Biblioteca del Congreso Nacional de Chile

Descripción del proyecto que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información (Boletín N° 14.847-06)

Serie Minutas Nº 81-22, 10-11-2022

por Víctor Soto Martínez

Resumen

Se describen los elementos centrales del proyecto de ley que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información (Boletín N° 14.847-06) y se realizan diversos comentarios generales a la institucionalidad y la normativa que allí se establece.

Departamento de Estudios, Extensión y Publicaciones - Biblioteca del Congreso Nacional
eMail: vsoto@bcn.cl, Anexo: 1877

TABLA DE CONTENIDOS

1. Ficha técnica del proyecto de ley

Número de Boletín	14.847-06
Fecha de ingreso	15 de marzo de 2022
Iniciativa	Mensaje
Cámara de origen	Senado
Estado de tramitación	Primer trámite constitucional
Urgencia	Suma

Cabe mencionar que, a la fecha de la presente minuta, el proyecto de ley ya ha sido revisado por la Comisión de Defensa y por la Comisión de Seguridad Pública del Senado, y el día 18 de octubre de 2022 fue aprobado en la Sala en general. En dicha ocasión, por lo demás, la Sala acordó que la tramitación en particular sea llevada por ambas comisiones unidas. Asimismo, se fijó como plazo máximo para ingresar indicaciones el 11 de noviembre de 2022.

2. Descripción del proyecto de ley

2.1. Objeto. Se fijan tres objetivos generales:

i) definir la institucionalidad, los principios y la normativa que regirán las acciones de ciberseguridad de los órganos de la Administración del Estado y la relación entre éstos y los particulares;

ii) establecer los requisitos mínimos para la prevención, contención, resolución y respuesta frente a los incidentes de ciberseguridad que se generen;

iii) establecer las atribuciones y obligaciones tanto de los órganos del Estado como de las instituciones privadas que posean infraestructura crítica de la información, estableciendo mecanismos de control y un sistema de infracciones y sanciones.

Un punto a destacar, por tanto, es que la ley no sólo regulará a la Administración, sino también a los privados que posean infraestructura crítica de la información.

2.2. Definiciones. Al tratarse de una ley que aborda un tema muy técnico, la necesidad de definiciones claras es evidente. De ahí que el proyecto establezca una serie de definiciones, de las cuales destacaremos las que nos parecen más relevantes para la comprensión de la ley. Así, por ejemplo, se define "ciberataque" como una "acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan" (art. 2, N° 2).

Por otra parte, la "ciberseguridad" sería "el conjunto de acciones destinadas al estudio y manejo de las amenazas y riesgos de incidentes de ciberseguridad; a la prevención, mitigación y respuesta frente a estos, así como para reducir sus efectos y el daño causado, antes, durante y después de su ocurrencia, respecto de los activos informáticos y de servicios" (art. 2, N° 4). En rigor, aquí no se está definiendo la ciberseguridad, sino que se la está describiendo en términos de manejo y mitigación de los incidentes que la comprometen. Este punto crítico será analizado con mayor detalle en los comentarios.

También hay definiciones como "sistema de información", "riesgo", "vulnerabilidad", "servicio informático", etc., y otras como "infraestructura crítica de la información". Esta última es relevante por cuanto se encuentra en la base de los objetivos planteados por el proyecto de ley. Así, se define como "aquellas instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación de servicio, interceptación, interrupción o destrucción puede tener una repercusión importante en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que éste debe proveer o garantizar" (art. 2, N° 9).

Otra definición interesante, por sus efectos prácticos, es la de "servicios esenciales": "todo servicio respecto del cual la afectación, degradación, denegación de servicio, interceptación, interrupción o destrucción de su infraestructura de la información pueda afectar gravemente: a) La vida o integridad física de las personas; b) La provisión de servicios sanitarios, energéticos o de telecomunicaciones; c) Al normal funcionamiento de obras públicas fiscales y medios de transporte; d) A la generalidad de usuarios o clientes de sistemas necesarios para operaciones financieras, bancarias, de medios de pago y/o que permitan la transacción de dinero o valores; y e) De modo general, el normal desarrollo y bienestar de la población" (art. 2, N° 15).

