Biblioteca del Congreso Nacional de Chile

Descripción y síntesis de la ley N° 21.663, Ley Marco de Ciberseguridad

Serie Minutas Nº 48-24, 13-05-2024

por Víctor Soto Martínez

Resumen

Se describen los elementos centrales de la Ley Marco de Ciberseguridad (ley N° 21.663, ingresada como 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. Tramitación legislativa

La ley se originó como mensaje del Presidente de la República (boletín N° 14.847-06), y fue ingresado al Senado el 15 de marzo de 2022[1]. Luego de su revisión por la Comisión de Defensa y por la Comisión de Seguridad Pública del Senado, el día 18 de octubre de 2022 fue aprobado en la Sala del Senado en general. En dicha ocasión la Sala acordó que la tramitación en particular fuera llevada por ambas comisiones unidas. Finalmente, el proyecto de ley se aprobó en particular en el Senado el 26 de abril de 2023.

En la Cámara de Diputados, en tanto, fue revisada en primer lugar por la Comisión de Seguridad Ciudadana, y luego por la Comisión de Hacienda, aprobándose en general y particular, con modificaciones, el 12 de diciembre de 2023. En esta misma fecha se llevó a cabo el tercer trámite constitucional, en el Senado, donde se aprobaron todas las enmiendas introducidas por la Cámara. Finalmente, la ley fue promulgada el 26 de marzo de 2024 y publicada en el Diario Oficial el 8 de abril[2].

2. Descripción de la ley

2.1. Objeto

Se fijan cuatro objetivos generales (art. 1):

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 de las instituciones que presten servicios calificados como esenciales (según definición del art. 4, inc. 2° y 3°)[3] y aquellas que sean calificadas como operadores de importancia vital (según definición

[1] Si bien esta fue la fecha de ingreso, su elaboración original correspondió al gobierno del Presidente Sebastián Piñera.

[2] El Tribunal Constitucional declaró inconstitucional el inciso tercero del artículo 53, relativo a los regímenes especiales en materia de ciberseguridad, porque buscaba regular por vía legal en esta materia a órganos autónomos constitucionales (STC, Rol 15.043-23).

[3] Cabe señalar que, mientras el inciso segundo define los servicios que se considerarán esenciales, entre los que se cuentan los provistos por órganos de la Administración del Estado, los prestados bajo concesión de servicio público, y los proveídos por diversas instituciones privadas (como aquellas que se dedican a la generación, transmisión o distribución eléctrica, entre otras), el inciso tercero señala que la Agencia Nacional de Ciberseguridad (organismo que se crea en esta ley, como veremos más adelante) "podrá calificar otros servicios como esenciales mediante resolución fundada del Director o 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 y/o de la Administración del Estado, a la defensa nacional, o a la seguridad y el orden público".

de los arts. 5 y 6). Esta redacción se debe a que la normativa incluye no sólo a los servicios públicos, sino también a ciertas instituciones privadas que allí se especifican[4].

iv) definir mecanismos de control, supervisión y responsabilidad ante las infracciones a la ley.

2.2. Definiciones

Al tratarse de una ley que aborda un tema muy técnico, la necesidad de definiciones claras y operativas es evidente. De ahí que se 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 un "intento de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático" (art. 2, N° 5)[5].

Por otra parte, la "ciberseguridad" sería la "preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad" (art. 2, N° 6). En tanto, un incidente de ciberseguridad es "todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos" (art. 2, N° 10).

También hay definiciones como "riesgo", "vulnerabilidad", "red o sistema informático", etc. Esta última se entiende como un "conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales" (art. 2, N° 12).

Finalmente, cabe destacar la definición de CSIRT, sigla que se utiliza bastante en la ley 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 multidisciplinarios que tienen por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos" (art. 2, N° 9).

2.3. Principios rectores

Se enumeran y definen varios principios rectores que regirán las acciones de ciberseguridad de los órganos de la Administración y de los privados que presten

[4] En la redacción original del proyecto de ley se hablaba de instituciones que poseyeran "infraestructura crítica de la información".

