectado ha aumentado el riesgo y las expectativas. En respuesta, el mercado medio puede aplicar estrategias holísticas de ciberseguridad.

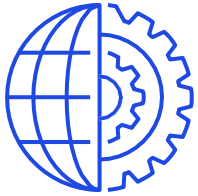
Ciber-estrategias para 2024

¿Qué medidas pueden tomar los CISO y las líneas de negocio más amplias en el próximo año para ayudar a garantizar que la seguridad sea el hilo conductor de la organización? A continuación, se ofrece una breve lista de recomendaciones que los CISO deben tener en cuenta a la hora de acelerar los tiempos de recuperación, reducir el impacto de los incidentes en el equipo de trabajo, clientes y terceras partes, y garantizar que sus planes de seguridad faciliten -en lugar de exponer- el negocio.

Personas

- Póngase en contacto con el equipo de ESG de su organización para determinar si consideran la ciberseguridad un aspecto clave de sus funciones. De no ser así, haga esfuerzos por concientizar la forma y las razones por la cuales es importante para las tres áreas de ESG.
- Aporte una nueva perspectiva a la junta directiva sobre lo que podrían ser agentes disruptores del negocio y lo que debería hacerse para gestionar esos riesgos sin afectar a las operaciones ni a la experiencia del cliente.
- Fomente comportamientos en toda la organización y la alineación cultural para dar prioridad a lo que realmente importa a la organización en términos de datos, servicios e infraestructura.
- Determine cómo y dónde integrar ciertas tareas de seguridad dentro de la empresa frente a subcontratarlas a un proveedor de servicios externo y supervise esas tareas para garantizar que se llevan a cabo correctamente.
- Use la practicidad. Un sistema de ciberseguridad eficaz no consiste tanto en conseguir que las terceras partes hagan las cosas de forma diferente como en replantear la conversación en toda la empresa para inspirar a otras áreas de la organización a que incorporen la seguridad a lo que ya practican.

Procesos

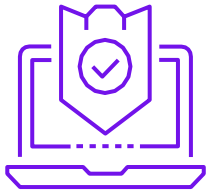


- Dirija el equipo cibernético como una empresa, lo que significa que debe renunciar a cierto grado de control sobre lo que hacen otras partes de la organización desde el punto de vista de la seguridad.
- Defina su visión y estrategia iniciales para la automatización. Considere sus objetivos de seguridad a corto y largo plazo, garantizando la forma en que dichos objetivos se alinean con las prioridades empresariales de la organización y determine el tipo de protecciones que requieren esos objetivos compartidos.
- Aumente la transparencia para generar confianza en las cadenas de suministro globales; en lugar de tratar las relaciones con proveedores terceros, cuartos e incluso quintos únicamente como transaccionales y contractuales (que lo son), acérquese a ellos como una extensión de su ecosistema.
- Actualice periódicamente los planes y guías de actuación para adaptarlos a la evolución del panorama de amenazas y a los cambios en la dependencia de las TI y la cadena de suministro.
- Adopte un enfoque basado en el riesgo para evaluar los procesos de terceros en lugar de un enfoque general para los diferentes proveedores que prestan diversos servicios.
- Fomente el intercambio de información e inteligencia tanto dentro de su organización como con terceros de confianza.
- Evalúe cómo la organización puede responder mejor y más rápido si se ve atacada de nuevo la semana que viene y el mes/año que viene para identificar "victorias rápidas", como agilizar los pagos, garantizar la liquidez, mejorar la comunicación y aumentar la velocidad de respuesta.

Datos y tecnología

- Identifique los datos que son accesibles para la organización de forma centralizada y defina un plan automatizado de supervisión de controles continuos para impulsar la eficiencia en las tres líneas de defensa.
- Conozca la ubicación de los datos críticos -estructurados y no estructurados- en toda la organización, así como dónde se comparten con terceras partes.
- Garantizar que la finalidad de los algoritmos de IA, ya sean desarrollados interna o externamente, esté claramente definida y documentada, y que los datos de formación sean pertinentes, adecuados para el objetivo empresarial y tengan un consentimiento seguro.
- Aprovechar la automatización inteligente para obtener una mayor visibilidad de los cambiantes perfiles de riesgo de los proveedores y crear un programa de terceros sostenible y escalable con visión futuro.
- Determinar qué herramientas crear en lugar de adquirir y comprender cómo se automatiza la cadena de suministros para reforzar la confianza entre las organizaciones y aprovechar ese aprendizaje cuando proceda.
- Explorar sistemas de identidad más ágiles e interoperables para facilitar un ecosistema federado de identidad.
- Considere su papel, ahora y en el futuro, como emisor de identidades/credenciales, parte de confianza, proveedor de monederos digitales o los tres en este ecosistema de identidad en evolución.

