Boardroom Questions

Mantener el enfoque en la ciberseguridad y privacidad de datos desde el Consejo

BOARD LEADERSHIP CENTER MEXICO

Alinear la definición de las estrategias de ciberseguridad y privacidad de datos con las prioridades del negocio permite determinar el tipo de protección que requiere la organización a corto y largo plazo.

A saber, una de las responsabilidades prioritarias del Consejo de Administración es salvaguardar los intereses de los accionistas, por lo que un incidente de ciberseguridad podría implicar un impacto negativo en el valor y reputación de la empresa, afectando directamente a los grupos de interés y erosionando su confianza.

Por ello, es fundamental que el Consejo y el Comité de Auditoría aseguren la implementación y el monitoreo de estrategias de ciberseguridad robustas y capaces de garantizar la continuidad operativa del negocio, así como la estabilidad y sostenibilidad de la compañía.

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

Sin duda, las amenazas cibernéticas continúan evolucionando, volviéndose más sofisticadas y su debida prevención se convierte en una prioridad estratégica, ya que representan un riesgo potencial para todas las funciones de la organización.

En este sentido, es esencial que el Consejo y el Comité identifiquen los cambios de dicha evolución para adaptar y optimizar las estrategias relacionadas. Algunas de las prácticas que se deben considerar son:

- Capacitar y concientizar al talento en la materia
- Implementar políticas y procedimientos efectivos
- Utilizar herramientas fundamentales como *firewalls*, sistemas de detección y prevención de intrusiones, *antimalware* y antivirus, herramientas de análisis de vulnerabilidades, de pruebas de penetración, así como de cifrado y gestores de contraseñas, fortalecerán la estrategia de ciberseguridad.
- Gestionar el acceso, monitoreo y detección oportuna de amenazas
- Definir un plan de contingencia y acción contra incidentes
- Vigilar y asegurar el cumplimiento normativo
- Evaluar y gestionar los riesgos

Lo anterior permite mantener un enfoque sólido en la ciberseguridad y privacidad de datos, al mismo tiempo que se protege la información personal y corporativa ante posibles amenazas, asegurando la continuidad operativa del negocio.

Impactos, beneficios e implicaciones para el Consejo

Entre los beneficios de mantener una estrategia de ciberseguridad y privacidad de datos destacan los siguientes:

a) Protección de datos activos: salvaguarda información sensible y activos digitales de la empresa contra accesos no autorizados, robos y daños

b) Reducción de riesgos: minimiza la probabilidad y el impacto de ataques de seguridad, y reduce los riesgos financieros y operativos asociados

c) Cumplimiento normativo: mitiga posibles sanciones y multas

d) Fortalecimiento de reputación y confianza con grupos de interés: al demostrar compromiso con la seguridad y protección de información sensible

e) Continuidad del negocio: garantiza la operatividad sin interrupciones significativas en caso de incidentes de seguridad

f) Generación de ventaja competitiva: establecer una postura sólida en materia de seguridad puede ser un diferenciador en el mercado y atraer clientes que valoran la protección de datos

Preguntas para el Consejo de Administración o el Comité de Auditoría

- ¿Se cuenta con una estrategia de ciberseguridad? ¿Cómo se alinea con los objetivos generales del negocio?
- ¿Cómo se adaptan las estrategias de ciberseguridad ante las nuevas amenazas y tecnologías?
- ¿La empresa se actualiza constantemente respecto a las mejores prácticas del sector en la materia?
- ¿Qué órgano de gobierno se designó para mitigar el riesgo de ciberseguridad?
- ¿Cómo se monitorea el establecimiento y cumplimiento de las estrategias de ciberseguridad?
- ¿Cómo se les da seguimiento a amenazas identificadas o incidentes materializados?
- ¿Cómo identifica y evalúa la empresa los riesgos cibernéticos y qué medidas se toman para mitigarlos?
- ¿Cómo se gestionan y comunican los incidentes de ciberseguridad interna y externamente?
- ¿Se realizan auditorías y evaluaciones de ciberseguridad frecuentemente?
- ¿Qué tipo de recursos financieros y humanos se dedican a la ciberseguridad?
- Al ser un riesgo creciente que puede afectar la continuidad del negocio, ¿cómo se define el presupuesto para mitigar los retos relacionados en la compañía?
- ¿Qué iniciativas de mejora se están implementando en la materia?

Preguntas para la Alta Dirección

- ¿Cuál es el plan de acción ante incidentes de ciberseguridad y cómo garantizan su eficacia?
- ¿Cuál es el proceso para determinar la asignación del presupuesto para las iniciativas en la materia?
- ¿Qué porcentaje del presupuesto anual se asigna para implementar y fortalecer las estrategias relacionadas?
- ¿Qué indicadores y métricas clave se utilizan para medir la eficacia de la ciberseguridad?
- ¿Cuáles son los resultados más recientes de las auditorías relacionadas y cómo se están tratando las áreas de oportunidad identificadas?
- ¿Cómo se promueve una cultura de seguridad en toda la organización?
- ¿Cómo se evalúa y gestiona el riesgo cibernético asociado con proveedores y terceros?
- ¿Qué acciones se implementan para garantizar que los proveedores y terceros con accesos al sistema cumplan con los estándares de ciberseguridad?
- ¿Cómo se reporta al Consejo de Administración y al Comité de Auditoría el estado de la ciberseguridad?
- ¿Qué programas de capacitación y sensibilización en la materia están disponibles para el personal y directivos?

Acciones que debe contemplar el Consejo

El Consejo de Administración juega un papel crucial en la implementación y mantenimiento del enfoque sólido en ciberseguridad y privacidad de datos, por lo que algunas acciones que debe considerar son:

- Designar un órgano de gobierno enfocado en ciberseguridad, ya sea mediante la creación de un comité o designando un responsable dentro del Consejo para la supervisión de las estrategias relacionadas
- Desarrollar, aprobar y actualizar continuamente las políticas de seguridad
- Asignar recursos adecuados
- Fomentar la capacitación continua
- Impulsar una cultura de seguridad que promueva los valores a través de comunicaciones internas
- Supervisar y monitorear informes regulares
- Realizar una evaluación de riesgos de forma periódica
- Definir un plan de acción contra incidentes; realizar simulacros para probar su efectividad, y actualizarlo de manera continua

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 EXPANSION 2024 TOP companies

ESR Empresa Socialmente Responsable Inversión Social