[5] "Exfiltrar" es un término proveniente de la jerga militar que, aplicado al ámbito informático, se refiere a cuando se incurre en la copia, transferencia o recuperación no autorizadas de datos de un servidor o el computador de un individuo. Véase: https://www.proofpoint.com/es/threat-reference/data-exfiltration [consultado el 09-05-2024]

servicios esenciales o de importancia vital (según lo dispuesto en los artículos 4, 5 y 6), entre los cuales cabe destacar:

-**Control de daños,** en virtud del cual las instituciones indicadas, frente a un ciberataque o a un incidente de ciberseguridad, deberán actuar de forma coordinada y diligente, y adoptar las medidas necesarias para evitar su escalada y posible propagación a otros sistemas informáticos (art. 3, N° 1).

-**Cooperación con la autoridad**. Según este principio, para resolver los incidentes de ciberseguridad, se deberá prestar cooperación a la autoridad competente y, si es necesario, cooperar entre diversos sectores, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios (art. 3, N° 2).

-**Seguridad en el ciberespacio**. De acuerdo con este principio, el Estado velará por que todas las personas puedan participar de un ciberespacio seguro, por lo que otorgará especial protección a las redes y sistemas informáticos que contengan información de aquellos grupos de personas que suelen ser en mayor medida objeto de ciberataques (art. 3, N° 4).

-**Racionalidad**, en virtud del cual 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, y al eventual impacto social y económico (art. 3, N° 7).

-**Seguridad y privacidad por defecto y desde el diseño**. Este principio es relevante por cuanto implica que 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 (art. 3, N° 8).

2.4. Calificación de servicios como esenciales o de importancia vital

Como ya se ha indicado más arriba, se le entrega la atribución de realizar esta calificación a la **Agencia Nacional de Ciberseguridad** (en adelante, la Agencia), a través de una resolución fundada de su Director/a. Ya vimos que en el caso de los servicios esenciales hay una enumeración de servicios de este tipo (art. 4, inc. 2°), pero también pueden incorporarse otros servicios "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 y/o de la Administración del Estado, a la defensa nacional, o a la seguridad y el orden público".

En tanto, en el caso de las instituciones de importancia vital, se puede calificar así a quienes reúnan 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. Al igual que en el caso anterior, la Agencia puede calificar así a instituciones privadas que, aunque no tengan la calidad de prestadores de servicios esenciales, reúnan los dos requisitos antes indicados, cuando ello sea indispensable por haber adquirido un rol crítico en el abastecimiento de la población, la distribución de bienes o la producción de aquéllos indispensables o estratégicos para el país; o por el grado de exposición de la entidad a los riesgos y la probabilidad de incidentes de ciberseguridad, incluyendo su gravedad y las consecuencias sociales y económicas asociadas (art. 5).

Cada tres años la Agencia deberá revisar y actualizar la calificación de operadores de importancia vital mediante una resolución dictada por el Director o la Directora Nacional, previo proceso de consulta pública (art. 6).

2.5. Obligaciones de ciberseguridad

Las instituciones incluidas en los artículos 4 y 5 deberán tomar, de forma permanente, medidas de naturaleza tecnológica, organizacional, física o informativa, para prevenir, reportar y resolver incidentes de ciberseguridad, lo cual supone, por cierto, cumplir con los protocolos y estándares establecidos por la Agencia (art. 7).

Algunos de sus deberes más específicos son **implementar un sistema de gestión de seguridad continuo** (art. 8, a), mantener un registro de las acciones ejecutadas que compongan el sistema de gestión de seguridad de la información (art. 8, b), y elaborar e implementar **planes de continuidad operacional y ciberseguridad,** los que deberán ser certificados por parte de los centros de certificación que la Agencia acredite (art. 8, c). Asimismo, deberán obtener todas las **certificaciones** que determine la Agencia mediante reglamento (art. 8, f), vinculado con el art. 28) y designar un **delegado de ciberseguridad** para que actúe como contraparte de la Agencia e informe a la autoridad o jefatura (art. 8, i), entre otros.

Por otra parte, se establece un **deber general de reportar al CSIRT Nacional** los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos[6], con un esquema de plazos (art. 9). Para analizar esto con mayor detalle, véase el cuadro N° 1.

