INFORME DE LA COMISIÓN DE SEGURIDAD PÚBLICA recaído en el proyecto de ley, en primer trámite constitucional, que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.

BOLETÍN Nº 14.847-06.

Objetivo(s) / Constancias / Normas de Quórum Especial (sí tiene) / Consulta Excma. Corte Suprema (no hubo) / Asistencia / Antecedentes de Hecho / Aspectos Centrales del Debate / Discusión en General / Votación en General / Texto / Acordado / Resumen Ejecutivo.

HONORABLE SENADO:

La Comisión de Seguridad Pública tiene el honor de informar el proyecto de ley de la referencia, iniciado en Mensaje de Su Excelencia el ex Presidente de la República, señor Sebastián Piñera Echenique, con urgencia calificada de “suma”.

Se hace presente que, de conformidad a lo dispuesto en el artículo 36 del Reglamento de la Corporación, la Comisión discutió solo en general esta iniciativa de ley, la que resultó aprobada por la unanimidad de sus integrantes (5x0).

- - -

OBJETIVO (S) DEL PROYECTO

Establecer la institucionalidad necesaria para robustecer la ciberseguridad; ampliar y fortalecer el trabajo preventivo; formar una cultura pública en materia de seguridad digital; enfrentar las contingencias en el sector público y privado, y resguardar la seguridad de las personas en el ciberespacio.

- - -

CONSTANCIAS

- Normas de quórum especial: Sí tiene

- Consulta a la Excma. Corte Suprema: No hubo.

- - -

NORMAS DE QUÓRUM ESPECIAL

Hacemos presente que de conformidad a lo dispuesto en el artículo 38 de la Constitución Política de la República, los artículos 8; 9 letras a), b), d), h), l) y m); 10; 13; 17; 22; 23; 24 letra b); 27; 28; 34; 36; 37; 38 y 41, permanentes; y los artículos segundo; quinto y sexto de las disposiciones transitorias, tienen el carácter de normas orgánicas constitucionales, por lo que requieren para su aprobación de las cuatro séptimas parte de los senadores en ejercicio, según lo prevé el inciso segundo del artículo 66 de la Carta Fundamental:

Por su parte, los artículos 16; 29; 30; 31 y 39, permanentes, tienen el carácter de normas de quórum calificado, de conformidad al artículo 8°, inciso segundo, de la Constitución Política de la República, por lo que requieren para su aprobación de la mayoría absoluta de los senadores en ejercicio, según lo dispone el inciso tercero del artículo 66, de la Constitución Política de la República.

\- - -

ASISTENCIA

- Representantes del Ejecutivo e invitados:

1.- Del Ministerio del Interior y Seguridad Pública:

- El Coordinador Nacional de Ciberseguridad señor Daniel Álvarez y la asesora jurídica y legislativa de dicha Coordinación, señora Michelle Bordachar.

- De la Subsecretaría de Prevención del Delito los asesores señor Rodrigo Muñoz y señora Carolina Codoceo.

2.- El ex Senador señor Felipe Harboe.

3.- El Director de la Unidad Especializada en Lavado de Dinero, Delitos Económicos, Delitos Medioambientales y Crimen Organizado (ULDECCO) del Ministerio Público, señor Mauricio Fernández.

- Otros

Los asesores parlamentarios: de la oficina del Honorable Senador señor Insulza la señora Javiera Gómez y el señor Guillermo Miranda; de la oficina del Honorable Senador señor Huenchumilla el asesor señor Rodrigo Vega; de la oficina del Honorable Senador señor Quintana el señor Claudio Rodríguez; de la oficina del Honorable Senador señor Ossandón el señor

Ronald Von Der Weth y de la oficina del Honorable Senador señor Van Rysselbergue el señor Juan Paulo Morales.

- - -

ANTECEDENTES DE HECHO

I. Antecedentes. Para el debido estudio de este proyecto de ley, se ha tenido en consideración el Mensaje de Su Excelencia el ex Presidente de la República señor Sebastián Piñera Echenique.

Expone que las tecnologías emergentes de la sociedad digital han generado un proceso de cambio cultural amplio, el cual se ha acelerado y profundizado en el contexto de diversas medidas sanitarias, como los confinamientos, producto de la pandemia del COVID-19.

Producto de lo anterior, afirma como necesario que el Estado profundice su transformación digital, la cual empezó con la publicación de la ley N°21.180 y ha continuado con el decreto supremo N°4, de 9 de noviembre de 2020, del Ministerio Secretaría General de la Presidencia y el DFL N° 1 de 2020 emanado de la misma Cartera de Estado.

Indica que tal modernización, es una tarea continua y permanente, que se enmarca dentro del principio rector consagrado en el artículo primero de nuestra Carta Fundamental, donde se reconoce que el Estado está al servicio de las personas, por lo que sostiene que el acceso a diversos servicios públicos mediante canales digitales, debe ser entregado con todos los resguardos y estándares de seguridad necesarios. Por tanto, expresa que se transita decididamente hacia un Estado que sea más integrador, ágil, innovador y efectivo para cumplir su función de servir al bien común.

Asimismo, el Mensaje recalca que los desafíos en materia de ciberseguridad requieren una convergencia, coordinación y articulación público-privada para la gestión de alertas preventivas y de incidentes de ciberseguridad. Por lo tanto, sostiene que es necesario gestionar los riesgos e implementar los más exigentes estándares que otorguen confianza y seguridad en las instituciones tanto públicas como privadas.

Agrega que el vertiginoso desarrollo de la sociedad digital conlleva un mayor riesgo de vulnerabilidad en todas las estructuras digitales, pero especialmente en aquellos sectores estratégicos donde existe infraestructura de la información que resulta ser crítica.

De tal manera, asegura que el presente proyecto de ley permitirá establecer el marco regulatorio necesario para el desarrollo robusto de la ciberseguridad, tanto en su dimensión operativa como regulatoria.

II. Fundamentos.

1. Relevancia de la ciberseguridad: En este ámbito, el Mensaje sostiene que el tránsito desde los soportes físicos hacia la infraestructura de la información, con el permanente riesgo de incidentes de ciberseguridad y ciberataques comienza a formar parte de los elementos a considerar en la discusión pública, siendo la gestión del riesgo y el control de la vulnerabilidad, aspectos destacados.

Posteriormente expresa que el Gobierno de Su Excelencia el ex Presidente Piñera, estableció entre sus objetivos la creación de condiciones para que Chile pueda insertarse de manera protagónica en la cuarta revolución industrial, adaptando las regulaciones a los desafíos que impone esta revolución digital.

2. Relevancia de la institucionalidad en materia de ciberseguridad: El Mensaje subraya que se requiere un órgano encargado de la seguridad en el ciberespacio, que proteja los bienes ya activos de la sociedad digital. Asimismo, explica que nuestro país requiere de una institucionalidad pública que se coordine con el sector privado de manera permanente, para garantizar la seguridad en el ciberespacio, que ayude a prevenir los delitos informáticos y proteja la infraestructura crítica de la información.

De esta manera, recalca que esa institucionalidad necesita de una gobernanza clara y una orgánica definida en sus roles, con amplias competencias, confiable, y altamente profesional, entre otros aspectos.

III. Objetivo del proyecto de ley.

El Mensaje anuncia que tiene como propósito establecer la institucionalidad necesaria para robustecer la ciberseguridad, ampliar y fortalecer el trabajo preventivo, la formación de una cultura pública en materia de seguridad digital, enfrentar las contingencias en el sector público y privado, y resguardar ña seguridad de las personas en el ciberespacio.

De igual modo fundamenta que se pretende proteger al Estado, sus redes y los demás sistemas informáticos e infraestructura de la información en el sector púbico, especialmente aquellas que son esenciales y críticas para los ciudadanos. En ese sentido, expresa que se protegerá la Seguridad Nacional, promoviendo el resguardo de datos, las redes y los sistemas informáticos de la información del sector privado, especialmente aquellas que son esenciales para el adecuado funcionamiento del país.

Finalmente, arguye que se procurará generar las capacidades para la prevención, mitigación, la efectiva y pronta recuperación ante incidentes de ciberseguridad que afecten a instituciones que posean infraestructura crítica de la información, para conformar un ciberespacio seguro, estable y resilente.

IV. Contenido del proyecto de ley

En primer término, el Mensaje sostiene que el ámbito de aplicación son los órganos de la Administración del Estado; los órganos del Estado y las instituciones privadas que posean Infraestructura Crítica de la Información.

En cuanto a su marco normativo, el Mensaje detalla los siguientes aspectos:

1.- El título primero contiene las disposiciones generales, donde destaca el objetivo del proyecto y los principios rectores.

2.- El título segundo, por su parte, establece la forma de determinación de la infraestructura crítica de la información y las obligaciones de las instituciones que poseen infraestructura de la información calificada como crítica. Asimismo, se señalan los deberes generales de los órganos del Estado cuya infraestructura de la información sea calificada como crítica, además de las facultades normativas de los reguladores o fiscalizadores sectoriales con competencia en sus respectivos sectores regulados.

3.- El título tercero crea y regula distintos organismos vinculados con la ciberseguridad como es la Agencia Nacional de Ciberseguridad, el Registro Nacional de Incidentes de Ciberseguridad, el Consejo Técnico de la Agencia Nacional de Ciberseguridad y el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática, denominado “CSIRT Nacional”.

4.- El título cuarto regula los Equipos de Respuesta a Incidentes de Seguridad Informáticos Sectoriales “CSIRT Sectoriales”, que podrán constituirse por los reguladores o fiscalizadores sectoriales.

5.- En el título quinto se crea y se regula el CSIRT de Gobierno y el CSIRT de Defensa. El primero de ellos se asocia a la información del Estado y el segundo, pertenece al Estado Mayor Conjunto del Ministerio de Defensa Nacional, el cual es responsable de la coordinación y protección de la infraestructura de la información calificada como crítica del sector Defensa.

6.- Desde otra vereda, en el título sexto, se regula la reserva de la información, la cual se considerará secreta y de circulación restringida para todos los efectos legales de todos aquellos antecedentes, datos, informaciones y registros que obren en poder de los CSIRT.

7.- En línea con lo anterior, el título séptimo establece las infracciones, regula las multas y el procedimiento sancionatorio, junto con establecer una agravante especial.

8.- En el título octavo se crea y regula el Comité Interministerial de Ciberseguridad, encargado de 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 servicios esenciales. Asimismo, establece que un reglamento expedido por el Ministerio del Interior y Seguridad Pública fijará las normas de funcionamiento del Comité.

9.- Finalmente, el título noveno contempla una modificación al Estatuto Orgánico del Ministerio de Defensa Nacional, y el título décimo contiene las disposiciones transitorias.

- - -

ASPECTOS CENTRALES DEL DEBATE

Los principales puntos discutidos por la Comisión dicen relación con los siguientes:

1) La debida armonía que debe guardar este proyecto de ley con la ley 21.459 sobre delitos informáticos y el proyecto de ley sobre datos personales que se encuentra en discusión en segundo trámite constitucional en la Cámara de Diputados (Boletines N°11.144-07 y 11.092-07, refundidos).

2) La creación de una institucionalidad pública a cargo de la ciberseguridad, con funciones y atribuciones tanto respecto al sector público como al sector privado.

3) La rigidez del concepto de infraestructura crítica, y ciertos cuestionamientos a la definición de servicios esenciales.

4) El carácter supletorio de la presente iniciativa de ley en cuanto a sus facultades normativas y principios, y específicamente en lo que refiere a la Agencia Nacional de Ciberseguridad.

5) La intención por parte del Ejecutivo de simplificar el proyecto de ley, especialmente en cuanto a su estructura orgánica, a objeto que la Agencia Nacional de Ciberseguridad sea una institución rectora en esta materia tanto para el sector público como privado.

- - -

DISCUSIÓN EN GENERAL[1]

A.- Presentación del proyecto de ley por el **Coordinador Nacional de Ciberseguridad del Ministerio del Interior y Seguridad Pública y Presidente del Comité Interministerial de Ciberseguridad, señor Daniel Álvarez Valenzuela.**

El señor Álvarez mediante una presentación, informó que el presente proyecto de ley se ingresó al Congreso Nacional a fines del Gobierno de Su Excelencia el ex Presidente de la República señor Sebastián Piñera, y que el Ejecutivo continuará en su tramitación con algunas modificaciones.

A modo de contexto, explicó que después de los incidentes ocurridos durante las últimas semanas en materia de ciberseguridad, resulta interesante comprender de qué manera el Estado se está haciendo cargo de esos temas, así como los particulares también debieran participar.

Como primera cosa, destacó que el Estado por su mandato constitucional, tiene el deber de proteger la información de las personas, en cuanto a las redes y sistemas. En ese sentido, destacó que cuando el Estado no actúa, las directamente afectadas son las personas en sus derechos, su patrimonio e incluso su seguridad individual.

