El marco legal de la ciberseguridad, nueva responsabilidad para los directorios

Hernán Orellana H.[1]

La digitalización ha traído importantes beneficios para la sociedad, desde el acceso mejorado a servicios hasta la optimización de operaciones críticas en sectores como la salud, finanzas y transporte. Sin embargo, la confianza pública es un factor esencial para que la adopción tecnológica sea masiva y exitosa. En este contexto, la ciberseguridad se convierte en un imperativo absoluto, ya que el crecimiento exponencial de delitos informáticos pone en riesgo tanto la infraestructura como la información sensible de los usuarios. A medida que los ataques cibernéticos se multiplican, las leyes y regulaciones sectoriales han avanzado para exigir a los proveedores de servicios que aseguren sus activos y garanticen la continuidad de servicios críticos. En este escenario, el gobierno corporativo tiene la responsabilidad de garantizar el debido cumplimiento de estas normativas, asumiendo un papel proactivo en la supervisión y gestión de los riesgos cibernéticos.

A partir del año 2023, Chile cuenta con una ley llamada Ley Marco de Ciberseguridad (N° 21.663). Uno de los aspectos más destacados de esta ley es que define a instituciones que presten servicios calificados como esenciales para el funcionamiento del país, como son los servicios de la administración del estado, los servicios de provisión y distribución de energía eléctrica, agua potable, combustibles, telecomunicaciones, infraestructura digital, servicios financieros, hospitales, entre otras. Dentro de estos sectores, define a los operadores de importancia vital (OIV), como aquellos que, en la provisión de sus servicios dependan de las redes informáticas y que la afectación en la provisión de dichos servicios signifique un impacto significativo para el funcionamiento del país.

La creación de la Agencia Nacional de Ciberseguridad (ANCI) es otro de los pilares de la nueva ley. La ANCI tendrá funciones fiscalizadoras, asegurando que las instituciones cumplan con los estándares establecidos y aplicando sanciones en caso de incumplimiento. Esto pone una mayor presión sobre los directorios, quienes deberán responder ante esta nueva agencia y garantizar que sus políticas de ciberseguridad estén alineadas con los requerimientos. La ANCI también fomentará el intercambio de información sobre amenazas y mejores prácticas, lo que será fundamental para crear una cultura de ciberseguridad a nivel nacional.

Los directorios de las empresas que presten servicios esenciales deberán aplicar de manera permanente medidas para prevenir, reportar y resolver incidentes de ciberseguridad, junto con implementar los protocolos y estándares que dicte la ANCI así como los que determine la autoridad sectorial. Estas empresas deberán prevenir y gestionar los riesgos asociados a la ciberseguridad, contener y mitigar los impactos que los incidentes puedan tener en la continuidad operacional del servicio prestado, preservar la confidencialidad y la integridad de la información, redes o sistemas informáticos.

---

[1] Director de Empresas y Asesor en Transformación Digital

Los directorios de las empresas que sean calificadas por la ANCI como OIV deberán cumplir con una serie de requerimientos más específicos, como son: implementar un sistema de gestión de riesgos de la Seguridad de la Información (SGSI), mantener un registro de las acciones ejecutadas según el SGSI, elaborar e implementar planes de continuidad operacional y de ciberseguridad, certificar dichos programas al menos cada 2 años, realizar continuamente operaciones de revisión y simulacros para comprobar la efectividad de dichos planes y programas, adoptar en forma oportuna medidas que reduzcan el impacto de un incidente de ciberseguridad, informar la ocurrencia de un incidente (en plazos acotados y definidos) y otras obligaciones que establezca la ANCI. Los OIV deberán contar con programas de capacitación y educación continua en ciberseguridad, incluyendo campañas de ciberhigiene y designar un delegado de ciberseguridad.

Como se aprecia de lo anterior, el desafío para los directorios no se limita a la implementación de tecnologías de ciberseguridad, sino también a asegurar que los equipos ejecutivos estén capacitados para responder eficazmente a incidentes. Los directores de empresas tendrán que asumir un papel más activo, integrando la ciberseguridad en la estrategia corporativa y asegurando que sus organizaciones estén preparadas para enfrentar los desafíos de un mundo cada vez más digital.