[6] El artículo 27 establece que un incidente tiene efecto significativo si "es capaz de interrumpir la continuidad de un servicio esencial o afectar la integridad física o la salud de las personas, así como en el caso de afectar sistemas informáticos que contengan datos personales", para lo cual se proponen diversos criterios, como el número de personas afectadas, entre otros.

Cuadro N° 1. Esquema de plazos para el deber de reportar (art. 9)

Acción	Tipo de institución	Plazo máximo
Envío de alerta temprana al CSIRT sobre ocurrencia del incidente	General	3 horas
Actualización de la información + evaluación inicial del incidente + indicadores de compromiso	Operador de importancia vital	24 horas en general
	General	72 horas
Plan de acción	Operador de importancia vital	7 días corridos
Informe final (descripción detallada del incidente, tipo de amenaza o probable causa principal, medidas de mitigación tomadas, repercusiones transfronterizas, si procede).		15 días corridos

Fuente: elaboración propia a partir de la ley

2.6. Agencia Nacional de Ciberseguridad

2.6.1. Objeto y naturaleza jurídica

Este es un elemento central de la ley, por cuanto no sólo regula el tema de la ciberseguridad en servicios esenciales o de importancia vital, públicos y privados, sino que además crea una institucionalidad para implementar esa regulación. Así, se crea 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 encargado de la seguridad pública[7]. Su domicilio estará en Santiago, pero podrá tener oficinas en otras macrozonas o regiones (art. 10).

2.6.2. Funciones y atribuciones

Su principales atribuciones son: asesorar al Presidente de la República, en la elaboración y aprobación de la **Política Nacional de Ciberseguridad**, y de los planes

[7] Actualmente, esta alusión hace referencia al Ministerio del Interior, pero se está tramitando un proyecto de ley para crear un Ministerio de Seguridad Pública, que asumiría estas funciones (Boletín N° 14614-07, en este momento en tercer trámite constitucional).

y programas de acción específicos para su implementación, ejecución y evaluación (art. 11, a); dictar los **protocolos y estándares** que deberán cumplir las instituciones regidas por esta ley (art. 11, b), así como aplicar e interpretar administrativamente las disposiciones legales y reglamentarias en materia de ciberseguridad (art. 11, c); coordinar y supervisar al CSIRT Nacional y a los demás CSIRT pertenecientes a la Administración del Estado, y requerir de éstos la información que sea necesaria para el cumplimiento de sus fines (art. 11, d); crear y administrar el **Registro Nacional de Incidentes de Ciberseguridad** (art. 11, f); prestar asesoría técnica a los organismos del Estado e instituciones privadas afectados por un incidente de ciberseguridad que haya comprometido sus activos informáticos críticos o afectado el funcionamiento de su operación (art. 11, m); **fiscalizar** el cumplimiento de esta ley, sus reglamentos, protocolos, estándares técnicos e instrucciones generales y particulares (art. 11, ñ), pudiendo asimismo instruir el inicio de procedimientos sancionatorios y sancionar las infracciones e incumplimientos en que incurran las instituciones obligadas por la ley (art. 11, o).

Asimismo, se le entregan dos atribuciones específicas en materia de incidentes de ciberseguridad: requerir a los organismos de la Administración del Estado y a las instituciones privadas señaladas en el artículo 4 acceso a la información necesaria para prevenir la ocurrencia de incidentes de ciberseguridad o para gestionar uno que ya hubiera ocurrido (art. 11, j); y requerir, mediante instrucción de su Director o Directora, en casos de incidentes de impacto significativo cuya gestión lo haga imprescindible, el acceso a redes y sistemas informáticos (art. 11, k).

Por otro lado, se le encomienda fomentar la formación ciudadana en el tema, para lo cual debe diseñar e implementar planes y acciones de formación ciudadana, capacitación, fortalecimiento, difusión y promoción de la cultura en ciberseguridad (art. 11, i). También se le encarga fomentar la investigación, innovación, capacitación y entrenamiento frente a amenazas, vulnerabilidades e incidentes de ciberseguridad y, en conjunto con los Ministerios de Economía, Fomento y Turismo, y de Ciencia, Tecnología, Conocimiento e Innovación, diseñar planes y acciones que fomenten el desarrollo o fortalecimiento de la industria de ciberseguridad local (art. 11, p).

