



Boardroom Questions

Enfoque estratégico en ciberseguridad desde el Consejo



La ciberseguridad se ha consolidado como un riesgo estratégico y financiero de primer nivel. Los ataques cibernéticos han incrementado su frecuencia, sofisticación e impacto, provocando interrupciones operativas, impactos reputacionales y exposición a sanciones por incumplimiento de normativas de protección de datos, especialmente cuando no se realiza una adecuada revelación de incidentes.

Ante este panorama, los entes reguladores han elevado sus expectativas respecto al papel que deben asumir los consejos de administración y los comités de auditoría, destacando la necesidad de que estos ejerzan una función activa en la supervisión y gestión de riesgos.



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



La ciberseguridad incide directamente en la sostenibilidad, el valor y la ejecución de la estrategia corporativa. Una sola brecha puede comprometer los planes de crecimiento, los procesos de digitalización y el posicionamiento en el mercado, al afectar la continuidad operativa.

Para el Comité de Auditoría, este riesgo representa un eje fundamental en su labor de supervisión del control interno, convirtiéndose en una pieza clave para monitorear y gestionar adecuadamente las amenazas que podrían comprometer la integridad de la información financiera y el cumplimiento regulatorio.

Impactos, beneficios e implicaciones para el Consejo de Administración y el Comité de Auditoría



El Consejo y el Comité deben incorporar la supervisión de la inteligencia artificial (IA) en sus agendas, mediante auditorías y evaluaciones de riesgo que aseguren el cumplimiento de normativas emergentes y prevengan sanciones, sesgos algorítmicos o el uso indebido de datos.

Aunque la IA impulsa la innovación y la eficiencia, es indispensable establecer lineamientos éticos y de control, así como exigir reportes claros que incluyan métricas de desempeño y riesgos potenciales.

Al designar al Comité de Auditoría como órgano principal de supervisión, se mitigan deficiencias en la gestión de riesgos, controles y revelaciones.

Asimismo, la capacitación continua y el apoyo de especialistas externos fortalecen la toma de decisiones, mientras que la coordinación con otros comités especializados garantiza una gestión transversal, alineada con la estrategia corporativa.



Preguntas para el Consejo de Administración o el Comité de Auditoría



- ¿Cómo se supervisa la efectividad del plan de continuidad del negocio y de recuperación ante desastres? ¿El Comité valida que estén diseñados, implementados y operando eficientemente?
- ¿Se realizan pruebas y simulacros periódicos, con seguimiento oportuno de los hallazgos?
- ¿Existe una estrategia de comunicación interna y externa para gestionar crisis de ciberseguridad?
- ¿Se llevan a cabo auditorías independientes para evaluar el nivel de madurez de la estrategia de ciberseguridad?
- ¿La ciberseguridad está integrada en el marco de gestión integral de riesgos de la organización?
- ¿Cómo se evalúan y priorizan los activos y sistemas digitales críticos, así como su nivel de protección?
- ¿El Consejo recibe reportes claros con métricas clave y seguimiento oportuno de incidentes y hallazgos?
- ¿Cómo se supervisa la ciberseguridad en la cadena de suministro y con proveedores estratégicos?
- ¿Qué riesgos emergentes, como la IA, los ciberdelitos o las tensiones geopolíticas, se monitorean activamente?

Preguntas para la Alta Dirección



- ¿Cómo se vincula la estrategia de ciberseguridad con la estrategia corporativa y digital?
- ¿Cuál es el nivel de preparación de la organización frente a ataques disruptivos, como el *ransomware*?
- ¿Se cuenta con los recursos, presupuesto y talento necesarios para enfrentar amenazas actuales y anticipar futuras?
- ¿Qué tan efectiva es la cultura de ciberseguridad en todos los niveles de la compañía?
- ¿Cómo se evalúan y gestionan los riesgos derivados de terceros y proveedores críticos?
- ¿Cuándo fue la última vez que se realizó un simulacro de incidente cibernético con participación del Consejo y la Alta Dirección?





Acciones que debe considerar el Consejo de Administración

- Reconocer la ciberseguridad como un riesgo estratégico e integrarla de forma recurrente en su agenda
- Garantizar una estructura de reporte efectiva, que contemple una Directora o Director de Seguridad de la Información (CISO, por sus siglas en inglés) independiente y con acceso directo al Consejo o Comité
- Impulsar la capacitación continua de consejeras y consejeros en tendencias y riesgos de ciberseguridad
- Establecer un plan de comunicación claro y oportuno hacia reguladores, inversionistas y clientes en caso de incidentes relevantes
- Incorporar la ciberseguridad en el plan anual de auditoría interna y en la evaluación del control interno
- Revisar periódicamente los reportes de auditoría interna, externa y regulatoria, así como del Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés), sobre controles de seguridad
- Solicitar indicadores consistentes y comparables de riesgo y desempeño en materia de ciberseguridad
- Supervisar el cumplimiento de marcos normativos como los de la Comisión Nacional Bancaria y de Valores (CNBV), el Reglamento General de Protección de Datos (RGPD), la Comisión de Bolsa y Valores de Estados Unidos (SEC, por sus siglas en inglés) y el Consejo de Supervisión Contable de Empresas Públicas (PCAOB, por sus siglas en inglés), así como la correcta revelación en los estados financieros
- Dar seguimiento a la implementación de hallazgos y recomendaciones derivados de auditorías y pruebas de penetración



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



Es posible que algunos o todos los servicios descritos en este documento no estén permitidos para los clientes de auditoría de KPMG y sus afiliados o entidades relacionadas.

La información aquí contenida es de naturaleza general y no tiene el propósito de abordar las circunstancias de ningún individuo o entidad en particular. Aunque procuramos proveer información correcta y oportuna, no puede haber garantía de que dicha información sea correcta en la fecha en que se reciba o que continuará siendo correcta en el futuro. Nadie debe tomar medidas con base en dicha información sin la debida asesoría profesional después de un estudio detallado de la situación en particular.

© 2025 KPMG Cárdenas Dosal, S.C., sociedad civil mexicana y firma miembro de la organización mundial de KPMG de firmas miembros independientes afiliadas a KPMG International Limited, una compañía privada inglesa limitada por garantía. Todos los derechos reservados. Prohibida la reproducción parcial o total sin la autorización expresa y por escrito de KPMG.