EL CONSEJO DE ADMINISTRACIÓN, PROTAGONISTA DE LA CIBERRESILIENCIA

La pasada primavera una oleada de ciberataques afectó a empresas españolas de todo tipo: Telecomunicaciones, bancos, instituciones gubernamentales y hasta federaciones deportivas. Su dirección y número de teléfono, los datos de su vehículo, la compañía de seguros que lo cubre... cayeron en las manos equivocadas. Y la nueva legislación europea responsabiliza directamente a muchos consejeros por la ciberseguridad de sus empresas, especialmente en los 18 sectores regulados.

TEXTO **MANUEL MONTERRUBIO***

* Extracto realizado por el autor del capítulo original del libro 'Cómo transformar desde el consejo' publicado por LID Editorial en octubre de 2024, del que es co-autor. Manuel Monterrubio, fundador y CEO de empresas, lidera cambios estratégicos como Senior Advisor. Ingeniero formado en UPM, IESE, IE, y MIT, es experto en ciberseguridad.

Este artículo explora la tremenda importancia que ya tiene la ciberseguridad en el ámbito corporativo y especialmente la que va a adquirir a nivel de consejo de administración. Si estos últimos años ha sido la sostenibilidad la que ha aterrizado de lleno en la responsabilidad de los consejos de administración, ahora con la legislación europea NIS 2 y DORA habrá un nivel mínimo de ciberresiliencia de las empresas esenciales de 18 sectores (y, en un lustro, posiblemente de todas las empresas medianas y grandes –*Mid Cap*–). Tambien se tratan la importancia de definir los roles más adecuados a cada empresa -según sector y tamaño- así como de los marcos y estándares más importantes. El artículo concluye con preguntas útiles a tratar en el consejo sobre todo lo concerniente a la ciberresiliencia de la compañía.

Introducción

Tener planes de ciberresiliencia es esencial para proteger empresas, países y ciudadanos frente a amenazas terroristas o de estados totalitarios. Los ciberataques, que ya son una realidad, pueden tener consecuencias catastróficas, como paralizar servicios críticos.

Un ejemplo es la ola de ataques que afectó a España en la primavera de 2024 a empresas de todo tipo (telecomunicaciones, bancos, instituciones gubernamentales y hasta federaciones deportivas). Hasta los datos de tu vehículo, la compañía de seguros que lo cubre, tu dirección y tu número de teléfono, cayeron en las manos equivocadas.

Dark web, reputación, ...

Los hackers roban estos datos para extorsionar o para venderlos en la dark web para diversos fines: desde campañas de phishing personalizadas, donde un cliente podría caer fácilmente, hasta usos menos amenazantes, como campañas de telemarketing que parecen inofensivas, pero que son alimentadas por la información robada.

La manida pregunta no es si tu empresa será atacada, sino cuándo y cómo lo hará el próximo ataque. ¿Están los consejeros y CEOs preparados para lidiar con la realidad de que los datos de sus clientes podrían estar a la venta en la dark web? ¿tiene tu empresa un discurso preparado para enfrentar la crisis si esto sale a la luz?

La reputación es uno de los activos más valiosos para cualquier compañía. Pero ¿se han planteado los líderes el verdadero coste de una crisis de reputación tras un ciberataque importante? Los efectos de un ataque no solo afectan la operativa diaria; pueden desmoronar la confianza que los clientes, socios y accionistas depositan en la organización. Y cuando la confianza se pierde, la recuperación es larga y costosa.

Ciber extorsión, pagar rescate ...

Respecto a la ciber extorsión, las empresas se enfrentan a la difícil decisión de pagar o no pagar un rescate. Pero ¿está tu

empresa preparada para tomar esa decisión de manera informada y estratégica? ¿Qué plan de acción tiene el consejo?

La ciberseguridad, lejos de ser una molestia o un gasto innecesario, es una prioridad que afecta directamente la supervivencia y continuidad de la empresa. ¿Qué nivel de importancia tiene hoy en tu empresa? En un contexto donde la inteligencia artificial está capturando el interés y los recursos, la ciberseguridad debe mantenerse como un foco crucial en las discusiones estratégicas.