Como podemos apreciar, se trata de un ente que, por un lado, tendrá un carácter técnico y estará orientado a asesorar al Presidente de la República en la elaboración de políticas públicas y, por otro lado, detentará un rol fiscalizador, con amplias atribuciones para dictar normativa en el ámbito de sus funciones. Cabe mencionar que, para evitar conflictos de competencia o antinomias con las agencias u órganos encargados de la regulación sectorial, se prevén diversos mecanismos de coordinación, especificados en el Título IV de la ley (arts. 25 y 26).

2.6.3. Estructura orgánica

La Agencia será dirigida por una autoridad unipersonal denominada Director o Directora Nacional, sujeta al sistema de alta dirección pública (art. 12). Asimismo,

contará con un Subdirector o Subdirectora, también designada por alta dirección pública (art. 13).

El personal estará regido por el Código del Trabajo, aunque se le aplicarán las normas sobre probidad y responsabilidad administrativa que se les aplican a los funcionarios de la Administración del Estado (art. 17). La estructura interna del servicio será definida mediante un reglamento expedido por el Ministerio encargado de la seguridad pública.

2.6.4. Órganos dependientes o vinculados a la Agencia

Por otro lado, se crea un **Comité Multisectorial de Ciberseguridad**, de carácter consultivo, cuya principal función será asesorar y formular recomendaciones a la Agencia en el análisis y revisión periódica de la situación de ciberseguridad del país, en el estudio de las amenazas existentes y potenciales en el ámbito de ciberseguridad, y proponer medidas para abordarlas.

Estará integrado por el Director o Directora Nacional de la Agencia, quien lo presidirá, y seis consejeros *ad honorem* designados por el Presidente de la República, escogidos entre personas de destacada labor en el ámbito de la ciberseguridad o de las políticas públicas vinculadas a la materia, que durarán 6 años en sus cargos, pudiendo ser prorrogados por un segundo período (art. 20). El Consejo sesionará, a lo menos, cuatro veces al año; sus recomendaciones serán de carácter público y deberán recoger la diversidad de opiniones existentes en él cuando no haya unanimidad respecto de las mismas (art. 21).

Asimismo, se crea la **Red de Conectividad Segura del Estado**, que proveerá servicios de interconexión y conectividad a internet a los organismos de la Administración del Estado. Para el mejor funcionamiento de esta red, la Agencia podrá suscribir los convenios de interconexión con instituciones públicas y privadas que considere necesarios. Un reglamento del Ministerio encargado de la seguridad pública y visado por el Ministro de Hacienda regulará el funcionamiento de la RCSE (art. 23).

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 ciberataques cuando sean de efecto significativo; coordinar a los CSIRT de los diversos órganos de la Administración del Estado; y servir de punto de enlace con CSIRT extranjeros o sus equivalentes, entre otras (art. 24). Este órgano es regulado en detalle en el Título V de la ley (arts. 29 al 32).

2.7. Comité Interministerial de Ciberseguridad

Tendrá por objeto asesorar al Presidente de la República en materias de ciberseguridad relevantes para el funcionamiento del país. Su principal función será asesorarlo en la elaboración de la Política Nacional de Ciberseguridad y coordinar su implementación (art. 48).

Estará compuesto por los subsecretarios (o por quien éstos designaren) de Interior; Defensa; Relaciones Exteriores; Secretaría General de la Presidencia, Telecomunicaciones; Hacienda; Ciencia, Tecnología, Conocimiento e Innovación; por el Director o Directora Nacional de la Agencia Nacional de Inteligencia; y por el Director o Directora Nacional de la Agencia Nacional de Ciberseguridad (art. 49). Su secretaría ejecutiva estará radicada en esta última institución (art. 50).

2.8. Reserva de información

Se consideran secretos y de circulación restringida, los antecedentes, datos, informaciones y registros que obren en poder de la Agencia, de los CSIRT, sean Nacional, de Defensa o que pertenezcan a organismos de la Administración del Estado, o de su personal, cualquiera que sea su cargo o la naturaleza de su vinculación jurídica con éstos. Asimismo, se indica que tendrán dicho carácter aquellos otros antecedentes respecto de los cuales el personal de tales organismos del Estado tome conocimiento en el desempeño de sus funciones o con ocasión de éstas (art. 33).

