Boletin Ciberseguridad
Enero 2024

Las innovaciones tecnológicas requieren pragmatismo estratégico.

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

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.

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

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

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.

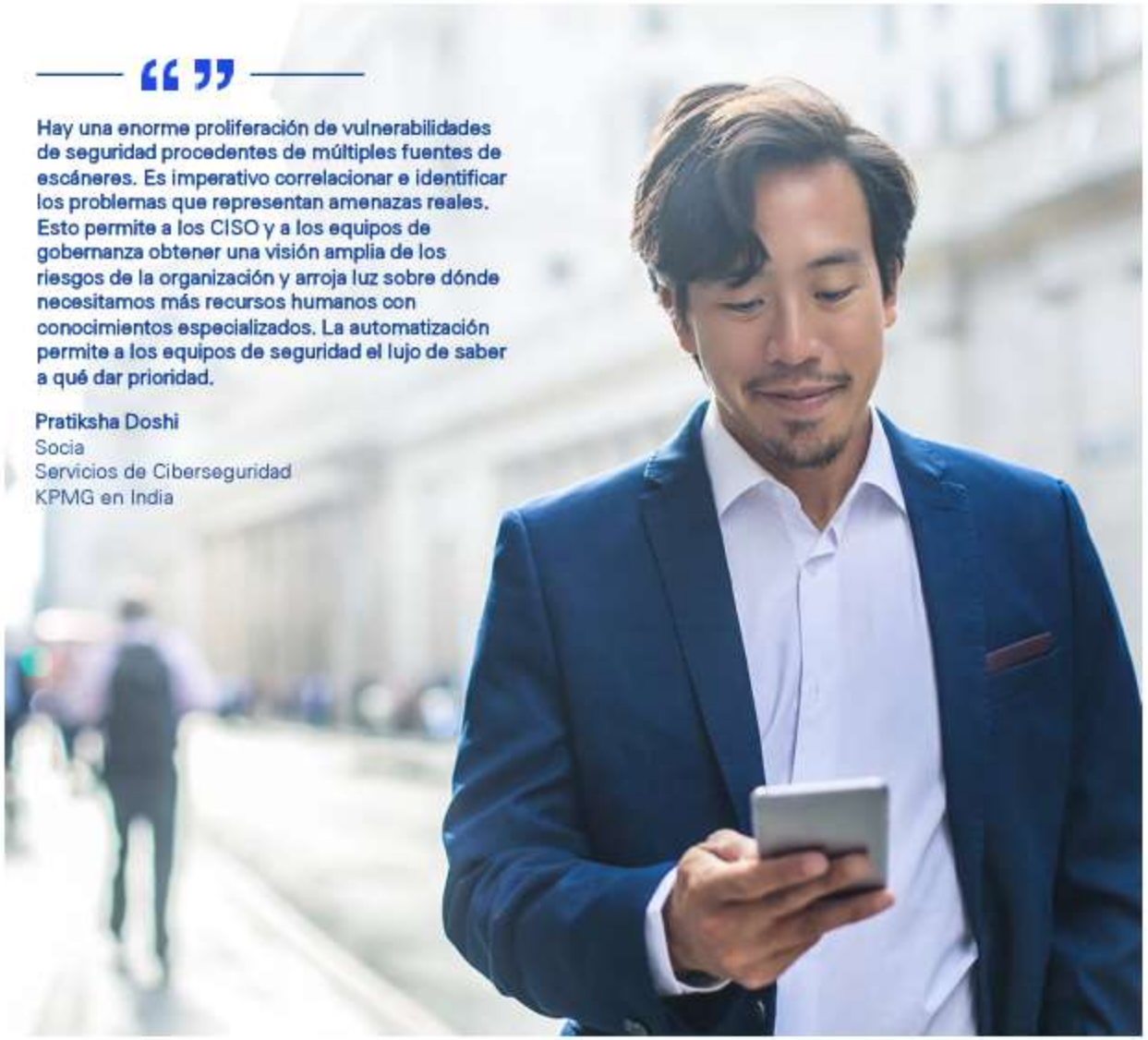
> Los datos son el eje fundamental de la seguridad en general y de la privacidad en particular. El sector necesita que los organismos gubernamentales de todo el mundo armonicen sus legislaciones, ya que la existencia de normativas dispares en las que unos países son más estrictos que otros desincentiva 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

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