Paralización cadena suministro …
Finalmente, para algunas organizaciones, el impacto de un ciberataque puede ser mucho más que un problema operativo. ¿Podría el bloqueo de las operaciones de tu empresa poner en riesgo la seguridad nacional? Y, ¿cómo afectaría un ataque a quienes intervienen en la cadena de suministro de tu empresa? Estas preguntas ya no son hipotéticas; forman parte de la realidad empresarial actual y de las preocupaciones de los consejeros y CEOs que buscan proteger no solo sus compañías, sino su reputación y su futuro en un entorno cada vez más amenazante.

En el artículo, se realiza un enfoque integral y se guía a los consejos de administración en la exigencia de prácticas de ciberseguridad dentro de la estrategia empresarial, equilibrando innovación y seguridad en la era de la inteligencia artificial.

"La ciberseguridad depende más de la actitud y la preparación que del presupuesto. Quien intenta resolver la ciberseguridad con tecnología no entiende ni la ciberseguridad ni la tecnología"

1 La ciberseguridad llegó al Consejo para quedarse

Los consejeros disfrutamos planteando alternativas para impulsar la empresa y que esta despunte, dándole sentido en el tiempo y con acciones que generen más valor y de forma más sostenible.

Normalmente, no disfrutamos con el *compliance*. Sin embargo, para operar, cada día se nos exigen más certificados, auditorías y requisitos varios. Tanto desde las AAPP como por parte de nuestros clientes donde somos parte de su cadena de suministro.

a) Si eres consejero te afecta directamente
La nueva legislación europea responsabiliza directamente a muchos consejeros por la ciberseguridad de sus empresas, especialmente en los 18 sectores regulados. Incluso si tu empresa no está en esos sectores, ser parte de la cadena de suministro también implica responsabilidades. En unos años, las normativas se ampliarán. La ciberseguridad es crítica y depende más de la actitud y la preparación que del presupuesto. Como se dice comúnmente, "quien intenta resolver la ciberseguridad solo con tecnología no entiende ni la ciberseguridad ni la tecnología".

b) Refuerza procesos y actitud más que presupuesto
Es evidente que unos procedimientos claros y una cultura organizativa adecuada, liderada desde la dirección y el Consejo, contribuyen significativamente a mejorar la ciberseguridad, sin necesidad de grandes inversiones en tecnología.

A continuación, resumimos algunos puntos clave que se deben tener presentes:
- *Concienciación y formación del personal:* La formación continua ayuda a prevenir incidentes, haciendo a los empleados menos vulnerables a ataques como el phishing.
- *Cultura de seguridad integrada en los procesos:* La seguridad debe integrarse en todos los procesos organizativos, siendo más efectiva que depender exclusivamente de soluciones tecnológicas.
- *Liderazgo claro desde el Consejo:* Es vital que el Consejo lidere la ciberseguridad, con un CISO que dependa del CEO o un CISO externalizado, pero, a ser posible, siempre independiente del CIO.
- *Evaluación y gestión de riesgos:* Las evaluaciones regulares de riesgos y auditorías anuales de ciberseguridad son imprescindibles, siendo más rentables que auditorías económicas y aportando mayor tranquilidad a la gestión.
- *Aprendizaje continuo y adaptación:* Es esencial una cultura de aprendizaje que permita adaptarse a las nuevas amenazas de manera efectiva, superando enfoques estáticos basados solo en tecnología.