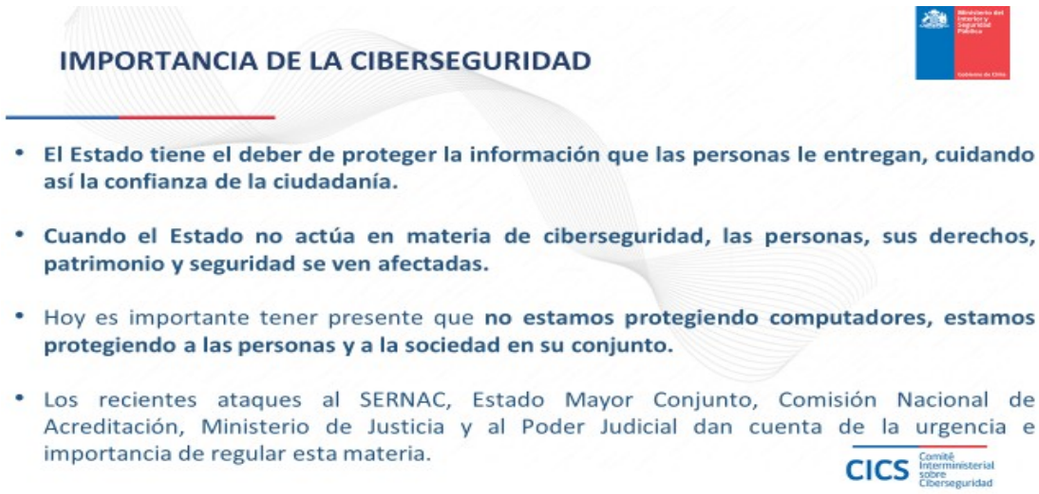
Aclaró que cuando se habla de ciberseguridad no se está pensando en proteger computadores, sino que, a una sociedad que se comunica e interactúa permanentemente a través de esos equipos.

De esta manera apuntó que la seguidilla de ataques acaecidos en los últimos meses, ya sea al SERNAC, al Estado Mayor Conjunto y al Poder Judicial, denotan que se trata de un problema país y requiere de respuestas lo más institucionales posibles.

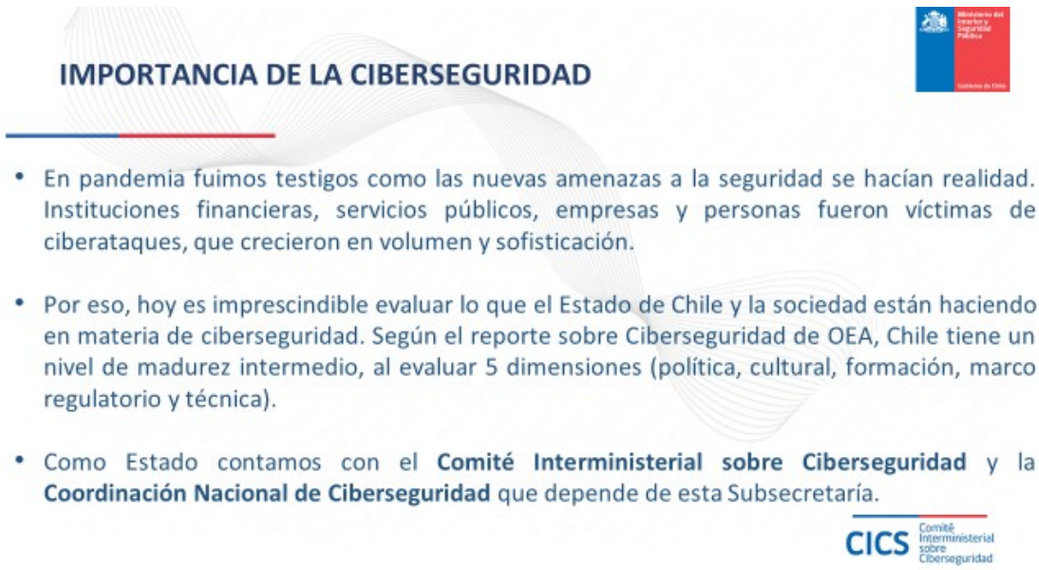
Lo expuesto se grafica en la lámina que sigue:

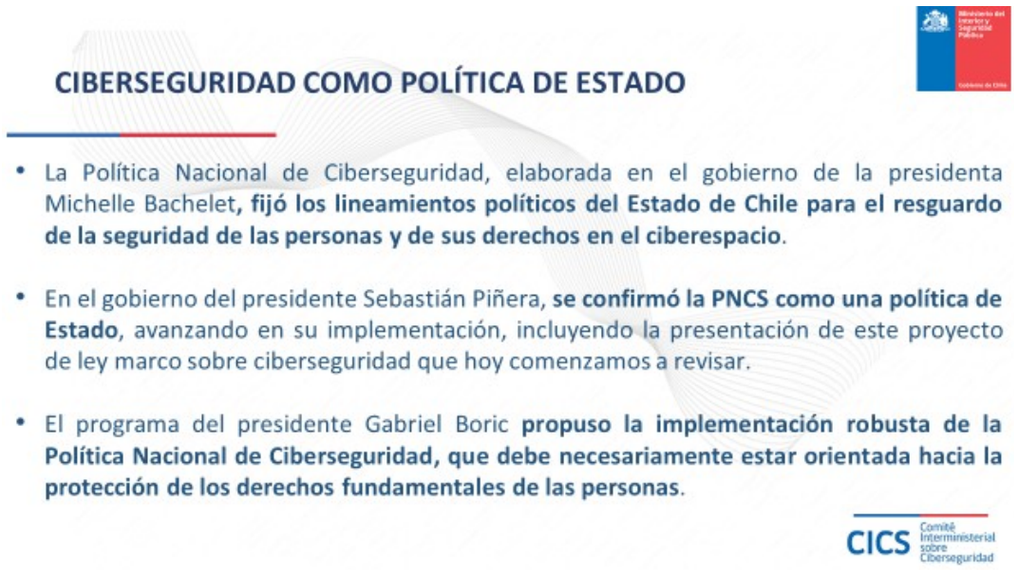
---

[1] A continuación, figura el link de cada una de las sesiones, transmitidas por TV Senado, que la Comisión dedicó al estudio del proyecto de ley:
Sesión celebrada el día 4 de octubre de 2022:
https://tv.senado.cl/tvsenado/comisiones/permanentes/seguridad-publica/comision-de-seguridad-publica/2022-10-04/082637.html
Sesión celebrada el día 11 de octubre de 2022:
https://tv.senado.cl/tvsenado/comisiones/permanentes/seguridad-publica/comision-de-seguridad-publica/2022-10-11/085718.html



Posteriormente, destacó que el año 2015 se constituyó el Comité Interministerial de Ciberseguridad, que aprobó la primera Política Nacional de Ciberseguridad del año 2017 vigente hasta el año 2022. Luego el gobierno de Su Excelencia el ex Presidente señor Sebastián Piñera continuó con la implementación de esta política, y finalmente el actual gobierno se comprometió a robustecerla y avanzar en la misma. De esta manera, recalcó que es una política de Estado que ha permanecido al menos durante tres gobiernos consecutivos.





Enseguida se refirió a las acciones que está tomando el gobierno desde el Comité Interministerial de Ciberseguridad y El Ministerio del Interior y Seguridad Pública.

Expresó que se iniciaron tres procesos en paralelo:

1) El primero fue evaluar el documento “Política Nacional de Ciberseguridad” para efectos de ver cómo funcionó. Agregó que fue una planificación de largo tiempo que tiene 5 objetivos estratégicos y 41 medidas específicas, respecto de los cuales se persigue identificar si las medidas que estaban diseñadas para este período, eran lo suficientemente precisas para hacerse cargo del cumplimiento de los objetivos. De lo señalado advirtió que actualmente se encuentran en ese proceso de evaluación.

2) Asimismo, explicó que se encuentran preparando la Política Nacional de Ciberseguridad 2023-2028, en un proceso abierto y participativo. Comunicó que el resultado esperado de dicho proceso es que en marzo del año 2023 el país cuente con una nueva Política Nacional de Ciberseguridad.

3) Finalmente, el último proceso según sostuvo, se trata de la discusión y aprobación del presente proyecto de ley.

Lo anterior se grafica en la siguiente lámina:

Con el afán de sintetizar la presente iniciativa legal, argumentó que se crea una institucionalidad pública a cargo de la ciberseguridad, con funciones y atribuciones tanto respecto al sector público como del sector privado.

Particularmente, indicó que tal institucionalidad recaería en la Agencia Nacional de Ciberseguridad, que se relacionaría con el Presidente de la República a través del Ministerio del Interior y Seguridad Pública.

Puso especial acento en que se deben concordar los proyectos de ley que actualmente se discuten en el Congreso respecto a la creación del nuevo Ministerio de Seguridad Pública, anunciando que se presentaría una propuesta a ese respecto.

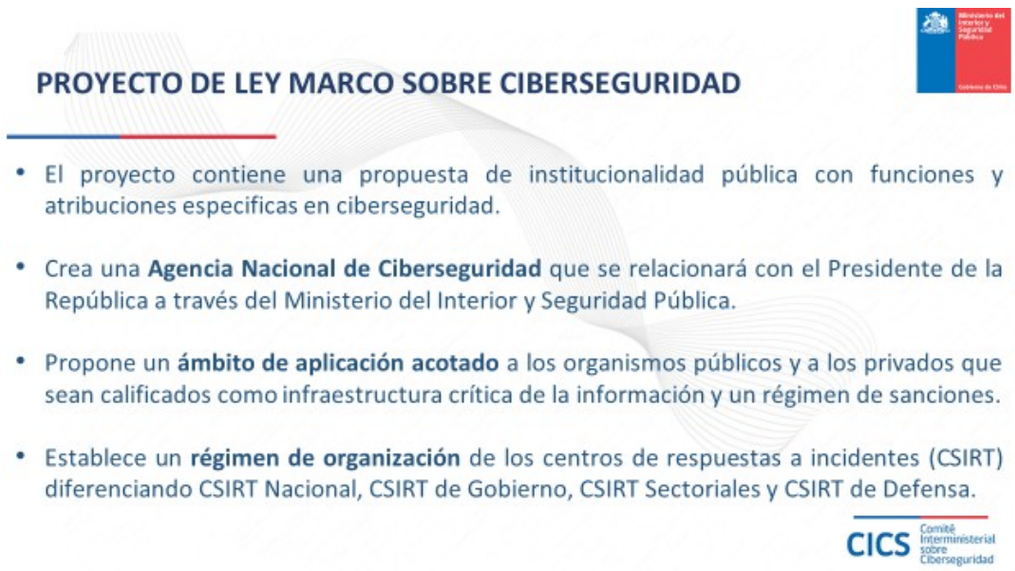
Por otra parte, indicó que el proyecto —de la forma que está presentado— establece un ámbito de aplicación acotado, lo que constituirá uno de los cambios fundamentales que se consultarán.

Particularmente, destacó que, de aprobarse sin modificaciones, se aplicaría a los órganos de la Administración del Estado y a aquellos privados que sean calificados como infraestructura crítica. Sin embargo, previno que muchas organizaciones privadas que manejan grandes volúmenes de información o aquella declarada sensible, pero que, sin embargo, no caben en la categoría de infraestructura crítica, podrían quedar eventualmente exentas de obligaciones en materia de ciberseguridad.

En otro orden de cosas, remarcó que el proyecto de ley establece un modelo de organización del Estado bastante complejo, donde crea muchos órganos y varios CSIRT con distintas funciones, además de otras entidades

que tendrían la función de coordinación y asesoría. Por lo que fue de la idea que se debe simplificar la propuesta.

