Guardians of digital trust
Mes de Concientización sobre la Ciberseguridad

Cómo pueden los Consejos mejorar sus conocimientos sobre ciberseguridad

Seis estrategias para proteger a su organización de las ciberamenazas

BDO

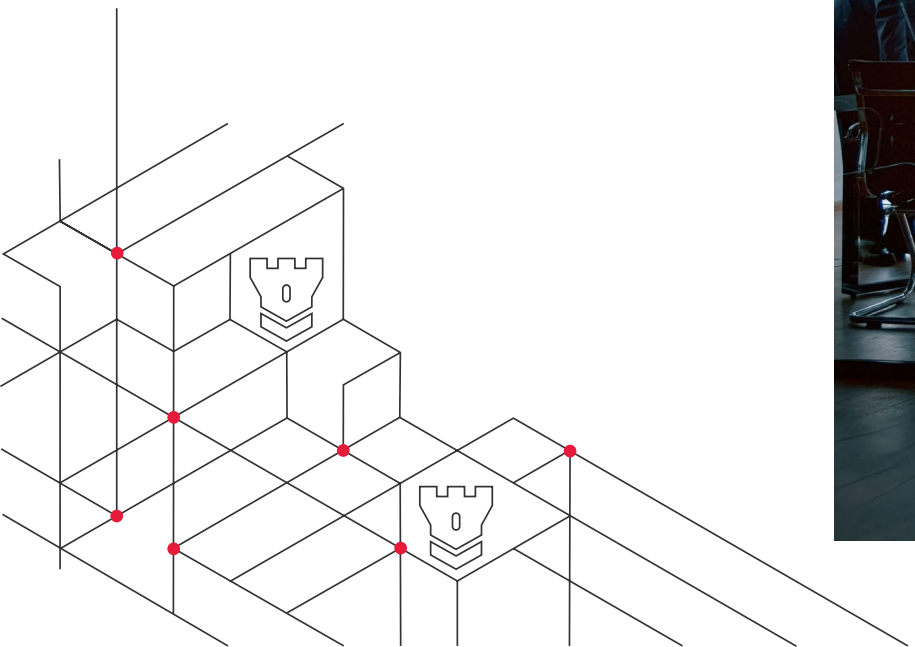
Cómo pueden los Consejos mejorar sus conocimientos sobre ciberseguridad: Seis estrategias para proteger a su organización de las ciberamenazas

Los incidentes de ciberseguridad no solo están aumentando en frecuencia, sino también en coste.

De hecho, el coste medio mundial de una filtración de datos en 2024 es de 4,88 millones de dólares, lo que supone un aumento del 10 % con respecto a 2023. También es el coste más alto hasta la fecha. Por supuesto, las repercusiones financieras no son el único coste al que se enfrentan las organizaciones cuando se enfrentan a un incidente de ciberseguridad, ya que los daños operativos y de reputación también pueden paralizar el negocio.

Los miembros de los Consejos de Administración deben desempeñar un papel activo en la mitigación y prevención de los ciberataques. Sin embargo, sólo el 12% de las empresas del S&P 500 cuentan con un miembro actual o anterior del Consejo que sea experto en ciberseguridad. Esta falta de conocimientos puede estar perjudicando a su organización ahora y en el futuro.

¿Cómo puede asegurarse de que su organización no acabe en el último ciclo de noticias sobre infracciones de ciberseguridad? Empieza por hacer las preguntas adecuadas.



Navegar por el panorama actual de la ciberseguridad: Áreas de interés para la junta directiva

Las capacidades tecnológicas han crecido significativamente a lo largo de los años, permitiendo a las organizaciones operar de forma más eficiente y obtener resultados más rápidos. A medida que la tecnología se entrelaza cada vez más con los objetivos empresariales, los miembros de los Consejos de Administración deben evaluar las decisiones tecnológicas del mismo modo que evalúan las decisiones empresariales estratégicas. Al igual que el Consejo guía la dirección empresarial de una organización, ahora también es responsable de garantizar que se habilitan los elementos tecnológicos correctos para respaldar la estrategia empresarial y que se alcanza y gestiona el nivel adecuado de tolerancia al riesgo cibernético.

Para garantizar una supervisión responsable, el Consejo debe centrarse en las siguientes áreas:

01

Alineación estratégica

Asegurarse de que las iniciativas de ciberseguridad están alineadas con los objetivos empresariales y tecnológicos de la organización. Para ser proactivos, los Consejos también deben asegurarse de que se tienen en cuenta los riesgos y tendencias futuros.