Aspecto reglamentario



- Optimice su estrategia de inteligencia reguladora global en torno a la cibernética en general y ESG y la privacidad en particular para garantizar el cumplimiento y la presentación de informes a tiempo; realice un seguimiento y manténgase familiarizado con las regulaciones cada vez mayores y sus efectos en sus esfuerzos cibernéticos.
- Alinee su marco de IA con las normas actuales y desarrolle una sólida gobernanza de la IA alineando las prioridades de los distintos líderes empresariales de la organización y obteniendo el apoyo interfuncional de aquellos con un interés personal en el éxito de la IA.
- Familiarizarse con las estipulaciones de la Ley de IA de la UE y la Orden Ejecutiva emitida por el gobierno de los Estados Unidos sobre Inteligencia Artificial Segura y de Confianza.
- Conozca el panorama normativo mundial y, en concreto, las normas pertinentes a nivel jurisdiccional.
- Mantenga su enfoque de identidad flexible para cumplir con el entorno normativo en evolución y asegúrese de que su arquitectura pueda integrar las tecnologías emergentes en el proceso de seguridad mucho más rápido que los procesos de dos, tres o cuatro años que vemos hoy en día.

Cómo KPMG puede ayudar a su organización

Las firmas de KPMG tienen experiencia en todo el proceso, que abarca desde la sala de juntas hasta el centro de datos. Además de evaluar su ciberseguridad y alinearla con sus prioridades de negocio, el equipo de KPMG puede ayudarle a desarrollar soluciones digitales avanzadas, asesorarle en la implementación y supervisión de los riesgos en curso y ayudarle a responder eficazmente a los incidentes cibernéticos. No importa en qué punto de su viaje hacia la ciberseguridad se encuentre, las firmas de KPMG pueden ayudarle a llegar a su destino.

Como proveedores e implementadores líderes de ciberseguridad, KPMG sabe cómo aplicar las prácticas de seguridad más avanzadas y crear otras nuevas que se ajusten a su propósito. Su enfoque progresivo de la ciberseguridad también incluye cómo pueden prestar servicios, por lo que puede esperar trabajar con personas que entienden su negocio y su tecnología.

Si bien está entrando en un nuevo mercado, lanzando productos y servicios, o interactuando con los clientes de una nueva forma, el equipo de KPMG puede ayudarle a anticiparse al futuro y a moverse de forma más eficiente con una tecnología segura y fiable. Esto se debea que puede aportar una combinación de experiencia tecnológica, amplios conocimientos empresariales y profesionales creativos apasionados por ayudarle a proteger y generar la confianza de las partes interesadas.

KPMG. Marca la Diferencia
Para mayor información, visite kpmg.com/cybersecurity

Conozca a los autores

Akhilesh Tuteja
Líder Global de Ciberseguridad KPMG International
Socio, KPMG en India

Además de liderar la práctica de Ciberseguridad Global, Akhilesh dirige las prácticas de Consultoría en Tecnologías de la Información y Consultoría de Riesgos para KPMG en India. Le apasiona cómo los avances en tecnología de la información pueden ayudar a las empresas a impulsar procesos inteligentes y resultados eficaces. Akhilesh ha asesorado a muchos clientes sobre ciberseguridad, estrategia de TI y selección de tecnología, y les ha ayudado a obtener los beneficios empresariales de la tecnología. También es experto en el área de la psicología del comportamiento y le entusiasma abordar los problemas de riesgo informático de forma holística, principalmente mediante la aplicación de análisis del comportamiento de los usuarios.

Kyle Kappel
Líder de la Red de Servicios de Ciberseguridad
Director, KPMG en EEUU

Como líder de la práctica de Ciberseguridad de KPMG en EE.UU., Kyle cuenta con más de 20 años de experiencia en el campo de los sistemas de información y una formación diversa en ciberseguridad, privacidad de datos, cumplimiento normativo, gestión de riesgos y cuestiones tecnológicas en general. Aunque posee grandes conocimientos técnicos, Kyle utiliza un enfoque centrado en el negocio para resolver problemas tecnológicos abordando las causas de raíz en lugar de los síntomas técnicos. Es asesor de confianza de numerosas organizaciones y trabaja con altos ejecutivos, incluidas juntas directivas, comités de auditoría, directores de información, directores financieros, directores de operaciones, directores de tecnología y directores de seguridad de la información.

Dani Michaux
Líder de Ciberseguridad de la Región EMA
Socia, KPMG en Irlanda

En sus más de 22 años en ciberseguridad, Dani ha trabajado con agencias gubernamentales en estrategias nacionales de ciberseguridad y con organismos reguladores internacionales sobre riesgos cibernéticos. Tiene una amplia experiencia trabajando con clientes para mejorar la comprensión de las juntas directivas en materia de ciberseguridad. Ha creado y dirigido equipos de ciberseguridad como CISO en empresas de telecomunicaciones y energía en Asia. Dani lucha por la inclusión y la diversidad y por la participación de las mujeres en la informática y la ciberseguridad. Previamente, dirigió las prácticas de Ciberseguridad y Riesgos Tecnológicos Emergentes para KPMG en Malasia y la región ASPAC y también dirigió el grupo de trabajo global de IoT de KPMG.