En resumen, el Consejo de administración debe tener una visión holística y equilibrada que integre tanto los aspectos tecnológicos como los organizativos y humanos. Aunque la tecnología es crucial, la cultura organizacional tiene un impacto igual o mayor en la gestión de riesgos, y el Consejo debe liderar este esfuerzo para garantizar una ciberseguridad efectiva.

c) Impacto de la ciberseguridad en la era de la Inteligencia Artificial
El uso de la IA en las empresas está comenzando a integrarse en muchos flujos, aunque en ocasiones sin la validación de áreas críticas como TI o ciberseguridad, lo que puede acarrear riesgos legales y regulatorios. En las grandes multinacionales, esto está más controlado, pero en empresas de todos los tamaños persiste el riesgo del "shadow IT", donde empleados pueden utilizar aplicaciones no controladas, como ChatGPT, para introducir datos sensibles.

■ La IA impulsa la ciberseguridad, pero también los ataques. La IA es una herramienta poderosa para detectar amenazas avanzadas y patrones complejos, pero también facilita ataques más sofisticados. Es fundamental que las empresas se protejan usando IA para respuestas automatizadas, análisis predictivo y mejorar la eficiencia en la seguridad.
- *Respuestas automatizadas:* La IA acelera la respuesta ante

incidentes y permite a los equipos de seguridad enfocarse en decisiones estratégicas.
- *Análisis predictivo:* La IA permite predecir patrones y tendencias, ayudando a las organizaciones a prepararse mejor contra futuras amenazas.
- *Eficiencia y escalabilidad:* La IA gestiona grandes volúmenes de datos imposibles de analizar manualmente, aumentando la eficiencia y capacidad de respuesta en la seguridad.

A pesar de estas ventajas, la IA también presenta riesgos en su uso.

■ Riesgos de nuestras herramientas de producción basadas en IA.
Las herramientas de producción basadas en IA pueden ser manipuladas mediante técnicas como el envenenamiento de datos. Si los algoritmos son comprometidos, la IA puede generar soluciones erróneas o de peor calidad. Para mitigar estos riesgos, las empresas deben controlar los datos de entrenamiento, realizar pruebas continuas a los algoritmos y equilibrar la automatización con supervisión humana.

En resumen, la IA transforma la defensa cibernética, pero requiere un enfoque cuidadoso que combine tecnología y supervisión humana para garantizar su eficacia y seguridad.

d) Produzcas tornillos o prestes servicios B2B, gobierna el dato
Vivimos en la "era del gobierno del dato", donde las empresas recopilan y analizan grandes volúmenes de datos, fundamentales para su éxito. Incluso las pequeñas empresas, que quizás no aprovechan estos datos, se ven obligadas a compartirlos con instituciones o entidades que sí lo hacen.

■ El gobierno del dato es una oportunidad.
Para las grandes empresas, datos fiables son clave en la toma de decisiones a todos los niveles. Una gestión de calidad permite reducir costos, mejorar la eficiencia y satisfacer mejor las necesidades del cliente, beneficiando a empresas de todos los tamaños.

■ Un mal gobierno del dato es un riesgo.
El mal uso de los datos puede generar problemas de seguridad, accesibilidad y cumplimiento normativo. El RGPD ha transformado la forma en que se gestionan los datos personales en Europa, imponiendo severas sanciones por incumplimientos. La ética en su manejo es esencial para garantizar la privacidad y confianza social.

En resumen, el gobierno de los datos es esencial para la sostenibilidad y el éxito de cualquier empresa, y su correcta gestión debe ser impulsada por el Consejo de administración para minimizar riesgos y maximizar oportunidades.

2 Controla el impacto de la ciberseguridad en el negocio

a) Recomendaciones para estar preparado
La ciberseguridad debe alinearse con los objetivos de negocio, asignando inversión y recursos adecuados para prevenir problemas ante futuras amenazas. Dos áreas clave requieren atención.

■ Pide un cumplimiento comparable a tu sector.
Es crucial que las empresas establezcan políticas y estándares de seguridad comparables a su sector. Un diseño seguro validado externamente garantiza que los riesgos se gestionan correctamente.

Se deberían dar al menos estos tres pasos: realizar una auditoría de ciberseguridad, evaluar activos y amenazas, y desarrollar políticas que sigan estándares reconocidos como la ISO 27001 o ENS. Además, es importante que la empresa forme continuamente a empleados y directivos sobre buenas prácticas de seguridad.