Lo anterior se esquematiza en la siguiente lámina:



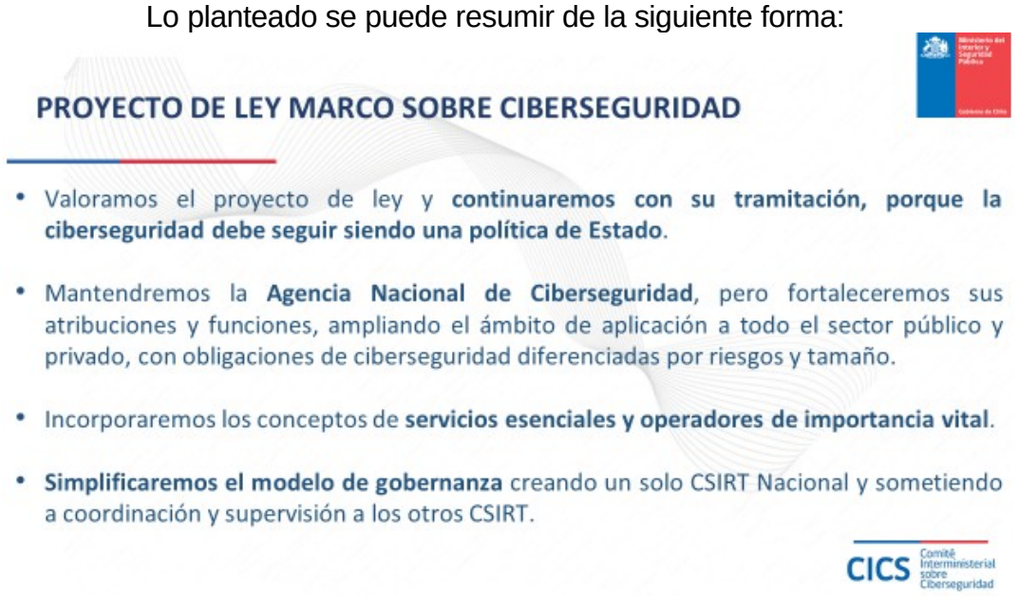
En ese contexto calificó como necesaria la creación de una Agencia Nacional de Ciberseguridad, no obstante, opinó que se deben fortalecer sus capacidades en cuanto tenga la facultad de fiscalizar, dictar normas, generar capacitación y formación, convirtiéndose en un órgano rector en materia de ciberseguridad para el sector público y privado.

A continuación, se refirió a que el concepto de infraestructura crítica que contiene el proyecto es extremadamente rígido, por lo que sostuvo que hay soluciones en el derecho comparado que plantean definiciones más modernas y flexibles, apuntando a los denominados “servicios esenciales”. Puso como ejemplo el hecho de que, al hacer la calificación de infraestructura crítica, se debe incorporar sin duda, al transporte puesto que presta un servicio esencial a la ciudadanía. No obstante, resaltó que como hoy en día existen tantas modalidades de transporte, como el transporte aéreo y terrestre, se debe también hacer hincapié en los medios de transporte privado como Uber, taxis, etc.

De esta manera, anticipó que dentro de las modificaciones que se propondrán al proyecto, está la incorporación del concepto de “servicios esenciales para el país” y los “operadores de importancia habitual dentro de esos servicios esenciales”. Así las cosas, indicó que, si se declara como servicios esenciales el sector transporte, probablemente se encontrarán entre estos últimos las líneas aéreas, las empresas públicas de transporte, el Metro, el tren o los barcos.

Desde otro ángulo, planteó que una de las propuestas de modificación a presentar apunta a simplificar el modelo de gobernanza, en el sentido de crear solo un CSIRT a nivel nacional, con la proyección de que, si en el futuro se crean otros, estos deben estar bajo la supervisión del primero. Por tanto, relevó la importancia de centralizar la capacidad de defensa en este aspecto.

Lo planteado se puede resumir de la siguiente forma:



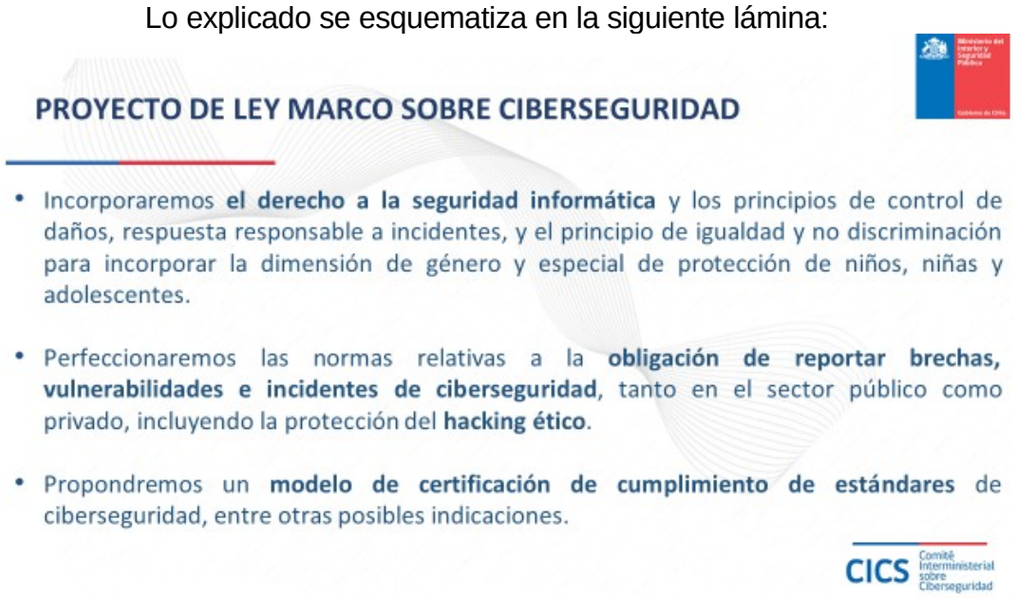
En otras materias, aludió a la incorporación en el proyecto, como se ha hecho a nivel comparado, de un derecho a la seguridad informática, de la misma manera como existe el derecho a la seguridad pública o ciudadana. Agregó también la necesidad de incluir ciertos principios, que a su juicio fueron omitidos por el Gobierno anterior, como el de Respuesta Responsable a Incidentes. En ese sentido, sostuvo que la modificación que se plantea se funda en que la respuesta debe siempre ser razonable, prudente, y no exponer a mayor daño, toda vez que hoy en día se desconoce si un incidente pequeño puede llevar a otro de mayor envergadura.

Se pretende, además, según manifestó, ampliar el ámbito de aplicación de la ley al sector público y sector privado, con algunas limitaciones respecto de pequeñas y medianas empresas en cuanto a establecer obligaciones diferenciadas, sin perjuicio del deber general de reportar brechas y vulnerabilidades. En ese sentido, recalcó que el factor común de todos los incidentes ocurridos últimamente, es que existió una vulnerabilidad o brecha que no se resolvió, acentuando que, dada la responsabilidad de los agentes en este tipo de materias, estos deben estar obligados a notificar, reparar, “parchar” y actualizar.

Desde otro punto de vista, comentó que se pretende incorporar en la presente iniciativa de ley, como se discutió ampliamente en el proyecto sobre delitos informáticos (Boletín N°12.192-25) —actual ley N°21.459— una norma referida al *hacking* ético. Lo anterior según apuntó, como una forma de mejorar la calidad de los sistemas.

Finalmente, agregó que se persigue incluir también, indicaciones respecto a modelos de certificación de cumplimiento. Particularmente descartó que fuese en la modalidad *compliance* utilizada en varias legislaciones especiales, sino que lo que se perseguiría es permitir que se certifiquen habilidades. Dio como ejemplo el que una empresa del sector bancario implementase todo el set de normas ISO. De esta forma, a través de la iniciativa se podría certificar a aquellas empresas que cumplan con los mejores estándares posibles.

Lo explicado se esquematiza en la siguiente lámina:



El **Honorable Senador señor Ossandón** consultó al Coordinador Nacional de Ciberseguridad señor Álvarez, respecto a sí se encuentra incluido en esta iniciativa, o se pretende incorporar vía indicaciones, lo que dice relación con una Agencia Nacional de Protección de Datos. Por otra parte, agregó si es posible canalizar los nexos de todas las instituciones, compartiendo conocimiento.

El **señor Álvarez** respondiendo la consulta efectuada, señaló que la ciberseguridad se trata de un sistema compuesto por la ley de delitos informáticos que actualizó nuestra legislación, el proyecto de ley sobre datos personales que se encuentra en discusión en segundo trámite constitucional y que en específico crea la Agencia de Protección de Datos Personales, y en la iniciativa que se debate en esta Comisión que pretende crear la Agencia Nacional de Ciberseguridad. De tal manera, explicó que se tendrá una especie

de ecosistema que mayormente estará regulado por esta ley de ciberseguridad, y en cuanto se trate de datos personales, deberá estar regulado conforme a la Agencia de Protección de Datos Personales.

En efecto, detalló que estos sistemas son muy dinámicos, por lo que establecer en la ley la forma en que se expiden las reglas técnicas, va a provocar que se limite bastante el ámbito de decisión. Fundamentó que lo anterior es la razón de que se le entregue a la Agencia Nacional de Ciberseguridad la facultad de dictar instrucciones generales, particulares y aprobar normas técnicas, de manera que el desarrollo cotidiano de sus funciones sea lo más flexible posible.

El **Honorable Senador Ossandón** opinó que al crearse el Ministerio de Seguridad Pública (Boletín N°14.614-07), este sistema debiese reportar a esa Cartera de Estado y no al Ministerio del Interior y Seguridad Pública.

El **Honorable Senador señor Insulza**, planteó que tal situación estaría saldada toda vez que, una vez que se cree el Ministerio de Seguridad Pública, las facultades que actualmente están radicadas en el Ministerio del Interior, de competencia del primero, se traspasarán por definición, con los respectivos ajustes.

El **Honorable Senador señor Huenchumilla** preguntó cuál será el tratamiento del CSIRT del Ministerio de Defensa Nacional, a lo que **el señor Álvarez** respondió que este requiere un espacio de discusión específico distinto a lo que hace este proyecto de ley. En atención a ello, citó que la iniciativa en discusión crea el Comando Conjunto Ciber, sin embargo, con las atribuciones actuales del Estado Mayor Conjunto, solo podría actuar en tiempos de conflicto. En ese sentido, reafirmó la idea de que debía tratarse separadamente.

El **Honorable Senador señor Huenchumilla** propuso regular ciertas materias vía reglamento, como, por ejemplo, en lo que dice relación con las definiciones, para así evitar el exceso de detalle en la ley.

El **Personero de Gobierno** se mostró de acuerdo con la idea planteada y agregó que lo que se propone es simplificar la redacción del proyecto de ley y entregar una potestad reglamentaria a la Agencia Nacional de Ciberseguridad. Sin embargo, opinó que hay ciertas definiciones que debiesen quedar en el cuerpo legal porque son amplias y permiten flexibilidad, puesto que emanan del derecho comparado por lo que se encuentran bastante estandarizadas.

B.- Exposiciones de los invitados y debate suscitado en la Comisión con ocasión de ellas.

1.- El **ex Senador señor Felipe Harboe** expresó que cualquier regulación que se quiera implementar y que se pretenda como eficaz en materia de control del cibercrimen, requiere tener presente que esta ley es uno de los instrumentos necesarios para poder ejecutarlo. No obstante, advirtió que la misma requiere ser complementada con la ley de protección de datos personales (Boletines N°11.144-07 y 11.092-07, refundidos), la que se encuentra en segundo trámite constitucional en la Cámara de Diputados.

Particularmente, detalló que los bienes más perseguidos por los cibercriminales corresponden a los datos, los cuales les permiten efectuar un conjunto de acciones ilícitas que les reportan importantes ganancias.

En la misma línea, valoró la promulgación de la ley 21.459 sobre delitos informáticos, toda vez que permitió actualizar el marco jurídico para la persecución penal de este tipo de ilícitos.

Seguidamente, a modo de contexto, explicó que entre 2020 y 2021, el costo promedio de las brechas de seguridad aumentó en un 10%, es decir, desde 3,8 a 4,2 millones de dólares, según señala el reporte de IBM. Añadió que en aquellas compañías con teletrabajo el costo de la brecha fue en promedio un millón de dólares más alto.

Afirmó que la tendencia sigue siendo que el área más perjudicada por los costos de las brechas de seguridad es salud, con un promedio global de 9 millones de dólares.

En el ámbito nacional, sostuvo que solo en el primer semestre del año 2021 —según la PDI— se registraron más de 2 mil millones de incidentes, los que apuntan a ataques y otros, en materia cibernética. En ese contexto, indicó que dentro de los delitos más investigados se encuentra la estafa, el sabotaje informático y la adquisición o almacenamiento de material pornográfico infantil. Detalló que tales aspectos tuvieron un alza de 30%, 45% y 55%, respectivamente.

Como respuesta a lo anterior, argumentó que el gran problema lo representa, por un lado, la antigua legislación sobre delitos informáticos, la que, si bien ya ha sido modificada, los casos acaecidos con anterioridad a su actualización, continúan rigiéndose por la ley anterior.

En el ámbito cautelar, apuntó a que el cibercriminal siendo un delincuente mediato, no se caracteriza por un nutrido prontuario de antecedentes, lo que a su juicio complejiza que el Ministerio Público pueda obtener que se imponga una medida cautelar a través de los jueces.

Seguidamente, destacó que Chile tiene un gran problema en este aspecto, el cual se manifestó en el hackeo sufrido por la División de Gobierno Digital dependiente de la Secretaría General de la Presidencia. En dicha

ocasión, arguyó que el resultado fue la intervención de 500 mil claves únicas, teniendo presente, que tal mecanismo se constituyó como un validador exigido por el Estado para el conjunto de trámites en línea. Finalmente agregó, que el autor de ese ciberataque fue un estudiante de ingeniería de 26 años.

