13 de diciembre de 2023

Congreso Nacional aprueba el Proyecto de Ley Marco sobre Ciberseguridad

Con fecha 12 de diciembre de 2023, la Cámara de Diputadas y Diputados aprobó en segundo trámite constitucional el proyecto de ley que "*Establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información*" (el "Proyecto"). En la misma fecha, el Proyecto se remitió al Senado y avanzó a tercer trámite constitucional, siendo aprobadas todas las modificaciones de la cámara revisora. De esta forma, el Proyecto se remitirá al Presidente de la República para su promulgación, sin perjuicio del control preventivo que debe efectuar el Tribunal Constitucional.

Los principales objetos del Proyecto son 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 para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad y ciberataque.

El Proyecto implica una serie de aspectos y cambios relevantes en materia de ciberseguridad. A continuación, destacamos algunos de ellos:

I. *Crea una nueva institucionalidad*

El Proyecto contempla la creación de nuevas instituciones en materia de ciberseguridad, disponiendo la creación de la Agencia Nacional de Ciberseguridad ("ANCI"), el Consejo Multisectorial sobre Ciberseguridad, el Comité Interministerial sobre Ciberseguridad y distintos Equipos de Respuesta a Incidentes de Seguridad Informática ("CSIRT"), entre ellos el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática, el Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional y los otros CSIRT que pertenezcan a organismos de la Administración del Estado.

En lo que refiere a la ANCI, esta autoridad estará encargada, entre otras cosas, de asesorar al Presidente de la República en materias propias de ciberseguridad, de colaborar en la protección de los intereses nacionales en el ciberespacio, de coordinar el actuar de las instituciones con competencia en materia de ciberseguridad, de velar por la protección, promoción y respeto del derecho a la seguridad informática, y de coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad. Para cumplir sus funciones, la ANCI contará con facultades normativas, fiscalizadoras y sancionatorias.

A modo ilustrativo, entre otras atribuciones, a la ANCI se le confieren facultades de "*dictar los protocolos y estándares que señala el artículo 7*" y "*las instrucciones generales y particulares, de carácter obligatorio, para las instituciones, tanto públicas como privadas obligadas por la presente ley*" (facultades normativas); facultades de "*fiscalizar el cumplimiento de las disposiciones de esta ley, sus reglamentos, protocolos, estándares técnicos y las instrucciones generales y particulares que emita la Agencia […]*" (facultades fiscalizadoras); y facultades de "*instruir el inicio de procedimientos sancionatorios y sancionar las infracciones e incumplimientos en que incurran las instituciones obligadas por la presente ley […]*".

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

Asimismo, el Proyecto contempla mecanismos de coordinación regulatoria entre la ANCI y entidades sectoriales en el caso de que los protocolos, estándares técnicos o instrucciones de carácter general que dicte en el ejercicio de sus funciones tengan efectos en las áreas de competencia de dichas entidades sectoriales. De la misma forma, las autoridades sectoriales podrán emitir normativas generales, técnicas e instrucciones necesarias para fortalecer la ciberseguridad en las instituciones de su sector, en conformidad con la regulación respectiva y en coordinación con la ANCI.

II. *Establece principios en materia de ciberseguridad*

El Proyecto introduce varios principios que las instituciones obligadas deberán observar en su conducta. Entre los principios que contempla el Proyecto de Ley Marco es posible destacar los siguientes:

1. Principio de control de daños. Este principio exige que, frente a un ciberataque, frente a un ciberataque o a un incidente de ciberseguridad, se deberá actuar coordinada y diligentemente, adoptando las medidas necesarias para evitar la escalada del ciberataque o del incidente de ciberseguridad y su posible propagación a otros sistemas informáticos.
2. Principio de cooperación con la autoridad. En aplicación de este principio, para resolver los incidentes de ciberseguridad se deberá prestar la cooperación debida con la autoridad competente y, si es necesario, cooperar entre diversos sectores, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios.
3. Principio de respuesta responsable. En virtud de este principio, la aplicación de medidas para responder a incidentes de ciberseguridad o ciberataque en ningún caso podrá significar la realización de, o el apoyo a, operaciones ofensivas.
4. Principio de seguridad informática. Este principio exige que toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere necesarias, incluyendo el cifrado.
5. Principio de racionalidad. En aplicación de este principio, las medidas para la gestión de incidentes de ciberseguridad, las obligaciones de ciberseguridad y el ejercicio de las facultades de la Agencia deberán ser necesarias y proporcionales al grado de exposición a los riesgos, así como al impacto social y económico que tendría.
6. Principio de seguridad y privacidad por defecto. En virtud de este principio, los sistemas informáticos, aplicaciones y tecnologías de la información deben diseñarse, implementarse y gestionarse teniendo en cuenta la seguridad y la privacidad de los datos personales que procesan.