■ Exige conocer los planes de respuesta a incidentes, continuidad, etc.
Toda empresa debe contar con Planes de Respuesta ante Incidentes (PRI), Procedimientos de Recuperación de Desastres (PRD) y Planes de Continuidad de Negocio (PCN). Estos permiten a la organización mitigar el impacto de los incidentes de seguridad, recuperarse ante desastres y seguir operando bajo condiciones mínimas mientras se restablecen los sistemas.

El PRI asegura la detección de incidentes, la comunicación efectiva y la mitigación de daños. El PRD se enfoca en la recuperación de sistemas tras un desastre, mientras que el PCN garantiza que la empresa pueda seguir funcionando a niveles básicos. Estos planes deben abarcar todas las áreas, no solo IT, e involucrar a marketing, RR. HH., legal, y operaciones. Además, se deben realizar simulacros periódicos para que todos sepan cómo actuar ante un incidente.

"La nueva regulación europea responsabiliza directamente a muchos consejeros de la ciberseguridad de sus empresas. El reglamento DORA, aplicable a empresas del sector financiero, y la directiva NIS 2, que cubre 18 sectores críticos como energía o transporte, comenzarán a aplicarse en 2025, con sanciones elevadas, y es fundamental conocerlos"

Para concluir con este apartado, un punto importante que deben conocer también los miembros de los consejos de administración, pues ha fallado hasta en reputadas empresas e instituciones, es que se debe confirmar que existen buenas copias de seguridad, que se realizan continuamente y que no están alojadas en las mismas instalaciones, ni conectadas a los sistemas que puedan ser atacados (este último punto es crucial aunque parezca obvio).

b) La empresa ha sufrido un ataque de ciberseguridad, ¿qué hace ahora?
Como ya se mencionaba en el apartado anterior, la empresa debe seguir los planes y, si hay una empresa especializada que respalda al equipo de tecnologías de la información, el problema estará más o menos controlado.

Cuando ocurre un incidente de ciberseguridad, es esencial actuar rápidamente y con claridad. La clave es contener el problema y luego analizarlo para mejorar la infraestructura y cultura de seguridad. A continuación, se describe un plan de acción básico:

■ Plan de acción para la respuesta a incidentes de ciberseguridad
La coordinación entre el CISO y el CIO es crucial.
a) Identificación y contención: Identificar el ataque y aislar los sistemas afectados para evitar su propagación.
b) Erradicación y recuperación: Eliminar la amenaza y restaurar los sistemas desde copias de seguridad seguras.
c) Comunicación y notificación: Informar a la dirección y, si es necesario, notificar a clientes y autoridades. Cumplir con normativas como RGPD o NIS 2 es crucial para evitar sanciones.
d) Análisis posterior al incidente: Analizar lo ocurrido para actualizar los protocolos y evitar que vuelva a suceder.

■ ¿Cómo minimizar el impacto del ataque?
Si contamos con PRD o PCN, simplemente debemos seguir los protocolos establecidos. Sin embargo, si no los tenemos, es importante pedir ayuda rápidamente. Además de las repercusiones operativas y financieras, no debemos subestimar el impacto reputacional. La comunicación transparente es clave, y el Consejo debe asegurarse de tener previsto un plan de comunicación de crisis para mantener la confianza de clientes, empleados y otras partes interesadas.

"Toda empresa debe contar con Planes de Respuesta ante Incidentes, Procedimientos de recuperación de Desastres, y Planes de Continuidad del Negocio"

c) Cómo mitigar el riesgo con seguros de responsabilidad civil y ciberseguros
En las empresas, al igual que con los sistemas contra incendios, los seguros de ciberseguridad son cada vez más comunes para cubrir imprevistos derivados de ataques. Los ciberseguros y los seguros de responsabilidad civil no solo ofrecen protección financiera, sino también servicios de respuesta ante incidentes.

