/Carey

Mayo de 2023

AVANZA PROYECTO DE LEY MARCO SOBRE CIBERSEGURIDAD

El pasado 26 de abril la Sala del Senado por unanimidad aprobó en particular (primer trámite constitucional) el Proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. Así, la propuesta legislativa paso a segundo trámite constitucional a la espera de ser discutida por la Cámara de Diputados y Diputadas.

El proyecto tiene como objeto establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares, así como establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad y ciberataques.

Los principales elementos del proyecto se indican a continuación:

• **Institucionalidad.** La iniciativa contiene un fuerte enfoque institucional, creando la **Agencia Nacional de Ciberseguridad** ("ANCI"), el **Consejo Multisectorial sobre Ciberseguridad** y los **Equipo de Respuesta a Incidentes de Seguridad Informática** (los "CSIRT" Nacional, de la Defensa Nacional y Sectoriales). En lo que refiere a la Agencia Nacional de Ciberseguridad, corresponderá a un servicio público técnico y especializado con facultades normativas, fiscalizadoras y sancionatorias. La Agencia regulara las acciones de los organismos de la Administración del Estado y las instituciones privadas en materia de ciberseguridad.
• **Operadores de importancia vital.** La Agencia deberá determinar los servicios que sean esenciales e identificará dentro de estos a los operadores de importancia vital, de conformidad a los criterios establecidos en la ley. Estas entidades están sujetas a deberes específicos, entre los cuales se encuentra la obligación de implementar sistemas de gestión de seguridad de la información, elaborar y mantener planes de continuidad operacional y designar un delegado de ciberseguridad, entre otros.
• **Deberes generales.** El proyecto obligará a todos los organismos del Estado y a las instituciones privadas adoptar las medidas necesarias

Esta alerta legal es proporcionada por Carey y Cía. Ltda. con fines educativos e informativos únicamente y no pretende ni debe interpretarse como asesoría legal.

Carey y Cía. Ltda.
Isidora Goyenechea 2800, Piso 43.
Las Condes, Santiago, Chile.
www.carey.cl

para prevenir, reportar y resolver incidentes de ciberseguridad; a gestionar los riesgos asociados; y a contener y mitigar el impacto que pudieran tener los incidentes sobre la continuidad operacional, la confidencialidad y la integridad de los servicios prestados. Además, se establece la prohibición de realizar pagos de cualquier tipo por rescate ante ataques de secuestro digital o ransomware.

• **Deber de reportar incidentes de ciberseguridad y ciberataques.** Todas las entidades, sean públicas o privadas, con excepción de aquellas eximidas por la Agencia, deberán reportar en un plazo de 3 horas, al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos. Asimismo, deberán informar acerca de su plan de acción tan pronto como lo hubieren adoptado.

• **Infracciones y sanciones asociadas.** El proyecto contempla un catálogo de infracciones que se dividen en leves, graves y gravísimas, con multas que ascienden a hasta las 20.000 UTM.

Autores: Guillermo Carey; José Ignacio Mercado; Iván Meleda