Finalmente, cabe destacar la definición de CSIRT, sigla que se utiliza bastante en el proyecto y que significa literalmente *Computer Security Incident Response Team*. El proyecto de ley la traduce adecuadamente como "Equipo de respuesta a incidentes de seguridad informática". Se trata de centros "conformados por especialistas multidisciplinarios capacitados para prevenir, detectar, gestionar y responder a incidentes de ciberseguridad" (art. 2, N° 5).

2.3. Principios rectores. Se enumeran y definen varios principios rectores que regirán las acciones de ciberseguridad de los órganos de la Administración, entre los cuales cabe destacar:

-**Responsabilidad,** en cuya virtud la seguridad de las redes, sistemas y datos es de responsabilidad de aquel que las ofrece u opera, *con independencia de la naturaleza pública o privada del organismo* (art. 3, N° 1);

-**Confidencialidad de los sistemas de información,** en virtud del cual los datos, conectividad y sistemas deberán ser exclusivamente accedidos por personas o entidades autorizadas a tal efecto (art. 3, N° 3);

-**Integridad de los sistemas informáticos y de la información,** que indica que los datos y elementos de configuración de un sistema sólo podrán ser modificados por personas autorizadas en el ejercicio de sus funciones o por sistemas que cuenten con la autorización respectiva (art. 3, N° 4); y

-**Control de daños,** en virtud del cual los órganos del Estado y aquellas instituciones privadas que posean infraestructura de la información calificada como crítica, en el caso de un incidente de ciberseguridad o de un ciberataque, deben siempre actuar diligentemente y adoptar las medidas necesarias para evitar la escalada del incidente de ciberseguridad o del ciberataque y su posible propagación a otros sistemas informáticos, notificando de igual forma el incidente de ciberseguridad al CSIRT respectivo (art. 3, N° 6).

2.4. Calificación de infraestructura como crítica. Se le asigna al **Ministerio del Interior y Seguridad Pública** la atribución de hacer esta calificación (mediante un decreto "expedido por orden del Presidente de la República"[1]), luego de haber recibido un informe del Consejo Técnico de la **Agencia Nacional de Ciberseguridad** que a su vez debe considerar los factores indicados en el art. 4 de la ley. Con todo, esta es la definición clave: "se entenderá que poseen infraestructura crítica de la información todos los órganos del Estado, incluidas las municipalidades, las entidades fiscales autónomas, las empresas del Estado o aquellas en las que el Fisco tenga intervención por aportes de capital" (art. 4, inc. Final).

2.5. Deberes específicos de instituciones con infraestructura crítica. Se enumeran diversos deberes, como, por ejemplo, **implementar un sistema de gestión de riesgo permanente**, mantener un registro de las acciones ejecutadas que compongan el sistema de gestión de riesgos, elaborar e implementar **planes de continuidad operacional y ciberseguridad**, etc.

[1] Se trata de una variación del decreto supremo, es decir, de una orden escrita dictada por el Presidente de la República sobre asuntos propios de su competencia. La diferencia es que, en estos casos, se autoriza al Ministro a dictar el decreto, pero siempre que el documento lleve la alocución "Por orden del Presidente de la República" (art. 3, de la ley N° 19.880, que establece las bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado).

2.6. Institucionalidad. Aquí lo más importante es la creación de la **Agencia Nacional de Ciberseguridad**, como un servicio público descentralizado, cuyo objeto será asesorar al Presidente de la República en materias propias de ciberseguridad, y que se relacionará con éste a través del Ministerio del Interior (art. 8). Su domicilio estará en Santiago, pero podrá tener oficinas en regiones.