III. *Ámbito de aplicación: servicios esenciales y operadores de importancia vital*

El Proyecto aplicará a las instituciones que presten servicios calificados como “esenciales” y a aquellas que sean calificadas como “operadores de importancia vital”.

El Proyecto establece que son servicios esenciales:

1. Aquellos que son provistos por los Órganos de la Administración del Estado y por el Coordinador Eléctrico Nacional, así como los que son prestados bajo concesión de servicio público; y
2. Aquellos que son proveídos por instituciones privadas que realicen las siguientes actividades:
    a. Generación, transmisión o distribución eléctrica;
    b. Transporte, almacenamiento o distribución de combustibles; suministro de agua potable o saneamiento;
    c. Telecomunicaciones;

d Infraestructura digital;

e Servicios digitales, servicios de tecnología de la información gestionados por terceros;

f Transporte terrestre, aéreo, ferroviario o marítimo, así como la operación de su infraestructura respectiva;

g Banca, servicios financieros y medios de pago;

h Administración de prestaciones de seguridad social;

i Servicios postales y de mensajería;

j Prestación institucional de salud por entidades tales como hospitales, clínicas, consultorios y centros médicos;

k Producción y/o investigación de productos farmacéuticos.

La ANCI podrá calificar otros servicios como esenciales mediante resolución fundada del o la Directora Nacional cuando su afectación puede causar un grave daño a la vida o integridad física de la población o a su abastecimiento, a sectores relevantes de las actividades económicas, al medioambiente, al normal funcionamiento de la sociedad, de la Administración del Estado, a la defensa nacional, o a la seguridad y el orden público.

Por su parte, corresponderá a la ANCI determinar a los prestadores de servicios esenciales que sean calificados como operadores de importancia vital mediante una resolución fundada, que cumplan con los siguientes requisitos: *(i)* que la provisión de dicho servicio dependa de las redes y sistemas informáticos; y *(ii)* que la afectación, interceptación, interrupción o destrucción de sus servicios tenga un impacto significativo en la seguridad y el orden público; en la provisión continua y regular de servicios esenciales; en el efectivo cumplimiento de las funciones del Estado; o, en general, de los servicios que éste debe proveer o garantizar.

Asimismo, la ANCI tendrá la facultad de calificar a instituciones privadas que, aunque no tengan la calidad de prestadores de servicios esenciales, reúnan igualmente los requisitos establecidos en el párrafo anterior bajo determinados supuestos.

IV. *Obligaciones de seguridad*

El Proyecto distingue entre deberes y obligaciones de carácter general, y aquellos específicos que deben ser cumplidos por las entidades que sean calificadas como operadores de importancia vital.

1 Deberes generales para aquellos prestadores de servicios esenciales y operadores de importancia vital.

a **Obligación de reportar.** Por un lado, se dispone que todos los servicios esenciales y operadores de importancia vital tendrán la obligación de reportar al CSIRT Nacional dentro de un plazo máximo de 3 horas los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos, de conformidad con los criterios que establece el Proyecto.

b **Otras obligaciones.** Por otro lado, el Proyecto también establece que todas las instituciones obligadas deberán aplicar de manera permanente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad, agregando que estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso. Además, debe tenerse presente que el cumplimiento de esas obligaciones exige la debida implementación de los protocolos y estándares establecidos por la ANCI, así como de los estándares particulares de ciberseguridad dictados de conformidad a la regulación sectorial respectiva, para prevenir y gestionar los riesgos asociados a la ciberseguridad, la contención y mitigación del impacto que los incidentes pueden tener sobre la continuidad operacional del servicio prestado o la confidencialidad, y la integridad de la información o de las redes o

sistemas informáticos.Cabe hacer presente que el contenido preciso de estas obligaciones no está cabalmente determinado en el Proyecto y es probable que aquél se precisará únicamente con las normas que dicte la ANCI en el futuro y las autoridades sectoriales respectivas, según corresponda.

