Marzo, 2022

PROYECTO SOBRE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA DE LA INFORMACIÓN INICIA TRAMITACIÓN EN EL SENADO

Con fecha 15/03/2022, ingresó a tramitación en el Senado el Proyecto de Ley que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.

El proyecto, ingresado mediante Mensaje, se estructura alrededor de diez títulos y cuarenta y un artículos, junto con siete artículos transitorios, y tiene como objetivo:

"*Establecer la institucionalidad, los principios y la normativa general que permiten estructurar, regular y coordinar las acciones de ciberseguridad de los órganos de la Administración del Estado y entre éstos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los órganos del Estado así como los deberes de las instituciones privadas que posean infraestructura de la información calificada como crítica y, en ambos casos, los mecanismos de control, supervisión, y de responsabilidad por la infracción de la normativa.*"

Así, el proyecto de ley marco establece una serie de definiciones y principios, pero también tiene un fuerte enfoque institucional, creando la **Agencia Nacional de Ciberseguridad**, estableciendo sus obligaciones y su orgánica básica institucional (art. 8), así como la institucionalidad y división de la labor tanto del **Consejo Técnico de la Agencia Nacional de Ciberseguridad** y de los diversos **CSIRTs (Equipos de Respuesta a Incidentes de Seguridad Informática)**, los cuales se organizan por área, pudiendo ser sectoriales (constituidos por fiscalizadores o reguladores sectoriales respecto de sus respectivas áreas), o del sector público (CSIRT Nacional, de Gobierno y de Defensa.)

Además de esto, el proyecto incluye criterios y lineamientos para la determinación de **infraestructura crítica de la información**, lo que conlleva obligaciones específicas para las entidades que la manejan, sean públicas o privadas, debiendo, por ejemplo "*aplicar permanentemente las medidas de seguridad tecnológica, organizacionales, físicas e informativas necesarias para prevenir, reportar y resolver incidentes de ciberseguridad y gestionar los riesgos, así como contener y mitigar el impacto sobre la continuidad operacional, la confidencialidad de integridad del servicio prestado*".

Es importante destacar que el proyecto da particular importancia a la regulación y fiscalización 'sectorial', incluso reconociendo la potestad de los reguladores y fiscalizadores sectoriales de dictar normas de carácter general, circulares, normas técnicas, etcétera, con tal de establecer los estándares de ciberseguridad, las que deberán considerar los estándares de la Agencia Nacional de Ciberseguridad (art. 7)

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

Finalmente, el proyecto también contempla la creación de un Registro Nacional de Incidentes de Seguridad (art. 16), en el cual ingresarán los datos técnicos y antecedentes necesarios para describir la ocurrencia de un incidente de seguridad, con su análisis de estudio. Dicha información tendrá carácter de reservado. Respecto de los CSIRTs (sean estos sectoriales o del sector público) se establece también un deber de reserva de la información importante que se extiende incluso a funcionarios y personas que hayan tomado conocimiento de información sensible que no sean parte de la Agencia.)

AUTORES: *Guillermo Carey, José Ignacio Mercado.*