Su principales atribuciones serán: asesorar al Presidente de la República, en el análisis y definiciones de la política nacional de ciberseguridad; dictar normas técnicas de carácter general y los **estándares mínimos de ciberseguridad** e impartir instrucciones particulares para los órganos de la Administración del Estado y para los privados cuya infraestructura de la información sea calificada como crítica *y no se encuentren sometidos a la regulación o fiscalización de un regulador o fiscalizador sectorial*; administrar el **Registro Nacional de Incidentes de Ciberseguridad**; prestar asesoría técnica a los órganos del Estado e instituciones privadas con infraestructura crítica, que estén o se hayan visto afectados por un incidente de ciberseguridad; fiscalizar y sancionar el cumplimiento de esta ley, sus reglamentos y su normativa técnica, *cuando ello no corresponda a un regulador o fiscalizador sectorial*. También se le encomienda fomentar la formación ciudadana en el tema, coordinar a los CSIRT Sectoriales y al CSIRT Nacional, en lo relativo a los estándares y tiempos de comunicación de incidentes de ciberseguridad o vulnerabilidades, fomentar la investigación en la materia (en conjunto con el Ministerio de Ciencias), etc.

La Agencia será dirigida por una autoridad unipersonal, sujeta al sistema de alta dirección pública (art. 10), al igual que todos sus altos directivos (se puede colegir, por tanto, que es un servicio adscrito a la Alta Dirección Pública).

Dentro de la estructura del servicio habrá un **Consejo Técnico**, que tendrá como objeto asesorar y apoyar técnicamente a la Agencia en el análisis y revisión periódica de las políticas públicas propias de su ámbito de competencia, en el estudio de las amenazas existentes y potenciales en el ámbito de ciberseguridad y proponer posibles medidas para abordarlas. Estará compuesto por el propio Director y **cuatro consejeros designados por el Presidente de la República**, mediante decreto supremo expedido a través del Ministerio del Interior y Seguridad Pública, quienes permanecerán en su cargo durante seis años, pudiendo ser reelegidos en sus cargos por una sola vez (art. 17).

También se crea legalmente -porque ya existe actualmente un órgano creado por decreto-, dentro de la Agencia Nacional de Ciberseguridad, el **Equipo Nacional de Respuesta ante Incidentes de Seguridad Informática** (CSIRT Nacional). Sus principales funciones serán: responder ante incidentes de ciberseguridad o ciberataque que vulneren o pongan en riesgo las instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información relativos a instituciones privadas con infraestructura crítica y que no estén sometidas a un regulador o fiscalizador sectorial; coordinar a los CSIRT Sectoriales frente a ataques, vulnerabilidades, incidentes y brechas de ciberseguridad; y servir de punto de enlace con CSIRT extranjeros o sus equivalentes, etc. (art. 22).

Cabe señalar que los reguladores o fiscalizadores sectoriales podrán constituir **CSIRT Sectoriales**, los que tendrán por finalidad dar respuesta a vulnerabilidades e incidentes de ciberseguridad que pongan en riesgo las instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información de sus respectivos sectores regulados (art. 23). Dentro de la misma Agencia habrá un CSIRT de Gobierno (a pesar de su nombre, que podría sugerir un grupo acotado de instituciones, se refiere a los diversos órganos del Estado), que se clasificará como un CSIRT sectorial (art. 27) y un CSIRT de Defensa (art. 28).

Por otro lado, se crea un **Comité Interministerial de Ciberseguridad**, cuya función será asesorar al Ministro del Interior y Seguridad Pública en materias de ciberseguridad relevantes para el funcionamiento de los órganos de la Administración del Estado y de los servicios esenciales. Estará integrado por 14 personas: los subsecretarios de Interior (quien lo presidirá), Defensa, Justicia, Relaciones Exteriores, Segpres, Telecomunicaciones, Hacienda, Economía y Empresas de Menor Tamaño, Minería, Energía y Ciencia, Tecnología, Conocimiento e Innovación; por los directores de la Agencia Nacional de Inteligencia y de la Agencia Nacional de Ciberseguridad; y, finalmente, por un representante de la Subsecretaría del Interior, experto en materias de ciberseguridad. La secretaría ejecutiva radicará en la Agencia Nacional de Ciberseguridad (véase arts. 36, 37 y 38 del proyecto).