2. Deberes específicos para los operadores de importancia vital:El Proyecto dispone que los operadores de importancia vital están sujetos a deberes específicos, entre los cuales se encuentra la obligación de implementar sistemas de gestión de seguridad de la información continuos; elaborar y mantener planes de continuidad operacional y ciberseguridad, los que deberán certificarse y someterse a revisiones periódicas; realizar continuamente operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos y sistemas; informar a los potenciales afectados sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos; designar un delegado de ciberseguridad, entre otros deberes específicos.

V. *Establece infracciones y sanciones asociadas*

El Proyecto establece una serie de sanciones ante la infracción a las disposiciones de la futura ley. La ANCI será la encargada de sancionar dichas infracciones, sin perjuicio de la facultadas de la autoridad sectorial respectiva para conocer y sancionar las infracciones, así como ejecutar las sanciones, a la normativa sobre ciberseguridad que hubiere dictado y cuyos efectos sean al menos equivalentes al de la normativa dictada por la ANCI.

Cabe destacar que el Proyecto clasifica las infracciones en infracciones leves, graves y gravísimas, además de establecer infracciones específicas para los operadores de importancia vital. A continuación, destacamos algunas infracciones que contempla el Proyecto:

1. Se consideran infracciones leves el (i) entregar fuera de plazo la información que se le requiera cuando ella no fuere necesaria para la gestión de un incidente de ciberseguridad; (ii) incumplir las instrucciones generales o particulares impartidas por la ANCI en los casos que no esté sancionado como infracción grave o gravísima; y (iii) cualquier infracción de las obligaciones de la futura ley que no tengan señalada una sanción especial.
2. Se consideran infracciones graves el (i) no haber implementado los protocolos y estándares establecidos por la ANCI para prevenir, reportar y resolver incidentes de ciberseguridad; (ii) no haber implementado los estándares particulares de ciberseguridad; (iii) entregar fuera de plazo la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de ciberseguridad; (iv) entregar a la ANCI de información manifiestamente falsa o errónea; (v) incumplir la obligación de reportar; (vi) negarse injustificadamente a cumplir una instrucción de la ANCI o entorpecer deliberadamente el ejercicio de las atribuciones de la ANCI durante la gestión de un incidente de ciberseguridad, siempre que la atribución no cuente con una sanción especial; y (vii) la reincidencia en una misma infracción leve dentro de un año.
3. Se consideran infracciones gravísimas el (i) entregar a la ANCI información manifiestamente falsa o errónea, cuando ella sea necesaria para la gestión de un incidente de ciberseguridad; (ii) incumplir las instrucciones generales o particulares impartidas por la ANCI durante la gestión de un incidente de impacto significativo; (iii) no entregar la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de impacto significativo; y (iv) la reincidencia en una infracción grave dentro de un año.

En cuanto a los montos, las infracciones leves serán sancionadas con multa de hasta 5.000 Unidades Tributarias Mensuales ("UTM"), pudiendo llegar hasta 10.000 UTM si el infractor es operador de importancia vital; las infracciones graves serán sancionadas con multa de hasta 10.000 UTM, pudiendo alcanzar las 20.000 UTM si el infractor es operador de importancia vital; y, finalmente, las infracciones gravísimas serán sancionadas con multa de hasta 20.000 UTM, pudiendo llegar a 40.000 UTM si el infractor es operador de importancia vital. En consecuencia, las sanciones podrían ascender hasta casi 3 millones de dólares.

VI. *Entrada en vigencia*

El Presidente de la República deberá dictar, dentro del plazo de un año de publicada la futura ley, uno o más decretos con fuerza de ley para determinar un período para la vigencia de las normas de la futura ley, el cual no podrá ser inferior a seis meses desde la publicación de la futura ley, la fecha de iniciación de las actividades de la ANCI, entre otras materias.

AUTORES: *Guillermo Carey, José Ignacio Mercado, Iván Meleda, Jorge Gatica.*