02

Cumplimiento de la normativa

Supervisar el cumplimiento por parte de la organización de las normas y leyes pertinentes. Esto incluye garantizar que se realicen las auditorías y evaluaciones necesarias y que el Consejo tenga conocimiento y una comprensión clara de los resultados.

03

Gobernanza y supervisión

Supervisar las políticas relacionadas con la ciberseguridad de la organización, las estrategias y la alineación con el marco general de gestión de riesgos. El Consejo debe comprender los riesgos cibernéticos relevantes para la organización y garantizar que las políticas establecidas apoyan la mitigación.

04

Seguimiento e informes

Como miembro de la junta directiva, es importante asegurarse de recibir actualizaciones periódicas con respecto a la cibersalud de la organización, incluidos los avances en iniciativas clave de ciberseguridad, métricas clave e indicadores clave de rendimiento.

05

Participación de expertos

Involucrar a expertos en ciberseguridad, ya sea mediante el nombramiento de un experto cibernético en el Consejo, aprovechando un CISO en el equipo de gestión o consultando a un CISO virtual externo (vCISO). Esto garantizará que el Consejo esté bien informado sobre las amenazas y tendencias emergentes.

06

Respuesta a incidentes cibernéticos

Asegúrese de que la organización cuenta con un programa definido de respuesta a incidentes y de que revisan periódicamente las actualizaciones de los resultados de las pruebas de respuesta a incidentes. En caso de incidente cibernético, el Consejo debe desempeñar un papel en la supervisión de la forma en que la organización se comunica con el público y las partes interesadas.

Seis estrategias para aumentar sus conocimientos sobre ciberseguridad

Para que los Consejos de Administración supervisen con éxito el programa de ciberseguridad de su organización, es esencial colmar la actual brecha de conocimientos. Esto ayudará a garantizar que la ciberseguridad se aborde adecuadamente en las reuniones periódicas de los Consejos de Administración y les permitirá desempeñar con confianza sus funciones en materia de ciberseguridad.

He aquí seis estrategias que puede utilizar para aumentar sus conocimientos y estar más preparado para integrar el riesgo tecnológico en los procesos de toma de decisiones:

01

Establezca sesiones periódicas de cibereducación.

Asegúrese de que recibe actualizaciones periódicas sobre ciberseguridad. Durante estas sesiones, dedique tiempo a debatir los principales riesgos de su sector y las experiencias relevantes de organizaciones similares, y formule preguntas sobre lo que hace su empresa para mitigar, prevenir o responder al riesgo de que se produzcan este tipo de incidentes en su organización. Las respuestas que reciba pueden ser clave para reforzar el marco de defensa de su organización.

02

Reorientar las métricas y aprovechar las referencias del sector.

Es importante cambiar el enfoque de las métricas técnicas a métricas de sentido común que destaquen el riesgo y el valor. Por ejemplo, identificar el número de sistemas al final de su vida útil con vulnerabilidades y los controles establecidos para mitigar sus riesgos, o debatir los costes completos de las violaciones cibernéticas, que incluyen el equipo de respuesta real, el apoyo jurídico, así como las repercusiones en las primas de seguros y los ingresos de la organización. Utilice puntos de referencia del sector para comparar su organización con otras de su sector, lo que le ayudará a comprender en qué punto se encuentra y qué mejoras son necesarias.

03

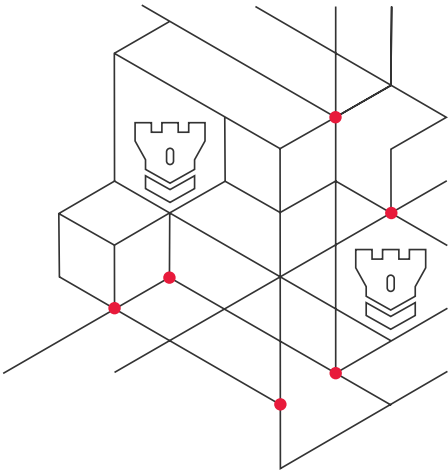
Recurra a expertos externos en ciberseguridad.

Al incorporar expertos externos en ciberseguridad, los miembros del Consejo no sólo pueden mejorar sus conocimientos sobre ciberseguridad, sino también obtener ayuda para «traducir» la información centrada en la tecnología en ideas y estrategias centradas en el riesgo. En última instancia, añadir un puesto de ciberseguridad al Consejo ofrecerá acceso regular a la experiencia que necesita y que complementa a los equipos de gestión de riesgos, seguridad y tecnología de su organización.

04

Realice cibersimulaciones.