Finalmente, en lo relativo a la institucionalidad, cabe destacar que existirá un **Registro Nacional de Incidentes de Ciberseguridad.** Aquí se ingresarán los datos técnicos y antecedentes necesarios para describir la ocurrencia de incidentes de ciberseguridad, con su análisis y estudio. Sobre la base de este registro se podrán realizar las respetivas investigaciones por parte de la Agencia, así como comunicar las alertas a los CSIRT Sectoriales, a los órganos del Estado señalados en el inciso final del artículo 4º y a las instituciones privadas que posean infraestructura crítica (art. 16).

2.6. Reserva de información. Se consideran secretos y de circulación restringida, los antecedentes, datos, informaciones y registros que obren en poder de los CSIRT, o de su personal, cualquiera que sea su cargo o la naturaleza de su vinculación jurídica con éstos. Asimismo, tendrán dicho carácter aquellos otros antecedentes respecto de los cuales el personal de tales órganos de la Administración del Estado tome conocimiento en el desempeño de sus funciones o con ocasión de éstas (art. 29). Adicionalmente, serán considerada como información secreta o reservada, la siguiente: i. Las matrices de riesgos de ciberseguridad; ii. Los planes de continuidad operacional y planes ante desastres; iii. Los planes de acción y mitigación de riesgos de ciberseguridad y, iv. Los reportes de incidentes de ciberseguridad.

La obligación de guardar secreto regirá, además, para aquellos que, sin ser funcionarios de la Agencia, tomaren conocimiento de las solicitudes para la ejecución de procedimientos especiales de obtención de información, de los antecedentes que las justifiquen y de las resoluciones judiciales que se dicten al efecto (art. 30).

2.7. Infracciones y sanciones. Serán consideradas infracciones para efectos de esta ley:

a) Retardar o entregar fuera del plazo señalado la información a la autoridad u órgano de la Administración del Estado habilitado para requerirla;

b) Negar injustificadamente información a la autoridad u órgano de la Administración del Estado habilitado para requerirla;

c) Entregar maliciosamente información falsa o manifiestamente errónea, e;

d) Incumplir los deberes previstos en el párrafo 2° del Título II.

En cuanto a las sanciones, podrán imponerse, a beneficio fiscal, multas entre 10 y 20.000 Unidades Tributarias Mensuales, de conformidad a la gravedad de la infracción. Para determinar la cuantía de la multa, se entenderá por:

a) Faltas gravísimas: aquellas señaladas en los literales b) y c) del inciso precedente. En este caso, la multa será de hasta a 20.000 Unidades Tributarias Mensuales.

b) Faltas graves: aquellas señaladas en el literal a) del inciso precedente. En este caso, la multa será de hasta 10.000 Unidades Tributarias Mensuales.

c) Faltas leves: aquellas obligaciones señaladas en esta ley cuyo incumplimiento negligente o injustificado no tenga señalada una sanción especial, caso en el que la multa será de 10 a 5.000 Unidades Tributarias Mensuales.

Un punto importante a notar en lo relativo a las sanciones es que, de conformidad al artículo 33, cuando las conductas constitutivas de infracción descritas en la presente ley posea una sanción mayor en una ley especial que rige a un sector regulado, se preferirá a aquella por sobre ésta.

2.8. Procedimiento. Las sanciones serán impuestas por resolución del Director de la Agencia Nacional de Ciberseguridad. Para ello se ordena la creación de un procedimiento sancionatorio *ad hoc*, establecido en un reglamento dictado por el Ministerio del Interior y Seguridad Pública. Por cierto, este procedimiento deberá fundarse en un procedimiento racional y justo y cumplir una serie de principios establecidos en el artículo 34 del proyecto de ley.

2.9. Modificaciones a otras normas. La única es la incorporación de una nueva atribución para el Jefe del Estado Mayor: "k) Conducir el Centro Coordinador CSIRT del Sector Defensa en coordinación con la Subsecretaría de Defensa" (art. 25 de la ley Nº 20.424, Estatuto Orgánico del Ministerio de Defensa Nacional).