Adicionalmente, será 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; y iii. Los planes de acción y mitigación de riesgos de ciberseguridad (art. 33).

La obligación de guardar secreto regirá, además, para aquellos que, sin ser funcionarios o funcionarias 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. 34).

2.9. Infracciones y sanciones

Se establecen tres tipos de infracciones a los deberes contenidos en esta ley: leves, graves y gravísimas. Dentro de las primeras, se cuenta entregar fuera de plazo la información que se le requiera cuando ella no fuere necesaria para la gestión de un incidente de ciberseguridad (art. 38, inc. 2°, N° 1). En tanto, un ejemplo de las segundas es no haber implementado los protocolos y estándares establecidos por la Agencia para prevenir, reportar y resolver incidentes de ciberseguridad (art. 38, inc. 3°, N° 1). Finalmente, un ejemplo de infracción gravísima es entregar a la Agencia información manifiestamente falsa o errónea, cuando ella sea necesaria para la gestión de un incidente de ciberseguridad (art. 38, inc. 4°, N° 1). Para hacerse una idea, la respuesta a un incidente de ciberseguridad, la realización de las acciones indicadas en el cuadro N° 1 fuera del plazo máximo establecido por la ley constituiría un caso de infracción grave, a menos que se tratara de un incidente de efecto significativo, en cuyo caso la infracción sería gravísima (véase el art. 38).

Ahora bien, la ley también dispone una particular gradación de infracciones para el caso de instituciones definidas como de importancia vital, que también va desde las leves a las gravísimas (art. 39).

En cuanto a las sanciones, el artículo 40 establece una escala detallada.

Cuadro N° 2. Escala de sanciones

Infracciones	Institución	Sanciones
Leves	General	Hasta 5.000 UTM
	Operador de importancia vital	Hasta 10.000 UTM
Graves	General	Hasta 10.000 UTM
	Operador de importancia vital	Hasta 20.000 UTM
Gravísimas	General	Hasta 20.000 UTM
	Operador de importancia vital	Hasta 40.000 UTM

Elaboración propia a partir de la ley

Cabe mencionar que el artículo 42 establece un procedimiento sancionatorio *ad hoc*, que se regirá supletoriamente por la ley de procedimiento administrativo (ley N° 19.880). Asimismo, se establece un procedimiento de reclamación judicial de tipo sumario, ante la Corte de Apelaciones, para las personas que estimen que un acto administrativo que paraliza el procedimiento, o una resolución final o de término emanado de la Agencia, es ilegal y les causa perjuicio (art. 46).

2.10. Modificaciones a otras normas

Se incorpora una nueva atribución para el Jefe del Estado Mayor: "k) Conducir al Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional en coordinación con la Subsecretaría de Defensa" (art. 25 de la ley Nº 20.424, Estatuto Orgánico del Ministerio de Defensa Nacional).

Por otro lado, se modifican algunos artículos de la ley N° 21.459, que establece normas sobre delitos informáticos.

2.11. Disposiciones transitorias

Se establecen diversas disposiciones transitorias, dentro de las cuales destacamos, en primer lugar, la autorización al Presidente de la República para regular, dentro del plazo de un año, mediante decretos con fuerza de ley, la fecha para la iniciación de actividades de la Agencia, la cual podrá contemplar un período para su implementación y uno a contar del cual entrará en operaciones, así como la fijación de su planta de personal y su sistema de remuneraciones y el traspaso de personal desde la Subsecretaría del Interior al nuevo organismo, entre otras (artículo primero transitorio).

Cabe señalar que también se le permite al Presidente designar directamente al primer Director o Directora de la Agencia Nacional de Ciberseguridad, quien asumirá de inmediato, por el plazo máximo de un año y en tanto se efectúa el proceso de selección pertinente que establece la señalada ley para los cargos del Sistema de Alta Dirección Pública (artículo segundo transitorio).

Por otro lado, es relevante tener en cuenta, en pos de la implementación, que se establece un plazo de 180 días desde la publicación de la ley, para que el Ministerio del Interior y Seguridad Pública expida los reglamentos señalados en ella (artículo cuarto transitorio).