Para comprender mejor las amenazas cibernéticas reales y cómo responder a ellas, considere la posibilidad de organizar simulacros de incidentes. Estos ejercicios le ayudarán a comprender su papel como miembro de la junta directiva durante un incidente cibernético, los posibles impactos, las áreas de mejora continua en los flujos de procesos y a desarrollar la memoria muscular.



05

Supervisar durante un incidente.

En caso de ciberataque, los miembros del Consejo de Administración deben participar activamente y recibir información actualizada de los expertos en seguridad y de los equipos de respuesta a incidentes. Al mantenerse al día sobre el progreso y los resultados del incidente, pueden ofrecer una supervisión independiente y hacer preguntas para descubrir cualquier riesgo persistente. También es importante que los Consejos comprendan cómo planea responder la organización a futuros ciberataques.

06

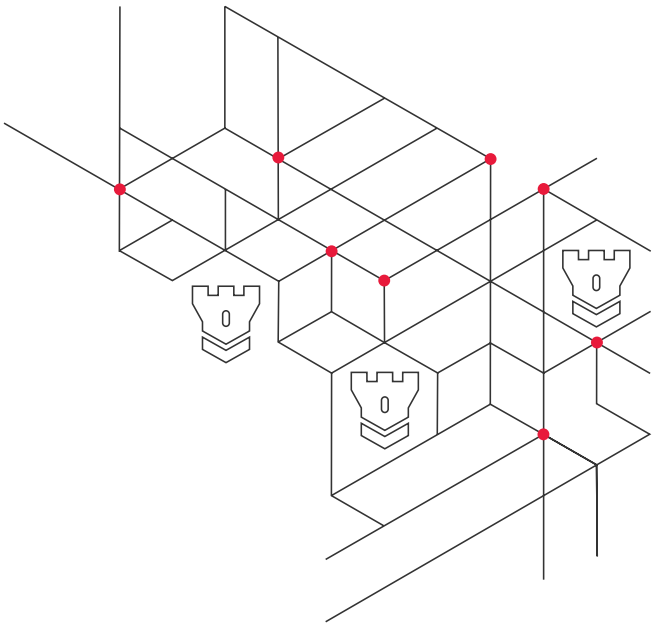
Mirar atrás con retrospectiva.

Lo que se puede aprender de las situaciones cercanas o incluso de un incidente cibernético anterior puede ser lo que impida que vuelva a ocurrir, sobre todo teniendo en cuenta que el 83% de las organizaciones han sufrido más de una brecha de ciberseguridad. Pregunte cuántas veces se han producido estos incidentes y qué ha aprendido la organización para identificar deficiencias y desarrollar medidas adecuadas.

El papel fundamental del Consejo de Administración en la gestión del ciberriesgo

Lo que ha cambiado en los últimos años es el nivel de escrutinio en torno al Consejo de Administración. Al fin y al cabo, los Consejos de Administración están ahí para ayudar a la organización a gestionar los riesgos, incluidos los derivados de incidentes de ciberseguridad.

En un estudio reciente de Gartner, el 88% de los Consejos de Administración afirmaron considerar la ciberseguridad como un riesgo empresarial, lo que pone de relieve la tendencia a dar prioridad a la ciberseguridad como foco de atención del Consejo. Es su deber fiduciario no sólo proporcionar una supervisión independiente para gestionar la postura de ciberseguridad de la empresa, sino también desafiar a su organización de diferentes maneras para elevar el listón de su marco de defensa.



Cómo puede ayudar BDO

En BDO, nuestro enfoque de la ciberseguridad incluye un enfoque centrado en el negocio para gestionar el riesgo cibernético. Ofrecemos sesiones de formación para Consejos de Administración con el fin de ayudar a reducir la brecha de conocimientos y permitir a los miembros de los Consejos de Administración mantenerse a la vanguardia del panorama tecnológico en rápida evolución. En estas sesiones, mostramos a los miembros de los Consejos de Administración cómo reorientar una conversación centrada en la tecnología hacia una conversación sobre el riesgo empresarial, de modo que los Consejos puedan ofrecer eficazmente un nivel responsable de supervisión y formular las preguntas adecuadas a sus equipos. Nuestras sesiones educativas para Consejos de Administración también cubren los últimos riesgos cibernéticos a los que se enfrentan las organizaciones hoy en día y lo que éstas están haciendo para mitigar esas amenazas.

CONECTE HOY MISMO CON NUESTRO EQUIPO DE LIDERAZGO EN CIBERSEGURIDAD

Mejore sus conocimientos sobre ciberseguridad y esté preparado para lo que le depare el panorama de amenazas.