Por su parte, informó que a nivel comparado las experiencias o consecuencias pueden ser incluso peores a nivel de Administración del Estado. Recordó que, en relación al conflicto ruso ucraniano, unas de los principales problemas fue que se produjeron más de 50 mil ciberataques durante los primeros meses del conflicto, con el objeto de impedir el desarrollo de acciones bélicas y de prestaciones a la población.

Luego citó el caso del ataque a Dropbox en el año 2012, donde 68 millones de usuarios se vieron afectados en sus correos y contraseñas, el que según afirmó, se hizo público 4 años después.

Enseguida se refirió al caso del Banco de Chile en el año 2018 y el de Banco Estado recientemente, que significó incluso la interrupción de las operaciones en un momento determinado.

A nivel latinoamericano, comentó que en Colombia existe el Plan Nacional de Protección de Infraestructura Crítica y Cibernética, que define un marco de gobierno, roles, responsabilidades y un conjunto de niveles de alerta y actuación, y la notificación y respuesta frente a eventos de ciberseguridad asociados a sectores críticos.

Posteriormente indicó que, en España, el Sistema de Protección de Infraestructuras Críticas se articula en torno a la conformación del Centro Nacional para la Protección de la Infraestructuras Críticas, donde trabajan mancomunadamente actores públicos y privados.

Por su parte, aseveró que Estados Unidos cuenta con la National Infrastructure Coordinating Center (NICC), el cual forma parte de la Cybersecurity Division of the Cybersecurity and Infrastructure Security Agency, así como del Centro de Operaciones Nacionalesdel Departamento de Seguridad Interior, añadiendo que tienen un funcionamiento permanente y coordinado que permite compartir información situacional sobre infraestructura crítica federal.

A continuación, citó el caso de Estonia —en que el Cyber Security Council— es el encargado de aportar una cooperación más fluida entre diversos organismos públicos del país, velando por el cumplimiento de metas y estrategias de ciberseguridad desde un punto de vista público y privado.

Finalmente, indicó que el Reino Unido a través del National Cyber Security Center respalda a organizaciones críticas del Estado.

En lo que respecta al proyecto de ley, observó ciertos elementos que según estimó debiesen ser estudiados en la discusión en particular.

1.) En cuanto a las definiciones, citó el caso de los denominados “servicios esenciales” del artículo 2° numeral 15). En ese contexto, manifestó la importancia de definir cuáles serán esos servicios esenciales, por lo que sugirió —dada la estructura del conjunto de definiciones— debiera establecerse una norma genérica que diga que se considerarán también como servicios esenciales “aquellos que sean calificados como estratégicos por la autoridad”.

Advirtió que de la definición dada en el proyecto sobre “servicios esenciales”, no se encuentra, por ejemplo, la industria del cobre que, en su opinión, una paralización o ataque a este sector puede significar una afectación estructural de la economía nacional.

2.) En lo que dice relación con los principios del artículo 3° numeral 8), junto con el artículo 7° sobre facultades normativas y el artículo 8° en cuanto a la definición de la Agencia Nacional de Ciberseguridad, cuestionó que el régimen de esta ley sea supletorio, considerándolo inadecuado. Postuló que ese debiese ser el marco general aplicable al sector público y privado, y además que exista una coordinación entre la Agencia y las autoridades reguladoras sectoriales. Por lo anterior, estimó que, de quedar como una ley supletoria, la convertirá en una regulación de escasa aplicación.

Asimismo, opinó que, sin perjuicio que en la estructura orgánica de esta norma se incorpore al regulador sectorial, la Agencia Nacional de Ciberseguridad no debe quedar sometida a lo que decida este regulador, sino que se debe propiciar el trabajo conjunto. Puso el caso en que el regulador sectorial establezca una norma particular en materia de ciberseguridad, con estándares que no sean compatibles con aquellos globales exigidos por la Agencia, lo que en la práctica provocaría que lo que diga esta última sea letra muerta. Añadió sobre este punto, que también puede haber diferencias de criterios desde el punto de vista normativo y sancionador, lo que graficó respecto de lo que sucede en las investigaciones que lleve a cabo el Ministerio Público en estas materias. En ese sentido, explicó que cuando este órgano requiera la participación de la autoridad sectorial como especialista en la materia, se tendrán diferentes criterios en la interpretación de las normas, su aplicación o en cuanto a lo que se entiende por estándares mínimos garantizados en la infraestructura crítica de la información.

En relación con estos planteamientos, el **Coordinador Nacional de Ciberseguridad del Ministerio del Interior y Seguridad Pública señor Daniel Álvarez,** manifestó compartir parte importante de las observaciones efectuadas. En efecto, indicó que, en cuanto a las definiciones, existen mejores marcos normativos de referencia que nos pueden llevar a reconsiderar el concepto de “servicios esenciales”, y reemplazarlo por “operadores de importancia vital”. Respecto a estos últimos, puntualizó que es una fórmula

mucho más dinámica de entender aquellos sectores de la economía o de la sociedad, que requieren de ciertas obligaciones especiales en materia de ciberseguridad.

En cuanto al carácter supletorio de la ley, concordó respecto a que se estima que la Agencia Nacional de Ciberseguridad sea el órgano rector de la ciberseguridad en Chile y que se coordine o incluso pueda supervisar a los entes regulados, para efectos que la eficacia material de las disposiciones que genere, tanto la propia ley como las instrucciones generales, particulares y normas técnicas, tengan la mayor penetración posible en la sociedad. Por lo tanto, adhirió a la opinión del señor Harboe, en cuanto a si se deja a la ley con un carácter supletorio, la fuerza de la Agencia se reducirá de manera considerable.

En otro orden de ideas, informó que, en materia de indicaciones, el Ejecutivo se encuentra evaluando cómo simplificar la estructura orgánica, de manera tal que la Agencia Nacional de Ciberseguridad sea una institución dinámica y que tenga la capacidad de hacerse cargo de los diversos desafíos y principalmente del cambio tecnológico. De este modo, reiteró su opinión de que el proyecto de ley abunda en exceso en definiciones técnicas, puesto que, en un corto tiempo, estas pueden quedar obsoletas.

En conclusión, indicó que las indicaciones a presentar estarán orientadas a que la ley se remita a regular procesos y resultados, además de ampliar su ámbito de aplicación a todo el sector público y privado. En efecto, señaló que, dado el estado de avance y el nivel de inmersión de las tecnologías digitales, es necesario que todos los actores tengan obligaciones en materia de ciberseguridad, ya sea con mayor o menos intensidad según la importancia del operador o del servicio esencial.

2) El **Director de la Unidad Especializada en Lavado de Dinero, Delitos Económicos, Delitos Medioambientales y Crimen Organizado (ULDECCO) del Ministerio Público, señor Mauricio Fernández** manifestó estar conteste con los comentarios del ex Senador señor Harboe, sin embargo, advirtió que el proyecto de ley no aborda la cibercriminalidad propiamente tal.

Comentó que un sistema como el que se pretende instaurar tiene mucha relación con la persecución penal, por lo que fue de la opinión que debe dialogar reguladamente con esta.

A mayor abundamiento, señaló que frente al tratamiento de múltiples incidentes de ciberseguridad que, además, pueden tener alguna connotación penal, debe haber alguna fórmula que permita un adecuado traspaso de información desde la Agencia Nacional de Ciberseguridad y el sistema de tratamiento de incidentes en ciberseguridad, al Ministerio Público. Lo anterior, dado que —a su entender— la ley debe hacerse cargo de aquellos casos en que no hay denuncia de hechos ilícitos en ciberseguridad, y que por

tal razón no llegan a la investigación criminal por falta de colaboración en ese sentido.

B.-Votación en general.

El señor Presidente de la Comisión, en atención a los planteamientos expuestos y la discusión habida en el seno de la Comisión, declaró cerrado el debate, procediendo a poner en votación en general la iniciativa legal, de manera de permitir que ella sea discutida, posteriormente por la Sala, para luego efectuar la discusión en particular, la que debiera ser realizada por las Comisiones de Defensa Nacional y la que preside, funcionando unidas.

- Puesto en votación el proyecto de ley, en general, fue aprobado por la unanimidad de sus integrantes, señores Huenchumilla, Insulza Quintana, Ossandón y Van Rysselberghe.

- - -

TEXTO DEL PROYECTO

De conformidad a lo precedentemente acordado, la Comisión de Seguridad Pública propone a la Sala la aprobación, en general, del texto despachado por la Comisión de Defensa Nacional en sus mismos términos, que es el siguiente:

PROYECTO DE LEY:

“TÍTULO I
Disposiciones generales

Artículo 1. Objeto. La presente ley tiene por objeto 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.

Artículo 2. Definiciones. Para efectos de esta ley se entenderá por:

1. Agencia: La Agencia Nacional de Ciberseguridad.

2. Ciberataque: 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.

3. Ciberespacio: Dominio global y dinámico dentro del entorno de la información que corresponde al ambiente compuesto por las infraestructuras tecnológicas, los 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.

Las infraestructuras tecnológicas corresponden a los equipos materiales empleados para la transmisión de las comunicaciones, tales como enlaces, enrutadores, conmutadores, estaciones, sistemas radiantes, nodos, conductores, entre otros.

Los componentes lógicos de la información, en tanto, son los diferentes softwares que permiten el funcionamiento, administración y uso de la red.

4. Ciberseguridad: 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.

5. Equipo de respuesta a incidentes de seguridad informática o CSIRT: Centros conformados por especialistas multidisciplinarios capacitados para prevenir, detectar, gestionar y responder a incidentes de ciberseguridad, en forma rápida y efectiva, y que actúan según procedimientos y políticas predefinidas, coadyuvando asimismo a mitigar sus efectos.

6. Estándares Mínimos de Ciberseguridad: Corresponden al conjunto de reglas y procedimientos técnicos básicos sobre ciberseguridad, dictados por la Agencia o por el regulador sectorial competente, los cuales deben ser cumplidos por los órganos de la Administración del Estado y por quienes posean infraestructura de la información calificada como crítica.

7. Gestión de incidente de Ciberseguridad: Conjunto ordenado de acciones enfocadas a prevenir en la medida de lo posible la ocurrencia de incidentes de ciberseguridad y, en caso de que ocurran, restaurar los niveles de operación lo antes posible.

8. Incidente de ciberseguridad: Todo evento que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas o datos informáticos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos a través sistemas de telecomunicaciones y su infraestructura, que puedan afectar al normal funcionamiento de los mismos.

9. Infraestructura Crítica de la Información: corresponde a 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 este debe proveer o garantizar.

10. Red o sistema de información: Medio en virtud del cual dispositivos, redes o plataformas almacenan, procesan o transmiten datos digitales, ya sea a través de redes de comunicaciones electrónicas, dispositivos o cualquier grupo de redes interconectadas o dispositivos o sistemas de información y plataformas relacionadas entre sí.

11. Regulador o fiscalizador sectorial: Son aquellos servicios públicos dentro de cuyas funciones se encuentra la regulación y/o supervigilancia de uno o más sectores regulados.

12. Resiliencia: Capacidad de las redes o sistemas de información para seguir operando pese a estar sometidos a un incidente de ciberseguridad o ciberataque, aunque sea en un estado degradado, debilitado o segmentado; y, también, la capacidad de restaurar con presteza sus funciones esenciales después de un incidente de ciberseguridad o ciberataque, por lo general con un efecto reconocible mínimo.

13. Riesgo: Toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes o sistemas de información. Se puede cuantificar como la probabilidad de materialización de una amenaza que produzca un impacto negativo en éstas.

14. Sector regulado: Sector que representa alguna actividad económica estratégica nacional, que se encuentra sometido a la supervigilancia de un regulador o fiscalizador sectorial.

15. 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.

16. Sistema informático: Todo dispositivo aislado o el conjunto de ellos, interconectados o relacionados entre sí, incluidos sus soportes lógicos, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

17. Vulnerabilidad: Debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.

Artículo 3. Principios rectores. En la aplicación de las disposiciones de esta ley se deberán observar los siguientes principios:

1. Principio de responsabilidad: aquel 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.

2. Principio de protección integral: se deberán determinar los riesgos potenciales que puedan afectar a las redes o sistemas de información y aplicar las medidas organizativas, de gestión y técnicas apropiadas para la protección de los mismos.

3. Principio de confidencialidad de los sistemas de información: los datos, conectividad y sistemas deberán ser exclusivamente accedidos por personas o entidades autorizadas a tal efecto, las que se encontrarán sujetas a las responsabilidades y obligaciones que señalen las leyes.

4. Principio de integridad de los sistemas informáticos y de la información: 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.

5. Principio de disponibilidad de los sistemas de información: los datos, conectividad y sistemas deben estar accesibles para su uso a demanda.