3. Comentarios

Lo primero que debemos destacar de esta ley es que se centra en la creación de una institucionalidad robusta para enfrentar el problema de la ciberseguridad. Hasta la publicación de la ley el país contaba 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, regulado originalmente por medio de la Resolución Exenta N° 5.006, de 2019[8]. Sin embargo, no existía un sistema ni una institucionalidad permanente y de alcance general que permitiera enfrentar el problema de manera coordinada. En este sentido, la creación de una **Agencia Nacional de Ciberseguridad**, 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, la ley provee diversas definiciones que serán útiles para la creación de un verdadero sistema de respuesta frente a los ciberataques. Se trata, por tanto, de definiciones operativas, pensadas para una adecuada implementación de la ley.

En este sentido, una definición clave es la de ciberseguridad. En un principio, el proyecto de ley la reducía a una situación de respuesta frente a los incidentes de ciberseguridad, lo que generaba una definición circular, que no iluminaba completamente el concepto. En contraste, la ciberseguridad ha sido entendida 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

[8] Véase: https://ciberseguridad.gob.cl/documents/204/RES.-EXENTA-N-5006-CREACION-DE-DIVISION-Y-UNIDAD.pdf [consultado el 13-05-2024]

allí ocurren. En este conjunto (…) los atributos claves a proteger son la confidencialidad, integridad y disponibilidad de la información"[9]. La nueva definición establecida en la ley toma esta base, centrándose en la "preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos" (art. 2, N° 6). Así, tiene la virtud de poner 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 vislumbraba en la definición dada por el proyecto original y que constituye, por tanto, un avance producto de su tramitación legislativa.

En cuanto a las atribuciones de la Agencia es importante advertir que tendrá diversos tipos de atribuciones. En primer lugar, podemos destacar su rol de participación y asesoría en la **elaboración de políticas públicas** (asesora al Presidente en la elaboración de la Política Nacional de Ciberseguridad y en los planes y programas de acción para su implementación).

En segundo lugar, cabe mencionar sus **potestades normativas y fiscalizadoras**. Así, podrá dictar protocolos y estándares técnicos de ciberseguridad. También podrá dictar instrucciones generales y particulares para las instituciones obligadas por la ley. La contracara de esto es que tendrá la atribución de fiscalizar y sancionar el cumplimiento de la ley, sus reglamentos y estándares técnicos. En otras palabras, se le entregan potestades fiscalizadoras bastante robustas para el cumplimiento de los objetivos de la ley.

En tercer lugar, tendrá también la **coordinación** del CSIRT Nacional y los demás pertenecientes a la Administración del Estado, lo que le entrega un rol de dirección general de los asuntos relativos a la ciberseguridad en Chile. En esta línea, cabe mencionar también su **rol de asesoría técnica** a los organismos del Estado e instituciones privadas afectados por un incidente de ciberseguridad.

Por último, le cabe a la Agencia también un **rol de fomento** de la investigación, innovación y capacitación en materia de ciberseguridad, entre otros aspectos.

Como comentario final, es preciso indicar que esta ley establece un marco para la ciberseguridad, pero en ningún caso agota todo lo que debiera entenderse por ciberseguridad en nuestro sistema jurídico. Así, se puede sostener que el elemento central en la ciberseguridad- la protección de la integridad de los datos de las personas- requiere del sustento de un verdadero ecosistema institucional. Este

[9] Véase: GOBIERNO DE CHILE. *Política Nacional de Ciberseguridad (2017-2022)*, p. 16. Puede consultarse en línea: https://biblioteca.digital.gob.cl/server/api/core/bitstreams/b5b26f36-2c47-441b-8848-00d767ec9b5c/content [consultada el 13-05-2024]. Cabe mencionar que actualmente la Política Nacional de Ciberseguridad (2023-2028) no establece una definición específica de ciberseguridad, pero sí incluye diversos objetivos fundamentales que incorporan varios de estos elementos. Véase: GOBIERNO DE CHILE, *Política Nacional de Ciberseguridad (2023-2028)*, p. 11. Disponible en: https://ciberseguridad.gob.cl/documents/4430/Pol%C3%ADtica_Nacional_de_Ciberseguridad_2023-2028.pdf [consultada el 13-05-2024]

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[10]. 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[11]. 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.

[10] 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.

[11] 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 tercer trámite constitucional (Comisión Mixta).