



IT Risk & Security
Internal Audit

Cyber Risk

**y el rol de los Directores en la
Junta Directiva**



CONTENIDO

1. Introducción

2. Cyber-Risk y el rol de la Junta Directiva

3. Reflexiones finales



1. Introducción

Las Juntas Directivas en nuestras latitudes, en su mayoría, han invertido tiempo en revisar el desempeño financiero, decidir sobre el plan estratégico y aprobar nombramientos claves.

La acelerada digitalización y dependencia de las organizaciones en la tecnología de información, ha obligado a que temas como el cyber-risk, formen parte de la agenda de la Junta Directiva. La sofisticación y el impacto de las amenazas-riesgos tecnológicos en un mundo interconectado y dependiente, demanda que los Directores en la Junta Directiva adopten un rol proactivo, decisivo y continuo sobre el impacto del cyber-risk en la organización.

1. Introducción

Es sano mencionar que existen dos términos que generalmente en la organizaciones se utilizan como si fueran lo mismo, cuando en realidad no lo son.

Cyber-risk

Es el riesgo de pérdida financiera, interrupción de la operación o daño a la reputación de una organización debido a algún tipo de falla de sus sistemas de tecnología de la información.

Cyber-security

Es el arte de proteger redes, dispositivos y datos del acceso no autorizado o uso delictivo a fin de garantizar la confidencialidad, integridad y disponibilidad de los datos.

A continuación, respondemos siete preguntas que usualmente nos hacen sobre el rol de los Directores en la Junta en cuanto al cyber-risk.

2. Cyber-Risk y el rol de la Junta Directiva

1

¿Es el cyber-risk tan crítico en la organización para requerir la atención de los Directores en la Junta Directiva (JD)?

Sí es crítico el cyber-risk. Según la revista Forbes, el riesgo no es solo financiero, de reputación o legal; ahora incluso la vida y la seguridad de las personas están en juego. Los ciberataques en la primera mitad de 2022 aumentaron un 42 % en comparación con 2021. El año 2022 terminará con un incremento preocupante. Los ataques cibernéticos a las compañías son cada vez más frecuentes y sofisticados. Los reguladores exigen más protección a los datos personales de los clientes. Para el año 2025, una respetada compañía en tecnología de información estima que el costo de los delitos informáticos alcanzará USD 10.5 Trillones.

2

Hay un Director en la JD que conoce de tecnología de información, ¿Por qué el resto de los Directores debemos conocer sobre cyber-risk?

Conocer sobre tecnología de información no significa conocer sobre cyber-risk y/o cyber-security. Por analogía sería pretender que un odontólogo haga un cirugía de corazón abierto y la anestesia la aplique un cardiólogo. Todos son doctores, pero con especialidades diferentes. Lo mismo ocurre con cyber-risk, cyber-security y tecnología de información; son temas relacionados, pero con enfoques, marcos de acción y perspectivas distintas.

2. Cyber-Risk y el rol de la Junta Directiva

3

Si existen un Comité de Riesgo y un Comité de Tecnología, ¿Por qué los Directores en la JD tienen que estar al corriente del cyber-risk?

Porque cada uno tiene roles distintos. El rol de los Directores en la JD ha dejado de ser ese cuerpo de gobierno, muy formal, a veces inalcanzable para los colaboradores, que se reúne regularmente para analizar indicadores financieros. Hoy día, los Directores en la JD tienen un rol más activo sobre temas claves que antes eran vistos solo por la Gerencia. El cyber-risk es solo uno de ellos. Un Director independiente que conozca sobre cyber-risk, podría ayudar mucho a la JD.

4

Los Directores en la JD aprueban la compra de tecnologías para proteger los sistemas informáticos y redes. Eso es estar al corriente del cyber-risk ¿o no?

No lo es. Es positivo que los Directores en la JD aprueben la compra de tecnologías y asesorías para proteger las redes y sistemas de la organización. No obstante, el rol de los Directores en la JD en cuanto al cyber-risk es más amplio y clave. En las respuestas de las preguntas seis y siete, ampliamos este tema.