6. Principio de control de daños: 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.

7. Principio de cooperación con la autoridad: los órganos de la Administración del Estado y los privados deberán cooperar con la autoridad competente para resolver los incidentes de ciberseguridad, y, si es necesario, deberán cooperar entre diversos sectores, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios.

8. Principio de especialidad en la sanción: en materia sancionatoria, se preferirá la aplicación de la regulación sectorial por sobre la establecida en esta ley.

TÍTULO II
De la determinación de Infraestructura Crítica de la Información

Párrafo 1°
Determinación de la infraestructura crítica de la información

Artículo 4. Calificación de la infraestructura de la información como crítica. Cada dos años, el Ministerio del Interior y Seguridad Pública requerirá al Consejo Técnico de la Agencia Nacional de Ciberseguridad un informe que detalle cuáles son aquellos sectores o instituciones que posean infraestructura de la información que deba ser calificada como crítica.

Para determinar si en un sector o institución existe infraestructura de la información que deba calificarse como crítica, se deberán tener en consideración, al menos, los siguientes factores:

a) El impacto de una posible interrupción o mal funcionamiento de los componentes de la infraestructura de la información, evaluando:

i. La cantidad de usuarios potencialmente afectados y su extensión geográfica;

ii. El efecto e impacto en la operación de infraestructura y/o servicios de sectores regulados cuya afectación es relevante para la población;

iii. La potencial afectación de la vida, integridad física o salud de las personas; y

iv. La seguridad nacional y el ejercicio de la soberanía.

b) Capacidad del sistema informático, red o sistema de información o infraestructura afectada, para ser sustituido o reparado en un corto tiempo.

c) Pérdidas financieras potenciales por fallas o ausencia del servicio a nivel nacional o regional asociada al producto interno bruto (PIB).

d) Afectación relevante del funcionamiento del Estado y sus órganos.

Dentro de los ciento veinte días siguientes a la recepción del informe, el Ministerio del Interior y Seguridad Pública, mediante la dictación de un decreto supremo bajo la fórmula “Por orden del Presidente de la República”, determinará aquellos sectores o instituciones que constituyen servicios esenciales y poseen infraestructura crítica de la información. Se entenderá que por el hecho de determinar que un sector posee infraestructura crítica de la información, las instituciones que conformen ese sector también poseerán infraestructura crítica de la información.

Sin perjuicio de lo dispuesto en los incisos anteriores, 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.

Párrafo 2°
De las obligaciones de las instituciones que poseen infraestructura de la información calificada como crítica

Artículo 5. Deberes generales. Será obligación de los órganos del Estado y de las instituciones privadas que posean infraestructura de la información calificada como crítica, 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 e integridad del servicio prestado, de conformidad a lo prescrito en esta ley.

Artículo 6. Deberes específicos. Los órganos del Estado señalados en el inciso final del artículo 4º y las instituciones privadas cuya infraestructura de la información sea calificada como crítica, deberán:

a) Implementar un sistema de gestión de riesgo permanente con el fin de determinar aquellos que pueden afectar la seguridad de las redes, sistemas informáticos y datos, y cuáles afectarían la continuidad operacional del servicio y cuáles de ellos facilitan la ocurrencia de incidentes de

ciberseguridad. Dicho sistema debe contar con la capacidad de determinar la gravedad de las consecuencias de un incidente de ciberseguridad.

b) Mantener un registro de las acciones ejecutadas que compongan el sistema de gestión de riesgos, de conformidad a lo que señale el reglamento. Lo anterior incluirá el registro del cumplimiento de la normativa sobre ciberseguridad y del conocimiento por los empleados, dependientes y proveedores de los protocolos de ciberseguridad y la aplicación de los mismos, tanto durante el funcionamiento regular como en caso de haber sufrido un incidente de ciberseguridad.

c) Elaborar e implementar planes de continuidad operacional y ciberseguridad. Dichos planes deberán ser actualizados periódicamente, a lo menos una vez al año.

d) Realizar continuamente operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos, plataformas y sistemas para detectar acciones o programas informáticos que comprometan la ciberseguridad y comunicar la información relativa a dichas acciones o programas al CSIRT Sectorial respectivo o al CSIRT Nacional, según correspondiere, en la forma que determine el reglamento.

e) Adoptar las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad, incluida la restricción de uso o el acceso a sistemas informáticos, si fuera necesario.

f) Contar con las certificaciones de los sistemas de gestión y procesos que determine el reglamento.

Artículo 7. Facultades normativas. Los reguladores o fiscalizadores sectoriales podrán dictar instrucciones, circulares, órdenes, normas de carácter general y las normas técnicas que sean necesarias para establecer los estándares particulares de ciberseguridad respecto de sus regulados o fiscalizados, de conformidad a la regulación sectorial respectiva, las que deberán considerar, a lo menos, los estándares establecidos por la Agencia Nacional de Ciberseguridad.

TÍTULO III
De la Agencia Nacional de Ciberseguridad

Párrafo 1°
Objeto, naturaleza y atribuciones

Artículo 8. Agencia Nacional de Ciberseguridad. Créase la Agencia Nacional de Ciberseguridad, como un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propios, de carácter técnico y especializado, cuyo objeto será asesorar al Presidente de la

República en materias propias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en materia de ciberseguridad y regular y fiscalizar las acciones de los órganos de la Administración del Estado y privados que no se encuentren sometidos a la competencia de un regulador o fiscalizador sectorial, y que posea infraestructura de la información calificada como crítica, según los preceptos de esta ley. Se relacionará con el Presidente de la República por intermedio del Ministerio del Interior y Seguridad Pública.

La Agencia tendrá domicilio en la ciudad de Santiago, sin perjuicio de contar con oficinas en otras localidades o regiones del país.

Artículo 9. Atribuciones. Para dar cumplimiento a su objeto, la Agencia tendrá las siguientes atribuciones:

a) Asesorar al Presidente de la República, en el análisis y definiciones de la política nacional de ciberseguridad, así como los planes y programas de acción específicos para su ejecución y cumplimiento, así como en temas relativos a estrategias de avance en su implementación.

b) 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, según corresponda.

c) Proponer al Ministro del Interior y Seguridad Pública las normas legales y reglamentarias que se requieran para asegurar el acceso libre y seguro al ciberespacio, así como aquellas que estén dentro del marco de su competencia.

d) Coordinar a los CSIRT Sectoriales y a aquellos que pertenezcan a órganos del Estado señalados en el inciso final del artículo 4º, a instituciones privadas y al CSIRT Nacional, en lo relativo a los estándares y tiempos de comunicación de incidentes de ciberseguridad o vulnerabilidades.

e) Administrar el Registro Nacional de Incidentes de Ciberseguridad.

f) Fomentar la investigación, innovación, capacitación y entrenamiento frente a amenazas, vulnerabilidades e incidentes de ciberseguridad.

g) Requerir de los CSIRT Sectoriales y del CSIRT Nacional la información que sea necesaria para el cumplimiento de sus fines y que sea de responsabilidad de estas instituciones.

h) Diseñar e implementar planes y acciones de educación, formación ciudadana, investigación, innovación, entrenamiento, fomento y difusión, destinados a promover el desarrollo nacional de una cultura de ciberseguridad.

i) Suscribir convenios con órganos del Estado e instituciones privadas destinados a facilitar la colaboración y la transferencia de información que permita el cumplimiento de los fines de la Agencia.

j) Cooperar con organismos públicos, instituciones privadas y organismos internacionales, en materias propias de su competencia, en coordinación con el Ministerio de Relaciones Exteriores, cuando corresponda.

k) Prestar asesoría técnica a los órganos del Estado e instituciones privadas cuya infraestructura de la información haya sido calificada como crítica, que estén o se hayan visto afectados por un incidente de ciberseguridad que haya comprometido sus activos informáticos críticos o haya afectado el funcionamiento de su operación, cautelando siempre los deberes de reserva de información que esta ley le impone, así como los consagrados por la ley N° 19.628.

l) Colaborar y coordinar con organismos de Inteligencia, para enfrentar amenazas que puedan afectar a la infraestructura crítica de información e implementar acciones preventivas.

m) Fiscalizar y sancionar el cumplimiento de esta ley, sus reglamentos y la normativa técnica que se dicte en conformidad con la presente ley, cuando ello no corresponda a un regulador o fiscalizador sectorial, según corresponda.

n) Informar a la Agencia Nacional de Inteligencia sobre riesgos e incidentes de ciberseguridad.

o) Conjuntamente con el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, diseñar planes y acciones que fomenten la investigación, innovación y desarrollo de la industria de ciberseguridad local.

p) Realizar todas aquellas otras funciones que las leyes le encomienden especialmente.

Párrafo 2°
Dirección, organización y patrimonio

Artículo 10. Dirección de la Agencia. La dirección y administración superior de la Agencia estará a cargo de un Director Nacional, quien será el jefe superior del Servicio, tendrá la representación legal, judicial y extrajudicial del mismo y será designado conforme a las normas del Sistema de Alta

Dirección Pública establecidas en la ley Nº 19.882, que regula la nueva política de personal a los funcionarios públicos que indica.

Artículo 11. Atribuciones del Director Nacional. Corresponderá especialmente al Director Nacional:

a) Planificar, organizar, dirigir, coordinar y controlar el funcionamiento de la Agencia;

b) Establecer oficinas regionales cuando el buen funcionamiento del Servicio así lo exija;

c) Dictar las resoluciones y demás actos administrativos necesarios para el buen funcionamiento de la Agencia;

d) Dictar, mediante resolución, la normativa que de acuerdo a esta ley corresponda dictar a la Agencia;

e) Ejecutar los actos y celebrar los convenios necesarios para el cumplimiento de los fines de la Agencia. En el ejercicio de esta facultad, podrá libremente administrar, adquirir y enajenar bienes de cualquier naturaleza;

f) Delegar atribuciones o facultades específicas en funcionarios de las plantas directiva, profesional o técnica de la Agencia, y

g) Instruir la apertura de procedimientos administrativos sancionadores, designar a los funcionarios a cargo, determinar las sanciones e imponerlas, respecto de los órganos de la Administración del Estado, en los términos señalados en el artículo 32 y respecto de aquellos privados que posean infraestructura de la información calificada como crítica, que no estén sujetos a un regulador o fiscalizador sectorial específico.

Artículo 12. Del patrimonio de la Agencia. El patrimonio de la Agencia estará constituido por:

a) Los recursos que anualmente le asigne la Ley de Presupuestos del Sector Público;

b) Los recursos otorgados por leyes generales o especiales;

c) Los bienes muebles e inmuebles, corporales e incorporales, que se le transfieran o que adquiera a cualquier título;

d) Los frutos, rentas e intereses de sus bienes y servicios.

e) Las donaciones que se le hagan, así como las herencias o legados que acepte, lo que deberá hacer con beneficio de inventario. Dichas donaciones y asignaciones hereditarias estarán exentas de toda clase de impuestos y de todo gravamen o pago que les afecten. Las donaciones no requerirán del trámite de insinuación;

f) Los aportes de la cooperación internacional que reciba a cualquier título, en coordinación con el Ministerio de Relaciones Exteriores; y

g) Los demás aportes que perciba en conformidad a la ley.

Artículo 13. Nombramiento de autoridades. La Agencia estará afecta al Sistema de Alta Dirección Pública establecido en la ley Nº 19.882, que regula la nueva política de personal a los funcionarios públicos que indica.

Artículo 14.- Del personal de la Agencia. El personal de la Agencia se regirá por las normas del Estatuto Administrativo.

Artículo 15.- De la estructura interna de la Agencia. Un reglamento expedido por el Ministerio del Interior y Seguridad Pública, determinará la estructura interna del Servicio, de conformidad con lo dispuesto en la ley N° 18.575, orgánica constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado que fue fijado por el decreto con fuerza de ley N° 1, de 2000, del Ministerio Secretaría General de la Presidencia, con sujeción a la planta y dotación máxima del personal.

Párrafo 3°
Registro Nacional de Incidentes de Ciberseguridad

Artículo 16. Del Registro Nacional de Incidentes de Ciberseguridad. Créase el Registro Nacional de Incidentes de Ciberseguridad, el que será administrado por la Agencia Nacional de Ciberseguridad y tendrá el carácter de reservado, por exigirlo el debido cumplimiento de las funciones de la Agencia, el debido resguardo de los derechos de las personas y la seguridad de la nación. En este registro 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 de la información calificada como crítica, que corresponda al caso.

Un reglamento expedido por el Ministerio del Interior y Seguridad Pública contendrá las disposiciones necesarias para regular la forma en que se confeccionará el referido registro, la operación del mismo y toda otra norma necesaria para su adecuado funcionamiento.

Párrafo 4°
Consejo Técnico de la Agencia Nacional de Ciberseguridad

Artículo 17. Consejo Técnico de la Agencia Nacional de Ciberseguridad. Créase el Consejo Técnico de la Agencia Nacional de Ciberseguridad, en adelante el “Consejo”, 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.