2.10. Transitorias. Se establecen normas para la creación de la Agencia, para la definición de su presupuesto y para el funcionamiento intermedio de los órganos públicos mientras se crean los CSIRT sectoriales.

3. Comentarios

Lo primero que debemos destacar de este proyecto de ley es que se centra en la creación de una institucionalidad robusta para enfrentar el problema de la ciberseguridad. Actualmente, el país cuenta con diversos equipos de respuesta frente a incidentes de ciberseguridad en los órganos públicos, incluido un *Equipo de Respuesta ante Incidentes de Seguridad Informática*, dependiente de la Subsecretaría del Interior, del Ministerio del Interior, creado el año 2018 y que se encuentra regulado en la Resolución Exenta N° 5.006, de 2019[2]. Sin embargo, no existe aún un sistema ni una institucionalidad permanente y de alcance general que permita enfrentar el problema de manera coordinada. En este sentido, la creación de una Agencia Nacional, descentralizada, que contribuya a la configuración de una política nacional en la materia (política que, a su vez, pasaría a formar parte integral del conjunto de políticas a ser definidas por los diversos gobiernos y no un esfuerzo aislado de cada gobierno), además de la institucionalización de los equipos de respuesta nacional y sectoriales (entre los cuales se cuenta uno de gobierno y uno de defensa), constituye un esfuerzo decidido en esa línea.

Ahora bien, en cuanto al articulado más específico, es importante detenerse por un momento en las definiciones. Por un lado, estas pueden ser útiles para la adecuada comprensión de la ley –que abarca diversos tecnicismos que pueden escapar al conocimiento de la ciudadanía-; pero, por otro lado, es necesario que ellas no se conviertan en una limitación para la elaboración de las políticas. Es decir, se debe buscar un equilibrio entre precisión y amplitud. En este sentido, llama la atención la definición que se hace de ciberseguridad. En realidad, estamos frente a una descripción de la ciberseguridad como respuesta frente a incidentes de ciberseguridad, lo que da cuenta de un concepto circular, que no explica mucho el fenómeno (oscureciendo, por tanto, los objetivos de política pública que el mismo proyecto señala).

Desde otra perspectiva, podríamos entender a la ciberseguridad como seguridad digital o seguridad frente a los ciberataques –adecuadamente definidos en el proyecto como acciones que comprometen los *sistemas de información y telecomunicaciones* o las infraestructuras que las soportan- o, de forma más general, como "una condición caracterizada por un mínimo de riesgos para el ciberespacio, entendido como el conjunto de infraestructuras físicas, lógicas y las interacciones humanas que allí ocurren. En este conjunto (…) los atributos claves a proteger son la confidencialidad, integridad y disponibilidad de la información"[3]. Esta definición tiene la virtud de poner

[2] Véase: https://www.csirt.gob.cl/media/2019/09/RES.-EXENTA-N-5006-CREACION-DE-DIVISION-Y-UNIDAD.pdf [consultado el 25-06-2021]

[3] Véase: GOBIERNO DE CHILE. *Política Nacional de Ciberseguridad (2017-2022)*, p. 16. Puede consultarse en línea: https://biblioteca.digital.gob.cl/bitstream/handle/123456789/738/Pol%C3%ADtica%20Nacional%20de%20Ciberseguridad.pdf?sequence=1 [consultado el 10-11-2022]. Cabe señalar que la definición de "ciberespacio" del proyecto de ley no difiere en lo sustantivo de esta definición más general ofrecida por la Política Nacional: "Dominio global y dinámico dentro del entorno de la información que corresponde al ambiente compuesto por las infraestructuras tecnológicas, los

el foco principal en la información y, por ende, en los datos de las personas que utilizan y acceden a los sistemas informáticos, cuestión que no se vislumbra directamente en la definición dada por el proyecto en comento.

Otro punto importante, relativo ahora a los principios rectores, es que ellos debieran entenderse de forma armónica y coordinada. Para reforzar esta interpretación, sería interesante contar con algún principio general, que permita enlazar a cada uno de estos principios.