2. Cyber-Risk y el rol de la Junta Directiva

5

**Los Directores en la JD tienen conocimientos diversos.
¿Por qué debemos ser expertos en cyber-risk?**

No se espera que los Directores en la JD sean expertos en cyber-risk, pero sí que manejen un lenguaje básico para tomar decisiones adecuadas cuando los expertos en riesgo, tecnología y seguridad de información lleven asuntos importantes que requieran la atención y juicio de los Directores en la JD. Ante la pregunta si solo un Director o todos deben conocer sobre cyber-risk, somos del criterio que deben ser todos. Para tal fin los Directores en la JD deben recibir capacitación básica y continua sobre cyber-risk, cyber-security y los riesgos-amenazas tecnológicas emergentes.

6

¿Cuál debe ser el rol de los Directores en la JD en cuanto al cyber-risk?

Muchas iniciativas de negocio que generan rentabilidad, dependen del uso de tecnología de información e inevitablemente, conllevan riesgos y amenazas tecnológicas. Los Directores en la JD deben diseñar estrategias, pero no articularlas. Enfocarse en actividades de seguimiento, monitoreo y revisión de las iniciativas que la Gerencia lleva adelante en cuanto al cyber-risk. Mantenerse actualizados sobre riesgos y amenazas tecnológicas, así como también sobre tendencias modernas en seguridad de información.

2. Cyber-Risk y el rol de la Junta Directiva

7

¿Cómo los Directores en la JD se pueden asegurar que las medidas en cyber-risk y/o cyber-security en la organización son efectivas?

Evaluando regularmente que:

- Los KPI definidos para el cyber-risk y cyber-security son los valores esperados a través del tiempo.
- Existan mecanismos para que los colaboradores puedan expresar a cualquier nivel de la organización alguna preocupación sobre riesgos y amenazas tecnológicas.
- La estrategia de cyber-security esté integrada a la estrategia de la organización.
- El apetito o tolerancia al cyber-risk definido por la Gerencia es adecuado.
- Los recursos y estructuras aprobadas por la Gerencia para las áreas a cargo de gestionar el cyber-security y cyber-risk son las adecuadas para la organización.
- En los Comités de Riesgo/Auditoría/Cumplimiento/Tecnología existan miembros independientes que conozcan sobre el cyber-risk.
- Actualizarse regularmente sobre las últimas tendencias en cyber-risk y/o cyber-security.

Fuentes: Institute of Risk Management; National Institute of Standard & Technology; Cybersecurity & Infraestructure Security Agency; Harvard Law School Forum on Corporate Governance; Cyber-security Ventures

3. Reflexiones finales

El rol de los Directores en la Junta Directiva va mucho más allá de las actividades tradicionales en las que se han involucrado hasta ahora.

Hoy los Directores en la JD deben jugar un rol proactivo. Tener una comprensión básica sobre cyber-risk, es imprescindible, al igual que estar vigilante de las iniciativas claves de la Gerencia en materia de cyber-security y/o cyber-risk.

El cyber-risk es mucho más que tecnología de información. Pensar que las decisiones y seguimiento de las amenazas-riesgos tecnológicos son aspectos exclusivos de las áreas de GRC (Governance, Risk & Compliance) es un error. Los Directores en la JD deben definir KPI's para monitorear las acciones mitigantes de la Gerencia sobre el cyber-risk.

Es comprensible que algunos Directores en la JD sientan que su limitado tiempo debe ser priorizado para decisiones de carácter financiero sobre otras como el cyber-risk. Es también evidente que la industria del ciberdelito existe, mueve billones de dólares americanos anualmente y está en crecimiento.

Que nadie es inmune, es sano tenerlo presente.



CONTACTOS

Panamá y CARICOM

Antonio Ayala I.
aayala@riscco.com

Rubén Fernández
rfernandez@riscco.com

Roberto Delgado
rdelgado@riscco.com

Raúl Lezcano
rlezcano@riscco.com

República Dominicana y Puerto Rico

Rubén Fernández
rfernandez@riscco.com

Costa Rica y El Salvador

Oscar Sánchez
osanchez@riscco.com

Guatemala, Honduras y Nicaragua

Luis Guillen
lguillen@riscco.com

riscco.com

Es una compañía regional independiente y dedicada de manera exclusiva ayudar a organizaciones a enfrentar sus desafíos en GRC (*Governance, Risk & Compliance*) y ESG (*Environmental, Social & Governance*); compuesta por profesionales con el conocimiento y credibilidad necesaria para traducir aspectos muy técnicos a un lenguaje simple y con sentido de negocio. Con trece (13) años de haber iniciado operaciones, RISCCO cuenta en su cartera de clientes con compañías privadas e Instituciones del Estado en la región líderes en su ramo.

