# Consideraciones en ciberseguridad 2024

Las innovaciones tecnológicas requieren pragmatismo estratégico

## Resumen ejecutivo

kpmg.com

Febrero de 2024

# Resumen ejecutivo

A medida que avanza 2024, los líderes de las organizaciones se enfrentan a muchos desafíos, como mantener el crecimiento, navegar por las tecnologías emergentes y adquirir y retener talento. *Por otro lado, los directores de seguridad de la información* (CISO) están estableciéndose cada vez más como socios proactivos en la gestión de las necesidades comerciales en curso, en lugar de ser llamados solo para brindar alivio a la organización en tiempos de crisis.

El informe ***"Consideraciones en ciberseguridad 2024"*** explora ocho consideraciones que los CISO deben priorizar en 2024. Asimismo, ofrece pasos prácticos que las organizaciones pueden adoptar para acelerar la recuperación, reducir el impacto de los incidentes en empleados, clientes y socios, y garantizar que sus planes de seguridad fortalezcan el negocio en lugar de exponerlo a riesgos.

# Consideraciones sobre seguridad cibernética para 2024

01

## Cumplir con las expectativas de los clientes y generar confianza

Los consumidores, los empleados y los proveedores -todas las *partes interesadas*-, esperan que las empresas persigan el crecimiento y las ganancias. Sin embargo, también se espera que las organizaciones operen de manera socialmente responsable. Las organizaciones deben prestar atención a este llamado y fortalecer la conexión entre la seguridad, la privacidad y los factores ambientales, sociales y de gobernanza (ESG). Esta conexión está siendo cada vez más reconocida en todo el ecosistema empresarial, especialmente por los servicios de calificación ESG, que buscan una mayor transparencia en la medición y comparación de las organizaciones.

02

## Incorporar la ciberseguridad y la privacidad de forma permanente

La seguridad, desde el CISO hasta todo su equipo, desempeña un papel muy diferente hoy en día. La ciberseguridad se está integrando en los procesos empresariales básicos. Esta realidad se refleja en un cambio que aleja la centralización de la ciberseguridad en el rol del CISO hacia un modelo federado, en el que el CISO actúa como un director de orquesta, estableciendo el marco, evaluando riesgos y apoyando en la implementación.

La seguridad es una parte integral de todas las áreas de la organización, desde el *front* office hasta el *back office*, y muchos líderes ahora reconocen el valor de integrar una mentalidad de seguridad en sus diferentes culturas y procesos comerciales.

03

## Navegar a través de fronteras globales muy difusas

Las organizaciones globales operan en un espacio regulatorio cibernético y de privacidad cada vez más complejo. Los intereses nacionales están en juego, lo que lleva al establecimiento de requisitos regulatorios sobre la soberanía de la información, la seguridad en la cadena de suministro, la transparencia en el cumplimiento de los controles cibernéticos, la notificación de incidentes y, por supuesto, la privacidad.

Las organizaciones necesitan calibrar sus reportes normativos para un mundo sin fronteras, así como mantener controles de seguridad que puedan personalizarse de acuerdo con los requisitos locales. También deben estar preparados para responder rápidamente a los cambios geopolíticos y a los diversos requisitos con sanciones.

04

## Modernizar la seguridad de la cadena de suministro

El enfoque de muchas organizaciones en materia de seguridad de terceros y de la cadena de suministro no está alineado con el complejo e interdependiente ecosistema actual de organizaciones asociadas. Los modelos tradicionales se han construido en torno a la premisa de que los terceros prestan servicios con base en la transacción.

Esta visión no refleja la intrincada red actual de API y procesos vinculados por un complejo conjunto de softwares como servicio (SaaS). Se alienta a las organizaciones a establecer asociaciones estratégicas más sólidas con los proveedores para monitorear y administrar continuamente los perfiles de riesgo en constante evolución de estos proveedores para fortalecer la resiliencia operativa.

# Consideraciones sobre seguridad cibernética para 2024

05

## Liberar cuidadosamente el potencial de la IA

Con una planificación y ejecución cuidadosas, la inteligencia artificial (IA) transformará cómo, cuándo y quién realiza el trabajo. Actualmente, todo lo que se habla gira en torno a la IA generativa, pero muchas otras ramas de la IA, desde la robótica hasta el aprendizaje automático, continúan transformando los negocios.

Calibrar la seguridad, la privacidad y las implicancias éticas inherentes a estas tecnologías es un desafío, y las organizaciones buscan establecer marcos que provean tanto la gestión de riesgos como la gobernanza al implementar la IA.

06

## Refuerce la seguridad con la automatización

Las empresas están migrando cada vez más los sistemas a la nube, el volumen de datos que necesitan protección está aumentando rápidamente y cada vez más personas trabajan de forma remota 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 eventos de clasificación para que los CISO administren. Hay mucho ruido en los centros de operaciones de seguridad (SOC) y no hay suficientes paneles de monitoreo o personas para manejar este volumen.

¿Cómo pueden los CISO seguir detectando amenaza tras amenaza y sentir que no se están perdiendo algo? Necesitan recopilar, correlacionar y escalar las señales que requieren una respuesta, y debe hacerse rápidamente. Y la única forma es a través de la automatización.

07

## Hacer que la identidad sea individual, 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, también lo hacen los métodos de autenticación. 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) se diseñaron originalmente para gestionar las identidades digitales y el acceso de los usuarios para organizaciones individuales. Muchos de ellos se están reconceptualizando para que puedan cubrir un nivel de resiliencia adecuado para entornos informáticos federados, privados, públicos o *multi-cloud*. Esto eliminará la necesidad de que las personas aseguren el proceso exhaustivo, lento e intrusivo de verificación de identidad cada vez que interactúan con una nueva institución, ya sea como cliente o empleado.

