



Columna

Carlos Honorato
CEO de Orión



Ley de Ciberseguridad

La ciberseguridad ha dejado de ser un asunto técnico para convertirse en un tema estratégico que debe ser gestionado desde el más alto nivel de las organizaciones. Con la nueva Ley de Ciberseguridad en Chile, los directorios ya no pueden limitarse a delegar este ámbito en sus equipos de tecnología.

Hoy, deben asumir un rol activo en la prevención de riesgos digitales, la supervisión del cumplimiento normativo y la toma de decisiones

El verdadero desafío para los directorios es integrar la ciberseguridad dentro de la estrategia corporativa y asignar recursos adecuados.

que garanticen la continuidad del negocio en un entorno cada vez más expuesto a amenazas cibernéticas.

El impacto de esta ley en la gobernanza empresarial es profundo. La normativa impone exigencias concretas, como la designación de un delegado de

ciberseguridad, la implementación de planes de continuidad operacional y la obligación de reportar incidentes en plazos estrictos.

Estas responsabilidades ya no recaen solo en el área de TI o en el equipo legal, sino que forman parte del mandato del directorio. Ignorarlas puede derivar en sanciones económicas millonarias y, en algunos casos, en responsabilidades legales individuales para los directores.

La pregunta clave es si los directorios están prepara-

dos para asumir esta nueva realidad. Durante años, la ciberseguridad ha sido percibida como un tema técnico y ajeno a la toma de decisiones estratégicas.

Pero actualmente, la gestión del riesgo digital es tan importante como la supervisión financiera o el cumplimiento regulatorio. Un ciberataque no solo afecta la operación de la empresa, sino que puede poner en jaque su reputación, su relación con clientes y proveedores e incluso su posición competitiva en el mercado.

El verdadero desafío para los directorios es integrar la ciberseguridad dentro de la estrategia corporativa y asignar los recursos adecuados para su implementación. Esto significa no solo contar con especialistas en la materia, sino también asegurar que los planes de acción sean efectivos y alineados con las mejores prácticas internacionales.

La falta de conocimiento técnico no puede ser una excusa. Así como los directores deben entender principios financieros para supervisar la salud económica de la empresa, ahora también deben comprender los riesgos y desafíos del entorno digital en el que operan.

El cambio de paradigma es inevitable. La ciberseguridad ya no es un tema opcional ni un gasto secundario, sino una inversión crítica en la sostenibilidad del negocio. Los directorios que no tomen en serio esta transformación corren el riesgo de quedar expuestos no solo a ciberataques, sino también a sanciones, pérdida de confianza y, en última instancia, al fracaso corporativo. La ciberseguridad es hoy un pilar esencial de la gobernanza empresarial. Ignorarla no es una opción.