Por otro lado, un punto que no queda absolutamente claro en el proyecto es la forma en que se fiscalizará y/o se hará el seguimiento de los planes de continuidad operacional y ciberseguridad que deberán elaborar las instituciones que tengan infraestructura crítica de la información.

En cuanto a las atribuciones de la Agencia es importante advertir que tendrá diversos niveles de atribuciones normativas. Por un lado, podrá dictar normas técnicas de carácter general y definir estándares mínimos de ciberseguridad. Estos últimos no obstan a la dictación, por parte de los órganos sectoriales, de estándares particulares para sus regulados, pero sí establecen el mínimo común que deberán considerar esos estándares (art. 7). Por otro lado, la Agencia también podrá dictar instrucciones, pero el alcance de estas es limitado, ya que sólo tendrán validez respecto de los órganos públicos y de aquellos privados con infraestructura crítica de la información que *no se encuentren sometidos a la regulación o fiscalización de un regulador o fiscalizador sectorial* (art. 9, b). Lo mismo ocurre respecto de su atribución de fiscalizar y sancionar el cumplimiento de la ley, sus reglamentos y su normativa técnica (art. 9, m).

Un último punto que llama la atención es la amplitud del ámbito de reserva de la información (art. 29). Por ejemplo, esta reserva incluye a los planes de manejo y mitigación de los incidentes, lo cual, si bien busca resguardar información clave para que los sistemas no sean intervenidos, también dificulta la fiscalización respecto del cumplimiento de estos planes. Asimismo, cabe señalar que toda ley que establezca espacios de reserva o secreto debe aprobarse por quórum calificado (art. 8 de la Constitución) y, en virtud de lo anterior, debiera ser revisada por el Tribunal Constitucional para asegurar un adecuado equilibrio entre el resguardo de la seguridad nacional y el derecho de acceso a la información pública.

Finalmente, es preciso indicar que esta ley establece un marco para la ciberseguridad, pero en ningún caso agota lo que debiera entenderse por ciberseguridad en nuestro sistema jurídico. Así, se puede sostener que el elemento central en la ciberseguridad-

componentes lógicos de la información, los datos (almacenados, procesados o transmitidos) que abarcan los dominios físico, virtual y cognitivo y las interacciones sociales que se verifican en su interior" (art. 2, N° 3). Se retienen aquí los elementos básicos, separándose los datos personales, que en la anterior definición se pueden entender como un elemento implícito. De esta forma, el ciberespacio quedaría estructurado en torno a la infraestructura tecnológica, los componentes lógicos de la información, los datos y las interacciones sociales.

la protección de la integridad de los datos de las personas- requiere del sustento de un verdadero ecosistema institucional. Este ecosistema vendría dado por diversas líneas de acción. En primer lugar, una adecuada definición de los ciberdelitos, lo que actualmente se resguarda mediante la ley N° 21.459, que actualiza la normativa penal y procesal penal de nuestro sistema, cumpliendo con las normas establecidas en el Convenio de Budapest[4]. En segundo lugar, el marco institucional que hemos analizado en esta minuta. Y, finalmente, la ley de protección de datos personales que actualmente se discute en el Congreso[5]. Esto último es clave, por cuanto son las personas el verdadero centro y objetivo de toda política pública en la materia. El marco institucional, por lo tanto, también debe entenderse orientado a su resguardo.

[4] Véase: SOTO, Víctor. "Análisis de la legislación, las políticas y las prácticas nacionales sobre ciberseguridad", Serie Minutas Nº 52-22, Biblioteca del Congreso Nacional, 2022.

[5] Chile ya cuenta con una ley de protección de datos personales (ley N° 19-628), pero ella se ha considerado insuficiente para resguardar muchas de las situaciones que se viven a partir de la digitalización del país. Para hacer frente a esta situación, se discute en el Congreso el proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (Boletín N° 11.144-07), actualmente en segundo trámite constitucional, en la Cámara de Diputados.