El Consejo estará integrado por el Director Nacional de la Agencia, quien lo presidirá, y cuatro consejeros designados por el Presidente de la República, mediante decreto supremo expedido a través del Ministerio del Interior y Seguridad Pública, entre personas de destacada labor en el ámbito de la ciberseguridad y/o de políticas públicas vinculadas a la materia, quienes permanecerán en su cargo durante seis años, renovándose en pares cada tres años, pudiendo ser reelegidos en sus cargos por una sola vez.

Los integrantes del Consejo estarán obligados a presentar una declaración de intereses y de patrimonio, en conformidad a lo dispuesto por la ley N° 20.880, sobre probidad en la función pública y prevención de los conflictos de intereses y estarán afectos al principio de abstención contenido en el artículo 12 de la ley Nº 19.880.

Artículo 18. Funciones del Consejo. Corresponderá al Consejo:

a) Asesorar a la Agencia en materias relacionadas con la ciberseguridad y la protección y aseguramiento de la Infraestructura Crítica de la Información;

b) Elaborar el informe que señala el artículo 4º de esta ley, relativo a la determinación de los sectores o instituciones que posean infraestructura de la información que deba ser calificada como crítica;

c) Asesorar en la redacción de propuestas de normas técnicas que la Agencia genere, y;

d) Asesorar a la Agencia en todas aquellas materias que ésta solicite.

Artículo 19. Funcionamiento del Consejo. El Consejo sólo podrá sesionar con la asistencia de, al menos, tres de sus miembros, previa convocatoria del Director de la Agencia. Sin perjuicio de lo anterior, el Presidente del Consejo estará obligado a convocar a una sesión extraordinaria cuando así lo requieran, por escrito, a lo menos tres de sus miembros. En todo

caso, el Consejo podrá autoconvocarse en situaciones urgentes o necesarias conforme a la decisión de la mayoría de sus integrantes.

El Consejo sesionará todas las veces que sea necesario para el cumplimiento oportuno y eficiente de sus funciones, debiendo celebrar sesiones ordinarias a lo menos una vez cada dos meses, con un máximo de doce sesiones pagadas por cada año calendario, y sesiones extraordinarias cuando las cite especialmente el Presidente del Consejo, o cuando aquéllas se citen por medio de una autoconvocatoria del Consejo. Podrán celebrarse un máximo de cuatro sesiones extraordinarias pagadas por cada año calendario.

Los acuerdos del Consejo se adoptarán por la mayoría absoluta de los consejeros presentes. El Presidente del Consejo tendrá voto dirimente en caso de empate. De los acuerdos que adopte el Consejo deberá dejarse constancia en el acta de la sesión respectiva. Podrán declararse secretas las actas en que, de conformidad a la ley, se traten materias que afectaren el debido cumplimiento de las funciones de la Agencia, la seguridad de la Nación o el interés nacional.

Cada uno de los integrantes del Consejo, con excepción de su Presidente, percibirá una dieta de quince unidades de fomento por cada sesión a la que asista, con un tope máximo de doce sesiones por año calendario. Esta dieta será compatible con otros ingresos que perciba el consejero.

Un reglamento expedido por el Ministerio del Interior y Seguridad Pública determinará las demás normas necesarias para el correcto funcionamiento del Consejo.

Artículo 20. Incompatibilidades de los miembros del Consejo. No podrán ser designados consejeros las personas que desempeñen empleos o comisiones retribuidos con fondos del Fisco, de las municipalidades, de las entidades fiscales autónomas, semifiscales, de las empresas del Estado o en las que el Fisco tenga aportes de capital, y con toda otra función o comisión de la misma naturaleza. Exceptúese a los empleos docentes y las funciones o comisiones de igual carácter de la enseñanza superior, media o especial.

Artículo 21. De las causales de cesación. Serán causales de cesación en el cargo de consejero las siguientes:

a) Expiración del plazo por el que fue designado.

b) Renuncia voluntaria aceptada por la autoridad que realizó la designación.

c) Incapacidad física o síquica para el desempeño del cargo.

d) Fallecimiento.

e) Sobreviniencia de alguna causal de incompatibilidad de las contempladas en el artículo 19.

f) Haber sido condenado por delitos que merezcan pena aflictiva por sentencia firme o ejecutoriada.

g) Falta grave al cumplimiento de las obligaciones como consejero. Para estos efectos, se considerará falta grave:

i. Inasistencia injustificada a dos sesiones consecutivas.

ii. No guardar la debida reserva respecto de la información recibida en el ejercicio de su cargo que no haya sido divulgada oficialmente.

El consejero respecto del cual se verificare alguna de las causales de cesación referidas anteriormente deberá comunicar de inmediato dicha circunstancia al Consejo. Respecto de la causal de la letra f), la concurrencia de dichas circunstancias facultará al Presidente de la República para decretar la remoción. Con todo, tratándose del ordinal ii) de dicho literal, será necesario, para cursar la remoción, la presentación de la respectiva querella por el delito de violación de secretos contemplado en los artículos 246, 247 y 247 bis del Código Penal.

Tan pronto como el Consejo tome conocimiento de que una causal de cesación afecta a un consejero, el referido consejero cesará automáticamente en su cargo.

Si quedare vacante el cargo de consejero deberá procederse al nombramiento de uno nuevo de conformidad con el procedimiento establecido en esta ley. El consejero nombrado en reemplazo durará en el cargo sólo por el tiempo que falte para completar el período del consejero reemplazado.

Párrafo 5°
Equipo Nacional de Respuesta a Incidentes de Seguridad Informática

Artículo 22. Equipo Nacional de Respuesta a Incidentes de Seguridad Informática. Créase dentro de la Agencia Nacional de Ciberseguridad el Equipo Nacional de Respuesta ante Incidentes de Seguridad Informática, en adelante “CSIRT Nacional”, el que tendrá las siguientes funciones:

a) 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 no sometidas a la supervigilancia de un regulador o

fiscalizador sectorial y que posean infraestructura de la información calificada como crítica, de conformidad a lo prescrito en esta ley.

b) Coordinar a los CSIRT Sectoriales frente a ataques, vulnerabilidades, incidentes y brechas de ciberseguridad.

c) Servir de punto de enlace con Equipos de Respuesta a Incidentes de Seguridad Informática extranjeros o sus equivalentes, para el intercambio de información de ciberseguridad, siempre dentro del marco de sus competencias.

d) Prestar colaboración o asesoría técnica a los CSIRT Sectoriales en la implementación de políticas y acciones relativas a ciberseguridad.

e) Ofrecer soporte a los CSIRT Sectoriales para asegurar la resiliencia de estos en caso de fallas operacionales graves, incidentes de ciberseguridad o ciberataques.

f) Consolidar y tratar los datos técnicos y antecedentes que describen la ocurrencia de incidentes de ciberseguridad, ciberataques, vulnerabilidades y demás información para efectos de la alimentación del registro previsto en los términos del artículo 16.

g) Realizar entrenamiento, educación y capacitación en materia de ciberseguridad, con la finalidad de procurar que los órganos del Estado e instituciones privadas que posean infraestructura de la información calificada como crítica cuenten con las competencias adecuadas para dar respuesta a incidentes de ciberseguridad o ciberataques.

h) Requerir a los CSIRT Sectoriales, dentro del ámbito de su competencia, información anonimizada de incidentes de ciberseguridad y vulnerabilidades encontradas y los planes de acción respectivos para mitigarlos.

i) Responder, conjuntamente con uno o más CSIRT Sectoriales, en la gestión de un incidente de ciberseguridad o de un ciberataque, dependiendo de las capacidades y competencias de los órganos del Estado que concurren a su gestión, cuando estos puedan ocasionar un impacto significativo en el sector, institución u órgano del Estado, según corresponda. En estos casos, el CSIRT Nacional podrá recomendar, colaborar, compartir información, coordinar y realizar todas las acciones conjuntas necesarias para asegurar una respuesta rápida frente al incidente. Además, podrá supervisar la implementación de medidas de mitigación de corto plazo, e informarse de las medidas de largo plazo adoptadas.

j) Generar y difundir información mediante campañas públicas y prestar asesoría técnica general a personas naturales o jurídicas, que no se encuentran reguladas por esta ley, que estén o se hayan visto afectadas por un

incidente de ciberseguridad que haya comprometido sus activos informáticos críticos o hayan afectado el funcionamiento de su operación.

k) Crear y administrar para el cumplimiento de sus funciones una red electrónica de comunicaciones segura destinada a comunicar y compartir información con los otros CSIRT Sectoriales, de Gobierno y Defensa. El funcionamiento de la red de comunicaciones se establecerá en el reglamento de la presente ley.

TÍTULO IV
De los equipos de respuesta a incidentes de seguridad informática sectoriales

Artículo 23. CSIRT Sectoriales. Los reguladores o fiscalizadores sectoriales podrán constituir Equipos de Respuesta a Incidentes de Seguridad Informática Sectoriales, en adelante 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.

Un reglamento expedido por el Ministerio del Interior y Seguridad Pública establecerá las instancias de coordinación entre la Agencia Nacional de Ciberseguridad, los reguladores y fiscalizadores sectoriales, así como de sus respectivos CSIRT, dentro del marco que fija esta ley.

Artículo 24. Funciones de los CSIRT Sectoriales. Corresponderá a los CSIRT Sectoriales:

a) Responder ante incidentes de ciberseguridad que vulneren o pongan en riesgo las instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información que afecten a los órganos de la Administración de Estado y de las instituciones privadas de su sector.

b) Coordinar a los equipos CSIRT, o sus equivalentes, de los órganos del Estado y de las instituciones privadas de su sector frente a ataques, vulnerabilidades, incidentes y brechas de ciberseguridad.

c) Prestar colaboración o asesoría técnica en la implementación de políticas y acciones relativas a ciberseguridad a los CSIRT de las instituciones reguladas.

d) Ofrecer soporte a los CSIRT de las instituciones reguladas para asegurar la resiliencia de estos en caso de fallas operacionales graves, incidentes de ciberseguridad o ciberataques.

e) Realizar entrenamiento, educación y capacitación en materia de ciberseguridad, con la finalidad de procurar que los órganos de la

Administración de Estado de su sector y de las instituciones reguladas cuenten con las competencias adecuadas para dar respuesta a incidentes de ciberseguridad o ciberataques.

f) Requerir a los CSIRT de sus instituciones reguladas, dentro del ámbito de su competencia, información anonimizada de incidentes de ciberseguridad y vulnerabilidades encontradas.

g) Generar y difundir información mediante campañas públicas dentro de su sector.

h) Trabajar conjuntamente con el CSIRT Nacional y con otros sectoriales, cuando corresponda, en la gestión de un incidente de ciberseguridad en los casos y forma previstas en el literal i) del artículo 20 de esta ley.

i) Informar al CSIRT Nacional, de vulnerabilidades, incidentes de ciberseguridad y ciberataques detectados o reportados en su sector, junto a sus respectivos cursos o planes de acción para subsanarlos.

j) Prestar asesoría técnica a los órganos de la Administración de Estado de su sector y a sus instituciones reguladas, que estén o se hayan visto afectadas por un incidente de ciberseguridad que haya comprometido sus activos informáticos críticos o hayan afectado el funcionamiento de su operación.

k) Difundir las alertas preventivas e informaciones de ciberseguridad emanadas por el CSIRT Nacional a los órganos de la Administración de Estado de su sector y a sus instituciones reguladas.

Artículo 25. Deber general de informar. La Agencia informará a cada CSIRT Sectorial los reportes o alarmas de incidentes de ciberseguridad, vulnerabilidades existentes, conocidas o detectadas, y los planes de acciones sugeridos para subsanar dichas brechas de ciberseguridad.

Cada CSIRT Sectorial informará a los órganos de la Administración de Estado y a las instituciones privadas de su sector que posean infraestructura de la información calificada como crítica sobre vulnerabilidades existentes o detectadas en ella, y elaborará recomendaciones para subsanar dichas brechas de ciberseguridad.

Cada CSIRT Sectorial deberá informar a su sector regulado de manera anonimizada de los reportes de incidentes de ciberseguridad, vulnerabilidades existentes, conocidas o detectadas y de los cursos de acción tomada en cada caso.

Toda institución que posea infraestructura de la información calificada como crítica tiene la obligación de informar a su respectivo CSIRT los reportes de incidentes de ciberseguridad e informar respecto del plan de acción que adoptó frente a esta en un plazo no superior a 24 horas, prorrogable, por una sola vez por el mismo plazo, contado desde que se tuvo conocimiento de su ocurrencia. Lo anterior se entiende sin perjuicio de la facultad del regulador de solicitar el cumplimento de esta obligación en un plazo menor si lo considera necesario.