■ Importancia de los seguros en la gestión de riesgos de ciberseguridad.
Cobertura financiera: Protegen contra pérdidas por interrupciones del negocio o sanciones normativas.
Recursos para la respuesta a incidentes: Algunas pólizas incluyen expertos en ciberseguridad y legales.
Cumplimiento regulatorio y protección reputacional: Cubren costos de gestión de crisis y reputación.

■ Evaluación de pólizas para diferentes riesgos de ciberseguridad.
Seguros de responsabilidad civil: Protegen contra reclamaciones por daños a terceros.
Ciberseguros: Cobertura frente a ransomware, brechas de datos, y otros incidentes.
Pólizas específicas según el tipo de empresa: Empresas con datos sensibles o regulaciones estrictas requieren coberturas especializadas.
El comité de riesgos debe considerar estos aspectos cuidadosamente.

3 Cumpliendo legislación y estándares de ciberseguridad de tu sector

El RGPD, transpuesto en la LOPD en España, es clave para el tratamiento de datos personales, pero otras normativas como DORA, NIS 2 o el ENS también impactan en la ciberseguridad y exigen atención por parte de los consejeros. Estas normativas, que solían ser responsabilidad del CISO o CIO, ahora trasladan parte de la responsabilidad a los Consejos de Administración.

a) Diferencias entre norma, estándar, reglamento y directiva
Norma y estándar son términos prácticamente equivalentes, como la ISO 27001. Realmente cuando usamos la palabra "norma" a veces puede parecer que es, como una norma de tráfico, de obligado cumplimiento, pero no es el caso, por eso es preferible usar la palabra "estándar".

Un reglamento, como el RGPD, es directamente vinculante en cada Estado miembro de la UE, mientras que una directiva, como NIS 2, requiere que los Estados miembros la incorporen en su legislación. Ambas, una vez aplicadas, tienen fuerza legal.

Existen también guías y marcos, como el NIST para ciberseguridad, que aunque no tienen fuerza legal, son ampliamente utilizados en la industria por su utilidad.

Es importante que los consejeros estén familiarizados con estos términos y normativas, aunque no sean de obligado cumplimiento. En el capítulo del libro de donde se ha extraído este artículo -por su limitada extensión- se ofrece una lista de conceptos clave para que los consejeros se familiaricen con la terminología esencial en su labor de supervisión.

b) ¿Qué legislación y estándares se aplican según sector y tamaño de empresa?
Las empresas, sean pequeñas o grandes, deben cumplir la legislación relativa a privacidad, ciberseguridad etc. Con

distintos niveles de rigor en cuanto al acceso a sistemas y la gestión de datos pero han de cumplir y la responsabilidad en cada vez más ocasiones, escala hasta el consejo de administración.

■ RGPD
El RGPD (o GDPR como tambien se conoce, en inglés) afecta a todas las empresas, independientemente de su tamaño, exigiendo la protección de datos personales y la notificación a las autoridades en caso de brechas de seguridad, con elevadas sanciones proporcionales a la gravedad de los incidentes.

■ ENS
Las empresas que trabajen con organismos públicos deben cumplir con el Esquema Nacional de Seguridad (ENS), que tiene varios niveles según el organismo y los servicios prestados.

■ DORA y NIS 2
El reglamento DORA, aplicable a empresas del sector financiero, y la directiva NIS 2, que cubre 18 sectores críticos, como energía o transporte, exigen a las empresas medidas de ciberseguridad y resiliencia digital. Estas regulaciones comenzarán a aplicarse en 2025 con sanciones elevadas y es muy importante conocerlas.

■ Reglamento de ciberseguridad y reglamento de ciberresiliencia de la UE
La UE está muy concienciada con el problema que suponen los ataques y está preparando un reglamento de ciberseguridad con estándares comunes y certificables para todos los Estados miembros, así como un reglamento de ciberresiliencia que regulará la seguridad de productos y servicios digitales desde el diseño hasta su ciclo de vida.