Matt O'Keefe
Líder de Ciberseguridad de la Región ASPAC
Socio, KPMG en Australia

Matt es responsable de impulsar la estrategia cibernética de KPMG dentro de las 12 firmas miembro de KPMG en Asia Pacífico. Cuenta con más de 25 años de experiencia en las áreas de tecnología, finanzas, aseguramiento y asesoramiento, centrándose en clientes del sector de servicios financieros. Matt está especializado en asesoramiento tecnológico, en particular en gestión de pensiones y patrimonios, banca y seguros, y presta una amplia gama de servicios en materia de gobernanza y riesgos tecnológicos, ciberseguridad, gestión de proyectos, estrategia y rendimiento de TI. Está particularmente interesado en el uso de la tecnología para avanzar en los objetivos de la organización, facilitando las estrategias digitales y los modelos operativos de los clientes, y protegiendo los datos, los activos y los sistemas.

Prasanna Govindankutty
Líder de Ciberseguridad de las Américas y Director
KPMG en EEUU

Prasanna es director de los servicios de ciberseguridad de KPMG en Estados Unidos. Es el líder de Americas Cyber con 20 años de experiencia especializada en ciberseguridad y transformación de riesgos tecnológicos. En el pasado, dirigió la solución Global and US Powered Cyber para KPMG. Con amplios conocimientos de las soluciones tecnológicas líderes del mercado para las funciones cibernéticas y de gobierno, riesgo y cumplimiento (GRC), ayuda a los clientes en su transformación integrada. Prasanna aprovecha su amplia experiencia en la transformación basada en la tecnología para ayudar a sus clientes de los sectores de la energía, medios de comunicación y telecomunicaciones.

Reconocimientos

Este informe no habría sido posible sin las invaluables contribuciones de planificación, análisis, redacción y producción de nuestros colegas alrededor del mundo.

Nuestro equipo global de consideraciones cibernéticas:

John Hodson
Billy Lawrence
Leonidas Lykos
Michael Thayer
Jessica Booth

Colaboradores de las firmas de KPMG:

Katie Boswell
KPMG en EEUU
katieboswell@kpmg.com

Pratiksha Doshi
KPMG en India
pratikshadoshi@kpmg.com

Danny Flint
KPMG en Australia
dflint@kpmg.com.au

Brian Geffert KPMG en EEUU
bgeffert@kpmg.com

Jason Haward-Grau
Director,KPMG en EEUU
jhawardgrau@kpmg.com

Elizabeth Huthman
KPMG en el Reino Unido
elizabeth.huthman@kpmg.co.uk

Sylvia Klasovec Kingsmill
KPMG en Canadá
skingsmill@kpmg.ca

Mika Laaksonen
KPMG en Finlandia
mika.laaksonen@kpmg.fi

Angela Leggett KPMG en EEUU
aleggett@kpmg.com

Orson Lucas KPMG en EEUU
olucas@kpmg.com

Dani Michaux
KPMG en Ireland
dani.michaux@kpmg.ie

Mitushi Pitti
KPMG en EEUU
mitushipitti@kpmg.com

Caroline Rivett
KPMG en el Reino Unido
caroline.rivett@kpmg.co.uk

Henry Shek
KPMG en China
henry.shek@kpmg.com

Akhilesh Tuteja
KPMG en India
atuteja@kpmg.com

Marko Vogel KPMG en Alemania
mvogel@kpmg.com

Jim Wilhelm
KPMG en EEUU
jameswilhelm@kpmg.com

Contactos

Mónica Barrios

Socia Líder de Advisory
KPMG en Venezuela
mbarrios@kpmg.com

Carolina Pereda

Directora de Ciberseguridad & CIO Advisory
KPMG en Venezuela
cpereda@kpmg.com

Caracas
Avenida Francisco de Miranda, Torre KPMG, Chacao, Caracas, estado Miranda, Venezuela.
Telfs.: 58 (212) 277.78.11
Fax: 58 (212) 263.63.50

Barquisimeto
Av. Los Leones, Torre Bel, Piso 13, Oficina13-2, Barquisimeto, estado Lara, Venezuela.
Contacto: kpmgvenezuela@kpmg.com

Maracaibo
Contacto: kpmgvenezuela@kpmg.com

Puerto Ordaz
Contacto: kpmgvenezuela@kpmg.com

Puerto La Cruz
Centro Comercial Plaza Mayor, edificio 6, nivel 2, Ofic. 6C-254
Complejo Turístico El Morro, municipio Urbaneja, Puerto La Cruz, estado Anzoátegui, Venezuela.
Telfs.: 58 (281) 282.08.33 / 01.33
Fax: 58 (281) 282.25.50

Valencia
Centro Comercial Concepto La Viña, piso 5, oficinas números 18 a 26; esquina entre Av. 104 La Victoria y calle 149 Uslar, urbanización La Viña, parroquia San José, Valencia 2001, estado Carabobo, Venezuela.
Contacto: kpmgvenezuela@kpmg.com

kpmg.com/ve

KPMG en Venezuela
@KPMG_VE
KPMG Venezuela
kpmgvenezuela@kpmg.com