KPMG

Boardroom Questions

Ciberseguridad: consideraciones críticas para el Consejo

BOARD LEADERSHIP CENTER MEXICO

Dada la creciente velocidad y sofisticación de las amenazas informáticas, la ciberseguridad continúa ganando relevancia, y el Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) se convierte en una función crucial para las compañías.

En este sentido, las prácticas de seguridad y estrategias de las organizaciones para reaccionar ante posibles ataques deben estar alineadas con los procesos del SOC, ya que su experiencia en la materia y su continua actualización de recursos, soluciones y tecnologías como la inteligencia artificial (IA), juegan un papel clave en la ciberseguridad y brindan un panorama robusto para la toma de decisiones de los integrantes del Consejo.

¿Qué es y por qué es un tema crítico para el Consejo y Comité de Auditoría?

El equipo del SOC integra personas, procesos y tecnología para identificar, monitorear y responder de manera oportuna y coordinada ante las ciberamenazas y mitigar su impacto.

Al respecto, no cabe duda de que toda entidad que utiliza internet tiene, inevitablemente, una superficie de ataque que puede ser explotada por los ciberdelincuentes, por lo que resulta beneficioso contar con un Oficial de Seguridad de la Información (CISO, por sus siglas en inglés) que tenga los recursos necesarios de preparación para hacer frente a potenciales amenazas.

Sin embargo, ninguna estrategia de defensa es infalible en materia de ciberseguridad, ya que, en el mejor panorama, una repuesta inadecuada frente a un incidente de ciberseguridad puede resultar en consecuencias menores y aisladas, pero, por lo general, suelen ser más graves.

Impactos, beneficios e implicaciones para el Consejo

Sin un SOC, el CISO depende de la efectividad de los controles y herramientas implementadas por la compañía para reaccionar ante un ataque, lo que puede dificultar la toma de decisiones oportunas y pertinentes.

A saber, dichas amenazas suelen contemplar escenarios simples, por ejemplo, donde un virus afecte la productividad de uno o más usuarios; no obstante, actualmente existen algunas más complejas y altamente lucrativas, como los ataques de *ransomware*, que pueden poner a toda la empresa en manos de ciberdelincuentes.

Contar con un equipo de SOC es crucial para las entidades que están expuestas a internet y dependen de este medio para generar ingresos, ya que actúa como garantía de mantenerse en constante actualización sobre nuevas técnicas y amenazas, y se encuentra preparado para accionar cuando ocurre un ataque, minimizando su impacto en las operaciones. En definitiva, la ciberseguridad ya no es solo un aspecto técnico u operativo; ahora, forma parte esencial de la *Agenda del Consejo de Administración*.[1]

Preguntas para el Consejo de Administración o el Comité de Auditoría

- Dentro del Consejo, ¿se conoce el nivel de exposición que tiene la empresa a posibles ciberataques?
- ¿La organización está preparada para responder ante un posible ataque de ciberseguridad?
- ¿Se conocen las amenazas y vulnerabilidades relacionadas en la compañía y el nivel de riesgo que representan?
- ¿Existe comprensión sobre cómo evolucionan las técnicas que utilizan los ciberdelincuentes para llevar a cabo ataques cada vez más sofisticados?
- ¿Se cuenta con el talento, procesos y tecnología necesarios para llevar a cabo las operaciones de ciberseguridad?
- ¿Qué tan difícil es reclutar y retener talento especializado en la materia?
- ¿Cuenta con programas efectivos para capacitar y mantener actualizados a los especialistas del SOC?
- ¿Se conocen, comprenden y reciben métricas de operación del SOC?
- ¿Qué papel desempeña la IA en su estrategia para el SOC?
- ¿Se dispone de un presupuesto adecuado para cubrir las necesidades actuales y futuras de ciberseguridad y del SOC en la compañía?

[1] *Agenda del Consejo de Administración 2024*, KPMG México, 2024.

Preguntas para la Alta Dirección

- ¿El gobierno de ciberseguridad es adecuado y está alineado con el de otras organizaciones comparables?
- ¿El CISO participa en las reuniones del Consejo y se le dan espacios para discutir aspectos relacionados con la ciberseguridad?
- ¿El CISO cuenta con la autonomía necesaria para tomar decisiones relacionadas con las operaciones de seguridad ante un ciberataque?
- ¿Se han establecido indicadores clave de desempeño (KPI, por sus siglas en inglés) para sus operaciones de ciberseguridad?
- ¿En qué medida la compañía se apoya en la tecnología para incrementar la eficiencia de sus operaciones de seguridad?
- ¿Considera óptimo el tiempo que requieren los especialistas para remediar una vulnerabilidad o responder ante un ciberataque?
- ¿Conoce el tiempo que necesita el SOC para detectar una amenaza de ciberseguridad?
- ¿Cuánto tiempo invierten los especialistas de ciberseguridad en analizar falsos positivos, alertas poco confiables o análisis de datos irrelevantes para un evento relacionado?
- ¿Qué nivel de confianza le inspira la IA como herramienta para optimizar sus operaciones de ciberseguridad?
- ¿La organización está preparada para hacer frente a futuros ciberataques?

Acciones que debe contemplar el Consejo

Sin duda, el SOC proporciona una mayor confianza respecto a la seguridad de las empresas, ya que su monitoreo continuo aumenta las probabilidades de detectar y responder oportunamente a próximos ciberataques y reduce el riesgo de un impacto significativo, asegurando la continuidad del negocio. Por ello, el Consejo debe considerar las siguientes acciones:

- Asegurar el compromiso de la Alta Dirección con la ciberseguridad y el SOC
- Garantizar la autonomía y capacidad de toma de decisiones del CISO en la materia
- Revisar los procesos de operaciones de seguridad para alinearlos con los marcos de referencia comúnmente reconocidos
- Destinar el presupuesto adecuado para el SOC, contemplando futuras tendencias de las ciberamenazas
- Invertir en capacitación continua de especialistas, no solo para mantenerlos actualizados, sino también como estrategia de atracción y retención de talento
- Invertir en tecnología adecuada, anticipándose al futuro y adoptando herramientas como la IA para incrementar la eficiencia
- Comprender las métricas y KPI del SOC para optimizar la toma de decisiones
- Identificar los riesgos que representan las amenazas de ciberseguridad para el negocio y tomar medidas acertadas para mitigarlos
- Incorporar una cultura de prevención de riesgos de ciberseguridad en toda la organización
- Buscar asesoría de especialistas para implementar, revisar y actualizar su estrategia de ciberseguridad y del SOC

KPMG

BOARD LEADERSHIP CENTER MEXICO

Acerca de KPMG Board Leadership Center en México

Es un programa global con presencia local exclusivo para miembros del Consejo de Administración en México, que tiene como objetivo promover un gobierno corporativo efectivo para impulsar el valor de la empresa a corto, mediano y largo plazo, generando confianza en los *stakeholders* de las organizaciones.

kpmg.com.mx
800 292 5764 (KPMG)
blc@kpmg.com.mx

KPMG MÉXICO · KPMG MÉXICO · @KPMGMEXICO · KPMGMX

SÚPER EMPRESAS EXPANSIÓN 2024 TOP companies

ESR Empresa Socialmente Responsable Inversión Social

Norma Mexicana en Igualdad Laboral y No Discriminación