■ Otras siglas muy habituales
Existen otros estándares como PCI DSS para datos financieros, SOC 2 para organizaciones de servicios, y C5, un estándar alemán para la nube, con los que las empresas pueden tener que cumplir dependiendo de su sector. Lógicamente cada empresa suele saber dependiendo de su actividad lo que debe cumplir pues sus clientes les exigirán lo mismo que a otros competidores.

c) Las seis medidas principales que se deben adoptar desde los órganos de administración de las empresas e instituciones
Independientemente de si la empresa está afectada por NIS2 o DORA, los consejeros deben implementar ciertas medidas de ciberseguridad para garantizar tranquilidad. NIS2 exige:
1) Medidas de gobernanza.
2) Gestión de riesgos de ciberseguridad.
3) Procesos de gestión de incidentes.
4) Garantizar la continuidad operativa.
5) Asegurar la cadena de suministro.
6) Evaluaciones periódicas de la gestión de riesgos.
Los órganos de administración son responsables de aprobar y supervisar estas medidas, además de recibir formación continua en gestión de riesgos de ciberseguridad.

d) Los fallos de seguridad de tus proveedores pueden ser tu problema
Los problemas de ciberseguridad de los proveedores pueden repercutir en la empresa. Para protegerse, los acuerdos de nivel de servicio (SLA) deben incluir:
1) Políticas de seguridad, estándares y certificaciones: los proveedores deben cumplir con estándares como ISO 27001 o ENS.
2) Planes de gestión de incidentes y controles técnicos: es necesario que los proveedores cuenten con un plan de respuesta a incidentes (PRI) efectivo, con medidas de seguridad robustas.
3) Auditorías externas: se deben solicitar auditorías periódicas de seguridad y considerar la realización de auditorías internas para proveedores críticos.

e) Conclusión sobre legislación y responsabilidad de consejeros
Las normativas como NIS2 y DORA imponen requisitos específicos a las empresas según su sector y tamaño. Los consejeros deben comprender estos reglamentos y tomar medidas proactivas para minimizar riesgos. Es fundamental adoptar una cultura de ciberseguridad y proteger los datos y sistemas, ya que estas normativas implican sanciones disuasorias que afectarán directamente a los Consejos de Administración.

"La UE está muy concienciada con el problema que suponen los ataques y está preparando un reglamento de ciberseguridad con estándares comunes y certificables para todos los Estados miembro, así como un reglamento de ciberresiliencia que regulará la seguridad de productos y servicios digitales desde el diseño hasta su ciclo de vida"

Con DORA y NIS2, los consejeros serán corresponsables de la ciberseguridad y deberán asegurarse de cumplir con las regulaciones para evitar sanciones y riesgos reputacionales.

4 El consejo de administración, el CEO y los roles clave en ciberseguridad

El Consejo de Administración tiene una responsabilidad creciente en la ciberseguridad debido a regulaciones como NIS2 y DORA, que lo sitúan como parte responsable en muchos sectores, y pronto en todos. Aunque el CISO es el encargado directo de supervisar las políticas y medidas de prevención, también hay otros roles clave dependiendo del tamaño y sector de la empresa.

■ El CISO
Es el responsable de todas las políticas y supervisión de ciberseguridad. Sin embargo, en empresas más grandes, puede estar acompañado de otras figuras clave.

■ El CSO
Cuando la seguridad física es tan crucial como la digital, el Chief Security Officer (CSO) puede tener la misma importancia o incluso estar al nivel del CISO, o supervisar ambas áreas.

■ El CRO (Chief Risk Officer)
En grandes empresas, el CRO gestiona los riesgos de ciberseguridad, financieros, regulatorios y estratégicos, trabajando en conjunto con otros roles para mitigar riesgos.

■ ¿El CIO y el CISO deben estar a la misma altura en el organigrama?
Existe un debate sobre si el CISO debiera estar al mismo nivel que el CIO. Mientras que sería lógico que ambos reportaran directamente al CEO, en la realidad, muchas veces el CISO depende del CIO. Según un estudio de Heidrick & Struggles en 2022, solo el 5% de los CISO reporta directamente al CEO, mientras que el 38 % reporta al CIO. La estructura depende de la relevancia que la ciberseguridad tenga en la empresa, y en algunas grandes compañías el CISO reporta al CRO o CSO.