Artículo 26. Deber especial de información a la Agencia. Los CSIRT Sectoriales deberán informar a la Agencia, a más tardar una hora después de haber verificado la existencia de un incidente de ciberseguridad, cuando este ha tenido un impacto significativo en la seguridad del sistema informático de una institución que posee infraestructura de la información calificada como crítica o en la continuidad de un servicio esencial.

Se considera que un incidente de ciberseguridad tiene impacto significativo si cumple al menos una de las siguientes condiciones:

a) Afecta a una gran cantidad de usuarios.

b) La interrupción o mal funcionamiento es de larga duración.

c) Afecta a una extensión geográfica considerable.

d) Afecta sistemas de información que contengan datos personales.

e) Afecta la integridad física, la salud, o la vida cotidiana de las personas, de manera significativa.

Corresponderá calificar el impacto significativo a los reguladores o fiscalizadores sectoriales o a la Agencia, según corresponda.

La obligación de tomar las providencias necesarias para apoyar en el restablecimiento del servicio afectado no deja sin efectos el deber de los CSIRT Sectoriales de notificar a la Agencia de la ocurrencia de un incidente de ciberseguridad en el plazo indicado en el inciso primero.

Deberán omitirse en los reportes de incidentes de ciberseguridad todo dato o información personal, conforme a lo dispuesto en el artículo 2 letra f) de la ley N°19.628 sobre Protección de la Vida Privada. Para efectos de lo dispuesto en este inciso, no se considerará que la dirección IP sea un dato o información personal.

El procedimiento específico para notificar un incidente de ciberseguridad, la forma, así como las condiciones de anonimato, la taxonomía

del informe y la periodicidad serán establecidos en el reglamento de la presente ley.

TÍTULO V
De los CSIRT del sector público

Artículo 27. Equipo de Respuesta ante Incidentes de Seguridad Informática del Sector Gobierno. Créase en la Agencia el Equipo de Respuesta a Incidentes de Seguridad Informática de Gobierno, en adelante CSIRT de Gobierno. El CSIRT de Gobierno para todos los efectos, se clasificará como un CSIRT sectorial, responsable de la prevención, contención, protección, detección, recuperación de los sistemas y respuesta, asociados a instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información del Estado. Tendrá las siguientes funciones principales:

a) Responder ante incidentes de ciberseguridad que vulneren o pongan en riesgo las instalaciones, redes, sistemas, plataformas, servicios y equipos físicos y de tecnología de la información que afecten a los órganos de la Administración del Estado.

b) Asegurar la implementación de los protocolos y estándares mínimos de ciberseguridad establecidos por la Agencia, en los órganos de la Administración de Estado.

c) Gestionar los ciberataques, incidentes, y vulnerabilidades detectadas, informando estas situaciones al CSIRT Nacional de acuerdo a las normas que se establezcan para tal efecto.

d) Difundir las alertas preventivas e informaciones de ciberseguridad emanadas por el CSIRT Nacional a los órganos de la Administración de Estado.

Artículo 28. Centro Coordinador del Equipo de Respuesta ante Incidentes de Seguridad Informáticos del Sector Defensa. Créase el Centro Coordinador del Equipo de Respuesta ante Incidentes Informáticos del Sector Defensa (CCCD o CSIRT Sectorial de Defensa), dependiente del Ministerio de Defensa Nacional, como el organismo dependiente del Comando Conjunto de Ciberdefensa, perteneciente al Estado Mayor Conjunto del Ministerio de Defensa Nacional, responsable de la coordinación y protección de la infraestructura de la información calificada como crítica, a su vez de los recursos digitales del sector Defensa, además de cumplir aquellas tareas que le sean encomendadas, con el propósito de resguardar la Seguridad Nacional.

Para efectos presupuestarios, dependerá del Ministerio de Defensa Nacional y, en lo que le sea aplicable, se regirá por la presente ley y por la reglamentación que dicte al efecto el Ministerio de Defensa.

Sus funciones principales serán las siguientes:

a) Responsable de la coordinación y enlace entre los diferentes CSIRT del sector Defensa (Ejército, Armada, Fuerza Aérea, Estado Mayor Conjunto, Subsecretaría de Defensa, Subsecretaría para las Fuerzas Armadas y otros órganos dependientes de dicho sector), con el objeto de asegurar la protección y defensa de los riesgos y amenazas presentes en el ciberespacio, que permitan preservar la confidencialidad, integridad y disponibilidad de la infraestructura de la información calificada como crítica del sector Defensa.

b) Asumir el rol de coordinador y enlace entre la Agencia y su CSIRT Nacional con el CSIRT Sectorial de Defensa, asegurando la cooperación, colaboración e intercambio de información pertinente que fortalezca la ciberseguridad.

c) Establecer los protocolos y estándares mínimos de ciberseguridad, tanto para la prevención, contención, protección, recuperación de los sistemas y respuesta dependientes de las Fuerzas Armadas y Estado Mayor Conjunto, considerando los lineamientos establecidos por la Agencia.

TÍTULO VI
De la reserva de información en el sector público en materia de ciberseguridad

Artículo 29. De la reserva de información. Se considerarán secretos y de circulación restringida, para todos los efectos legales, los antecedentes, datos, informaciones y registros que obren en poder de los CSIRT, sean el CSIRT Nacional, de Gobierno, Defensa o los CSIRT Sectoriales, 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.

Los estudios e informes que elabore la Agencia podrán eximirse de dicho carácter con la autorización su Director Nacional, en las condiciones que este indique.

Los funcionarios de CSIRT, sean del CSIRT Nacional, de Gobierno, Defensa o de los CSIRT Sectoriales, que hubieren tomado conocimiento de los antecedentes a que se refiere el inciso primero, estarán obligados a mantener el carácter secreto de su existencia y contenido aun después del término de sus funciones en los respectivos servicios.

De igual forma, será considerada secreta o reservada la información contenida en los sistemas de gestión de riesgos y los registros previstos en el

artículo 6º, entendiéndose para todo efecto que su divulgación, comunicación o conocimiento afectarán la seguridad de la Nación o el interés nacional.

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.

Artículo 30. Extensión de la obligación de reserva. 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.

Artículo 31. Deber de reserva de la Agencia. La Agencia cautelará especialmente la reserva de los secretos o información comercial sensible que llegare a conocer en el desempeño de su labor, como también el respeto a los derechos fundamentales de las personas, particularmente el respeto y resguardo del derecho a la vida privada y el derecho a la protección de datos personales.

Artículo 32. Sanciones. La infracción a las obligaciones dispuestas en el presente título, serán sancionadas en la forma prevista en los artículos 246, 247 o 247 bis, todos del Código Penal, según corresponda. Lo anterior es sin perjuicio de la responsabilidad administrativa que procediere.

TÍTULO VII
De las infracciones y sanciones

Artículo 33. De las infracciones. 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.

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.

La multa será fijada teniendo en consideración si el infractor adoptó las medidas necesarias para resguardar la seguridad informática de las operaciones, la probabilidad de ocurrencia del riesgo, la gravedad de los efectos de los ataques, la reiteración en la infracción dentro del plazo de tres años y la capacidad económica del infractor.

Cuando cualquiera de 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.

Las infracciones cometidas por funcionarios de la Administración del Estado o de los órganos del Estado se regirán por su respectivo estatuto sancionatorio.

Artículo 34. Procedimiento. Las sanciones que se cursen con motivo de las infracciones contempladas en el artículo precedente, serán impuestas por resolución del Director de la Agencia, de conformidad a lo dispuesto en esta ley.

El procedimiento sancionatorio deberá fundarse en un procedimiento racional y justo, que será establecido en un reglamento dictado por el Ministerio del Interior y Seguridad Pública y deberá, al menos, establecer:

a) El procedimiento para designar al funcionario de la Agencia que llevará adelante el procedimiento;

b) El contenido de la formulación de cargos, la cual deberá señalar circunstanciadamente los hechos constitutivos de infracción, las normas legales que fueron infringidas y la gravedad de la infracción;

c) El plazo para formular descargos, el cual no podrá ser inferior a 15 días hábiles;

d) Un periodo para rendir y observar la prueba, el cual no podrá ser inferior a 10 días hábiles, pudiendo aportar las partes los medios de prueba que estimen pertinentes;

e) La forma y contenido de la resolución que absuelve o condena, la cual deberá contener la exposición de los hechos, el razonamiento que permite arribar a la resolución y la decisión que acoge o desecha los cargos formulados.

Tratándose de sectores regulados, las sanciones serán impuestas por los reguladores o fiscalizadores sectoriales y el procedimiento corresponderá al determinado por la normativa sectorial respectiva.

Artículo 35. Agravante especial. Si como consecuencia de la perpetración de un delito resultare la destrucción, inutilización o alteración grave del funcionamiento de infraestructura crítica de la información, se impondrá la pena que corresponda, aumentada en un grado.

Lo mismo se observará cuando el delito consistiere en la alteración o supresión de los datos soportados por infraestructura de la información calificada como crítica o en la obstaculización del acceso o la alteración perjudicial del funcionamiento de un sistema informático que formare parte de la Infraestructura Crítica de la Información.

TÍTULO VIII
Del Comité Interministerial de Ciberseguridad

Artículo 36. Comité Interministerial de Ciberseguridad. Créase el Comité Interministerial de Ciberseguridad, en adelante el Comité, 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 servicios esenciales.

Artículo 37. De los integrantes del Comité. El Comité será presidido por el Subsecretario del Interior y estará integrado por los siguientes miembros permanentes:

a) Por el Subsecretario de Defensa o quien éste designe;

b) Por el Subsecretario de Relaciones Exteriores o quien éste designe;

c) Por el Subsecretario de Justicia o quien éste designe;

d) Por el Subsecretario General de la Presidencia o quien éste designe;

e) Por el Subsecretario de Telecomunicaciones o quien éste designe;

f) Por el Subsecretario de Economía y Empresas de Menor Tamaño o quien éste designe;

g) Por el Subsecretario de Hacienda o quien éste designe;

h) Por el Subsecretario de Minería o quien éste designe;

i) Por el Subsecretario de Energía o quien éste designe;

j) Por el Subsecretario de Ciencia, Tecnología, Conocimiento e Innovación o quien éste designe;

k) Por el Director Nacional de la Agencia Nacional de Inteligencia;

l) Por el Director Nacional de la Agencia Nacional de Ciberseguridad;

m) Por un representante de la Subsecretaría del Interior, experto en materias de ciberseguridad.

Con todo, el Comité podrá invitar a participar de sus sesiones a funcionarios de la Administración del Estado u otras autoridades públicas, así como a representantes de entidades internacionales, públicas o privadas, académicas y de agrupaciones de la sociedad civil o del sector privado.

Artículo 38. De la secretaría ejecutiva. El Comité contará con una Secretaría Ejecutiva radicada en la Agencia, la que prestará el apoyo técnico, administrativo y de contenidos para el desarrollo de las reuniones del Comité.

El Director Nacional de la Agencia dirigirá la Secretaría Ejecutiva y le corresponderá, entre otras funciones, despachar las convocatorias, según le instruya el Subsecretario del Interior; coordinar y registrar las sesiones del Comité e implementar los acuerdos que se adopten.

Artículo 39. De la información reservada. Constituido el Comité en sesión secreta, los funcionarios que estén en conocimiento de información

reservada que sea atingente a los fines del Comité, podrán compartirla para su análisis y no se podrá levantar acta mientras se encuentre en tal condición.

La revelación de la información será sancionada de conformidad al delito de violación de secretos contemplado en los artículos 246, 247 y 247 bis del Código Penal.

Artículo 40. Del reglamento. Un reglamento expedido por el Ministerio del Interior y Seguridad Pública fijará las normas de funcionamiento del Comité.

TÍTULO IX
De las modificaciones a otros cuerpos legales

Artículo 41. Incorpórase al siguiente literal k), nuevo, en el artículo 25 de la ley Nº 20.424, Estatuto Orgánico del Ministerio de Defensa Nacional:

"k) Conducir el Centro Coordinador CSIRT del Sector Defensa en coordinación con la Subsecretaría de Defensa.".

TÍTULO X
Disposiciones transitorias

Artículo Primero Transitorio.- Facúltase al Presidente de la República para que en el plazo de un año de publicada en el Diario Oficial la presente ley, establezca mediante uno o más decretos con fuerza de ley, expedidos por intermedio del Ministerio del Interior y Seguridad Pública, los que también deberán ser suscritos por el Ministro de Hacienda, las normas necesarias para regular las siguientes materias:

1. Fijar la planta de personal de la Agencia Nacional de Ciberseguridad.

En el ejercicio de esta facultad, el Presidente de la República deberá dictar todas las normas necesarias para la adecuada estructuración y operación de la planta de personal que fije, así como el número de cargos para cada planta, los requisitos específicos para el ingreso y promoción de dichos cargos, sus denominaciones y niveles jerárquicos para efectos de la aplicación de lo dispuesto en el Título VI de la ley Nº 19.882, que regula la nueva política de personal a los funcionarios públicos que indica, y en el artículo 8º del decreto con fuerza de ley Nº 29, de 2004, del Ministerio de Hacienda. Igualmente, fijará su sistema de remuneraciones y las normas necesarias para la fijación de las remuneraciones variables, en su aplicación transitoria.