08

## Alinear la ciberseguridad con la resiliencia organizacional

Durante un incidente cibernético, las organizaciones necesitan una respuesta medida 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 en sectores de infraestructura crítica como la energía, la comunicación y el transporte, con ejecutivos centrados en la recuperación en caso de que fallen los controles preventivos.

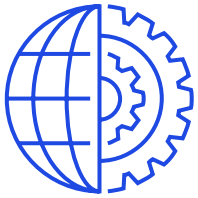
La resiliencia debe buscar una integración perfecta con la ciberseguridad, haciendo hincapié en la protección, la detección, la respuesta rápida y la recuperación. La resiliencia cibernética es vital para mantener las competencias operativas de la empresa, proteger la confianza de los clientes y reducir el impacto de futuros ataques. Estas disciplinas deben trabajar juntas para ayudar a las organizaciones a gestionar el riesgo.

# Acciones clave que las organizaciones deben considerar para 2024

## Gente

- Conéctese con el equipo de ESG de su organización para determinar si el equipo considera que la ciberseguridad es un aspecto clave de su competencia. Si no es así, trabaje para crear conciencia sobre "cómo" y "por qué" esto es importante para las tres áreas de ESG.
- Aporte una nueva perspectiva a la junta sobre lo que podría causar interrupciones en el negocio y lo que se debe hacer para gestionar esos riesgos sin afectar las operaciones y la experiencia del cliente.
- Impulse un comportamiento organizacional amplio y la alineación cultural para priorizar lo que realmente importa en términos de datos, servicios e infraestructura.
- Los equipos de seguridad deben determinar cómo y dónde incorporar ciertas tareas de seguridad dentro de la empresa, en lugar de subcontratarlas a un proveedor de servicios, supervisándolas para garantizar que se realicen correctamente.
- Sé práctico. La ciberseguridad efectiva no se trata tanto de asegurarse de que los socios comerciales hagan las cosas de manera diferente; se trata mucho más de replantear las conversaciones en toda la empresa para inspirar a otras áreas de la organización a incorporar la seguridad en lo que ya se está haciendo.

## Proceso

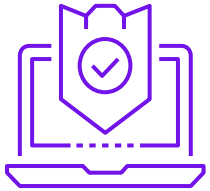


- Defina su visión y estrategia iniciales para la automatización, alineando los objetivos de seguridad a corto y largo plazo con las prioridades empresariales de su organización.
- Genere confianza en las cadenas de suministro globales mejorando la transparencia y tratando a los proveedores como una extensión de su ecosistema.
- Adopte un enfoque basado en el riesgo para evaluar los procesos de terceros, en lugar de un enfoque único para diferentes proveedores que brindan diversos servicios.
- Fomente el *crowdsourcing* y el intercambio de inteligencia, tanto dentro de su organización como con terceros de confianza.
- Evalúe cómo la organización puede responder mejor y más rápido a futuros ataques para identificar "ganancias rápidas", como acelerar los pagos, garantizar la liquidez, mejorar la comunicación y aumentar la velocidad de respuesta.

# Datos y tecnología

- Identifique los datos a los que tiene acceso la organización de forma centralizada y defina un plan automatizado para la supervisión continua de los controles con el fin de impulsar la eficiencia en las tres líneas de defensa.
- Sepa dónde se encuentran los datos críticos en toda la organización, así como dónde se comparten con terceros.
- Asegúrese de que el propósito de los algoritmos de IA, ya sea desarrollado interna o externamente, esté claramente definido y documentado, y que los datos de entrenamiento sean relevantes, apropiados para el objetivo comercial y garanticen un consentimiento seguro.
- Aproveche la automatización inteligente para obtener una mayor visibilidad de los perfiles de riesgo cambiantes de los proveedores y establecer un programa de terceros escalable y con visión de futuro.
- Determine qué herramientas desarrollar en *lugar* de adquirir, y comprenda cómo los socios de la cadena de suministro están automatizando para fortalecer la confianza.
- Explore sistemas de identidad más ágiles e interoperables para facilitar un ecosistema de identidad federado. Considere su rol como emisor de identidad/credencial, parte de confianza y/o proveedor de billetera digital.

# Regulación



- Mejore su inteligencia regulatoria global en torno a la ciberseguridad en general, y ESG y privacidad en particular, para garantizar el cumplimiento y la presentación de informes oportunos. Manténgase al tanto y familiarícese con las regulaciones cada vez más completas y sus efectos en sus esfuerzos de ciberseguridad.
- Alinee su marco de IA con las regulaciones actuales y desarrolle una sólida gobernanza de la IA alineando las prioridades de los diversos líderes de la organización y obteniendo el apoyo multidisciplinario de aquellos que tienen un interés personal en el éxito de la IA.
- Familiarícese con las disposiciones de la Ley de IA de la UE (Ley de Inteligencia Artificial de la Unión Europea) y la Orden Ejecutiva de la administración Biden sobre Inteligencia Artificial Segura, Protegida y Confiable, vigente en los Estados Unidos.
- Mantener una comprensión del panorama regulatorio global, especialmente cuando se trata de comprender las reglas relevantes a nivel detallado y jurisdiccional.
- Mantenga un enfoque flexible de la identidad 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 en dos, tres o cuatro años como vemos hoy en día.

# Hable con nuestro equipo

**Leandro Augusto Marco Antonio**
**Socio Líder de Seguridad Cibernética y Privacidad**
KPMG en Brasil y América del Sur
lantonio@kpmg.com.br

Ciertos aspectos de algunos de los servicios descritos en este material no están autorizados para clientes de auditoría de KPMG y susfiliales o entidades relacionadas.

**kpmg.com**