■ Variación de roles según industrias y tamaños
Los roles de ciberseguridad varían según la industria. En el sector financiero, por ejemplo, se requieren roles como CRO, CSO y CISO debido a la importancia de la seguridad normativa, la protección contra fraudes y la seguridad de las transacciones. Este sector también tiene un enfoque en la vigilancia en tiempo real y en la seguridad de los datos.

"Los cada ves más comunes seguros de ciberseguridad y los seguros de responsabilidad civil no solo ofrecen protección financiera sino también servicios de respuesta ante incidentes"

En sectores como la salud, la protección de la privacidad del paciente es fundamental, con normativas como el RGPD en Europa y la HIPAA en Estados Unidos, que regulan la privacidad de la información médica.

Para cualquier empresa, especialmente las que presten servicios críticos o dependen de la tecnología, la figura del CISO es crucial. Si la empresa no puede permitirse un CISO a tiempo completo, es recomendable optar por un CISO as a Service.

Podríamos concluir con que a medida que las empresas avanzan en el uso de la tecnología, IA y datos, la importancia del CISO aumenta. Incluso en compañías más pequeñas, donde el tamaño no justifica un CISO a tiempo completo, esta figura debe ser considerada como parte fundamental en la gestión de riesgos tecnológicos. De no ser posible, se debe optar por soluciones externalizadas como el CISO as a Service.

5 Conclusiones

El capítulo aborda de manera exhaustiva la creciente importancia de la ciberseguridad en el entorno corporativo, destacando su impacto tanto en la estrategia empresarial como en la gestión de riesgos.

Enfatiza que la ciberseguridad no depende únicamente de las inversiones tecnológicas, sino de una cultura organizacional robusta y procesos bien definidos. La integración de prácticas de ciberseguridad en todos los niveles de la empresa, desde la alta dirección hasta los empleados, es crucial para crear una defensa eficaz contra las amenazas.

Además, resalta que la adopción de tecnologías emergentes, como la inteligencia artificial, debe ser gestionada con cuidado, asegurando un equilibrio entre innovación y seguridad.

Por último destaca el papel del consejo de administración como fundamental en este contexto, debiendo liderar con una visión holística y proactiva la integración de la ciberseguridad en la estrategia general de la empresa.

6 Posibles preguntas útiles para tratar en el Consejo

- ¿Cómo se alinean los recursos dedicados a ciberseguridad con nuestras prioridades y riesgos estratégicos identificados?
- ¿Qué procesos tenemos para la evaluación y mejora continua de la estructura de ciberseguridad en la empresa? ¿Y para ajustar de manera continua nuestra inversión en ciberseguridad?
- ¿Qué cambios en la actitud o la cultura corporativa son necesarios para reforzar nuestra resiliencia frente a las amenazas cibernéticas?
- ¿Cómo estamos evaluando y mitigando los riesgos asociados con la adopción de tecnologías de IA?
- ¿Cómo equilibramos la innovación y el uso efectivo de datos con las necesidades de ciberseguridad?
- ¿Cómo están integrados nuestros planes de ciberseguridad y continuidad del negocio?
- ¿Realizamos auditorías y simulacros periódicos para probar la resiliencia de nuestra estrategia de ciberseguridad? ¿Qué criterios usamos para seleccionar a los auditores?
- ¿Tenemos un marco de cumplimiento actualizado? ¿Cómo lo comparamos con los estándares de nuestra industria?
- ¿Estamos al día con las regulaciones más críticas? ¿Qué distancia nos separa con los estándares en nuestra industria?
- ¿Cómo están definidos actualmente los roles clave de ciberseguridad en nuestra organización y cómo se alinean con nuestros objetivos estratégicos? ■