Además, podrá establecer las normas para el encasillamiento del personal en la planta que fije, las que podrá incluir a los funcionarios que se

traspasen desde la Subsecretaría del Interior a la Agencia Nacional de Ciberseguridad.

2. Determinar la fecha para la entrada en vigencia de las plantas que fije, del traspaso y del encasillamiento que se practique. Además, fijará la fecha en que la Agencia entrará en funcionamiento, pudiendo contemplar un período para su implementación.

3. Determinar la dotación máxima de personal de la Agencia Nacional de Ciberseguridad, a cuyo respecto no regirá la limitación establecida en el inciso segundo del artículo 10 de la ley Nº 18.834.

4. Disponer, sin solución de continuidad, el traspaso de los funcionarios titulares de planta y a contrata, desde la Subsecretaría del Interior.

En el respectivo decreto con fuerza de ley que fije la planta de personal, se determinará la forma en que se realizará el traspaso y el número de funcionarios que serán traspasados por estamento y calidad jurídica, pudiéndose establecer, además, el plazo en que se llevará a cabo este proceso, quienes mantendrán, al menos, el mismo grado que tenía a la fecha del traspaso. A contar de la fecha del traspaso, el cargo del que era titular el funcionario traspasado se entenderá suprimido de pleno derecho en la planta de la institución de origen. Del mismo modo, la dotación máxima de personal se disminuirá en el número de funcionarios traspasados.

La individualización del personal traspasado se realizará a través de decretos expedidos bajo la fórmula "Por orden del Presidente de la República", por intermedio del Ministerio del Interior y Seguridad Pública. Conjuntamente con el traspaso del personal, se traspasarán los recursos presupuestarios que se liberen por este hecho.

5. Los requisitos para el desempeño de los cargos que se establezcan en el ejercicio de la facultad prevista en este artículo no serán exigibles para efectos del encasillamiento respecto de los funcionarios titulares y a contrata en servicio a la fecha de entrada en vigencia del o de los respectivos decretos con fuerza de ley. Asimismo, a los funcionarios o funcionarias a contrata en servicio a la fecha de entrada en vigencia del o de los respectivos decretos con fuerza de ley, y a aquellos cuyos contratos se prorroguen en las mismas condiciones, no les serán exigibles los requisitos que se establezcan en los decretos con fuerza de ley correspondientes.

El uso de las facultades señaladas en este artículo quedará sujeto a las siguientes restricciones, respecto del personal al que afecte:

a) No podrá tener como consecuencia ni podrán ser considerados como causal de término de servicios, supresión de cargos, cese de funciones o término de la relación laboral del personal traspasado.

b) No podrá significar pérdida del empleo, disminución de remuneraciones respecto del personal titular de un cargo de planta, modificación de los derechos estatutarios y previsionales del personal traspasado. Tampoco importará cambio de la residencia habitual de los funcionarios fuera de la Región en que estén prestando servicios, a menos que se lleve a cabo con su consentimiento.

c) Respecto del personal que en el momento del encasillamiento sea titular de un cargo de planta, cualquier diferencia de remuneraciones se pagará mediante una planilla suplementaria, la que se absorberá por los futuros mejoramientos de remuneraciones que correspondan a los funcionarios, excepto los derivados de reajustes generales que se otorguen a los trabajadores del sector público. Dicha planilla mantendrá la misma imponibilidad que aquella de las remuneraciones que compensa. Además, a la planilla suplementaria se le aplicará el reajuste general antes indicado.

d) Los funcionarios traspasados conservarán la asignación de antigüedad que tengan reconocida, así como también el tiempo computable para dicho reconocimiento.

6.Podrá disponer el traspaso, en lo que corresponda, de los bienes que determine, desde la Subsecretaría del Interior a la Agencia Nacional de Ciberseguridad.

Artículo Segundo Transitorio.- El Presidente de la República, sin sujetarse a lo dispuesto en el título VI de la ley Nº 19.882, podrá nombrar, a partir de la publicación de la presente ley, al primer Director 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. En el acto de nombramiento, el Presidente de la República fijará el grado de la escala única de sueldos y la asignación de alta dirección pública que le corresponderá al Director, siempre que no se encuentre vigente la respectiva planta de personal. La remuneración del primer Director se financiará con cargo al presupuesto de la Subsecretaría del Interior, incrementándose para ese solo efecto en un cargo su dotación máxima de personal, siempre que no se encuentre vigente la respectiva planta de personal.

Artículo Tercero Transitorio.- El Presidente de la República, por decreto supremo expedido por intermedio del Ministerio de Hacienda, conformará el primer presupuesto de la Agencia Nacional de Ciberseguridad y podrá modificar el presupuesto del Ministerio del Interior y Seguridad Pública. Para los efectos anteriores podrá crear, suprimir o modificar las partidas, capítulos, programas, ítems, asignaciones y glosas presupuestarias que sean pertinentes.

Artículo Cuarto Transitorio.- Dentro del plazo de ciento ochenta días posteriores a la publicación de la ley, el Ministerio del Interior y Seguridad Pública deberá expedir los reglamentos señalados en esta ley.

Artículo Quinto Transitorio.- En el tiempo intermedio en que los ministerios, subsecretarías, superintendencias y demás órganos de la Administración del Estado reguladores o fiscalizadores vinculados directamente con sectores regulados no cuenten con CSIRT Sectoriales operativos, o se encuentren en la etapa de creación de éstos, de conformidad a lo dispuesto en el artículo 22, el CSIRT Nacional tendrá, para todos los efectos legales, la calidad de CSIRT Sectorial correspondiente, con todas sus atribuciones y facultades.

Artículo Sexto Transitorio.- Para los efectos de la renovación parcial de los miembros del Consejo Técnico de la Agencia a que se refiere el inciso segundo del artículo 17, sus miembros durarán en sus cargos el número de años que a continuación se indica, sin perjuicio de que podrán ser designados por un nuevo período:

a) Dos consejeros durarán en sus cargos por un plazo de dos tres años;

b) Dos consejeros durarán en sus cargos por un plazo de seis años.

Artículo Séptimo Transitorio.- El mayor gasto fiscal que represente la aplicación de la presente ley durante su primer año presupuestario de vigencia se financiará con cargo al presupuesto el Ministerio del Interior y Seguridad Pública. No obstante lo anterior, el Ministerio de Hacienda con cargo a la partida presupuestaria Tesoro Público podrá suplementar dicho presupuesto en la parte del gasto que no pudiere financiar con esos recursos. Para los años siguientes, se financiará de acuerdo con lo determinen las respectivas leyes de Presupuestos del Sector Público.”.

- - -

Tratado y acordado en sesión celebrada el día 4 de octubre de 2022 con la asistencia de los Honorables Senadores señores Francisco Huenchumilla Jaramillo, José Miguel Insulza (Presidente), Manuel José Ossandón Irarrázabal, Jaime Quintana Leal y Enrique van Rysselberghe Herrera; y en sesión celebrada el día 11 de octubre de 2022, con la asistencia de los Honorables Senadores señores Francisco Huenchumilla Jaramillo, José Miguel Insulza (Presidente), Manuel José Ossandón Irarrázabal, Jaime Quintana Leal y Enrique van Rysselberghe Herrera.

Sala de la Comisión, a 12 de octubre de 2022.

FRANCISCO JAVIER VIVES DIBARRART
Secretario de Comisiones

RESUMEN EJECUTIVO

INFORME DE LA COMISIÓN DE SEGURIDAD PÚBLICA, RECAÍDO EN EL PROYECTO DE LEY, EN PRIMER TRÁMITE CONSTITUCIONAL, QUE ESTABLECE UNA LEY MARCO SOBRE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA DE LA INFORMACIÓN (BOLETÍN N° 14.847-06).

I. OBJETIVO (S) DEL PROYECTO PROPUESTO POR LA COMISIÓN: Establecer la institucionalidad necesaria para robustecer la ciberseguridad; ampliar y fortalecer el trabajo preventivo; formar una cultura pública en materia de seguridad digital; enfrentar las contingencias en el sector público y privado, y resguardar la seguridad de las personas en el ciberespacio.

II. ACUERDOS: aprobado en general por unanimidad (5x0).

III. ESTRUCTURA DEL PROYECTO APROBADO POR LA COMISIÓN: consta de 41 artículos permanentes y 7 disposiciones transitorias.

IV. NORMAS DE QUÓRUM ESPECIAL:

Hacemos presente que de conformidad a lo dispuesto en el artículo 38 de la Constitución Política de la República, los artículos 8; 9 letras a), b), d), h), l) y m); 10; 13; 17; 22; 23; 24 letra b); 27; 28; 34; 36; 37; 38 y 41, permanentes; y los artículos segundo; quinto y sexto de las disposiciones transitorias, tienen el carácter de normas orgánicas constitucionales, por lo que requieren para su aprobación de las cuatro séptimas parte de los senadores en ejercicio, según lo prevé el inciso segundo del artículo 66 de la Carta Fundamental:

Por su parte, los artículos 16; 29; 30; 31 y 39, permanentes, tienen el carácter de normas de quórum calificado, de conformidad al artículo 8°, inciso segundo, de la Constitución Política de la República, por lo que requieren para su aprobación de la mayoría absoluta de los senadores en ejercicio, según lo dispone el inciso tercero del artículo 66, de la Constitución Política de la República.

V. URGENCIA: Suma.

VI. ORIGEN E INICIATIVA: Senado. Mensaje de Su Excelencia el ex Presidente de la República señor Sebastián Piñera Echenique.

VII TRÁMITE CONSTITUCIONAL: primero.

VIII. INICIO TRAMITACIÓN EN EL SENADO: 15 de marzo de 2022.

IX. TRÁMITE REGLAMENTARIO: Primer informe, en general.

X. LEYES QUE SE MODIFICAN O QUE SE RELACIONAN CON LA MATERIA: 1.- Ley N° 20.424, estatuto orgánico del Ministerio de Defensa Nacional; 2.- Ley N° 21.180, sobre transformación digital del Estado; 3.- Ley N° 19.882, que regula nueva política de personal a los funcionarios públicos que indica; 4.- Decreto con fuerza de ley N° 29 de 2005, del Ministerio de Hacienda, que fija texto refundido, coordinado y sistematizado de la ley Nº 18.834, sobre Estatuto Administrativo; 5.-Ley N° 19.628, sobre protección de la vida privada; 6.- Ley N° 19.974, sobre el sistema de inteligencia del Estado y crea la Agencia Nacional de Inteligencia; 7.- DFL 1-19.653 de 2001, del Ministerio Secretaría General de la Presidencia, que fija texto refundido, coordinado y sistematizado de la ley Nº 18.575, orgánica constitucional de Bases Generales de la Administración del Estado; 8.- Ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado; 9.- Ley N° 20.880, sobre probidad en la función pública y prevención de los conflictos de intereses; 10.- Código Penal; 11.- Decreto N° 83, de 2017, del Ministerio de Relaciones Exteriores, que promulga el Convenio sobre la Ciberdelincuencia (Convenio de Budapest); 12.- Ley N° 21.459, que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest; 13.- Ley N° 21.113, que declara el mes de octubre como el de la ciberseguridad; 14.- Ley N° 18.168, general de telecomunicaciones; 15.- Decreto N° 533, de 2015, del Ministerio del Interior y Seguridad Pública, que crea el Comité Interministerial sobre Ciberseguridad; 16.- Instructivo Presidencial 1/2017, de 27 de abril de 2017, que aprueba e instruye la implementación de la Política Nacional de Ciberseguridad; 17.- Decreto N° 3, de 2018, del Ministerio de Defensa Nacional, que aprueba la Política de Ciberdefensa; 18.- Ley N° 21.130, que moderniza la legislación bancaria; 19.- Ley N° 20.453, que consagra el principio de neutralidad en la red para los consumidores y usuarios de internet; 20.- Decreto N° 60, de 2012, del Ministerio de Transportes y Telecomunicaciones, reglamento para la interoperación y difusión de mensajería de alerta, declaración y resguardo de la infraestructura crítica de telecomunicaciones e información sobre fallas significativas en los sistemas de telecomunicaciones; 21.- Decreto supremo N° 83, de 2005, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos, y 22.- Artículo 19, número 4°. de la Constitución Política de la República.

Valparaíso, a 12 de octubre de 2022.

FRANCISCO JAVIER VIVES DIBARRART
Secretario de Comisiones