INFORME DE LA COMISIÓN DE HACIENDA, 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

HONORABLE SENADO:

La Comisión de Hacienda tiene el honor de emitir su informe acerca del proyecto de ley de la referencia, en primer trámite constitucional, originado en Mensaje de Su Excelencia el ex Presidente de la República, señor Sebastián Piñera Echenique, con urgencia calificada de "discusión inmediata".

- - -

Cabe señalar que, de acuerdo a lo autorizado por la Sala del Senado con fecha 18 de octubre de 2022, el proyecto de ley fue considerado previamente en particular por las comisiones de Defensa Nacional y de Seguridad Pública, unidas.

A la Comisión de Hacienda, en tanto, le correspondió pronunciarse sobre los asuntos de su competencia, de conformidad con lo prescrito en el artículo 17 de la Ley Orgánica Constitucional del Congreso Nacional y a lo dispuesto por la Sala del Senado con fecha 15 de marzo de 2022.

- - -

A la sesión en que la Comisión analizó esta iniciativa de ley, asistieron, además de sus miembros, las siguientes personas:

Del Ministerio del Interior y Seguridad Pública, el Subsecretario, señor Manuel Monsalve; el Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, y la Jefa de la División Jurídica, señora Camila Barros.

La asesora del Honorable Senador Coloma, señora Carolina Infante.

El asesor del Honorable Senador Edwards, señor Ignacio Pinto.

El asesor del Honorable Senador García, señor

José Miguel Rey.

Los asesores del Honorable Senador Insulza, señora Lorena Escalona y señor Carlos Fernández.

El asesor del Honorable Senador Lagos, señor Reinaldo Monardes.

El asesor del Honorable Senador Núñez, señor Elías Mella.

De la Biblioteca del Congreso Nacional, el analista, señor Samuel Argüello.

- - -

NORMAS DE QUÓRUM ESPECIAL

En lo relativo a las normas de quórum especial, la Comisión de Hacienda se remite a lo consignado en el segundo informe de las comisiones de Defensa Nacional y de Seguridad Pública, unidas.

- - -

NORMAS DE COMPETENCIA DE LA COMISIÓN DE HACIENDA

De conformidad con su competencia, la Comisión de Hacienda se pronunció respecto de las siguientes disposiciones del proyecto de ley: artículo 6, inciso primero, en sus letras a), b) c), d), g) y h), artículo 8, inciso primero, artículo 9, letras f) e i), artículo 10, artículo 11, letra e), artículo 12, artículo 14, incisos quinto, sexto, séptimo, octavo noveno y final, artículo 19, inciso primero, artículo 21, inciso cuarto, artículo 25, artículo 32, artículo 33, incisos primero y quinto, artículo 36, incisos tercero y cuarto, y artículo 42, inciso segundo, permanentes; y artículos primero, segundo, tercero y séptimo transitorios. Lo hizo en los términos en que fueron aprobados por las comisiones de Defensa Nacional y de Seguridad Pública, unidas, como reglamentariamente corresponde de acuerdo con lo dispuesto en el artículo 41 del Reglamento de la Corporación.

- - -

Se deja constancia de que la Comisión de Hacienda no introdujo enmiendas al texto despachado por las comisiones de Defensa Nacional y de Seguridad Pública, unidas.

- - -

DISCUSIÓN

Previo a la consideración de los asuntos de competencia de la Comisión de Hacienda, en **sesión de 25 de abril de 2023**, se escuchó primeramente al **Coordinador Nacional de Ciberseguridad del Ministerio del Interior y Seguridad Pública, señor Daniel Álvarez**, quien refirió que el proyecto de ley objeto de estudio forma parte de la agenda de seguridad del Gobierno, por lo que existe un compromiso político para su despacho por el Congreso Nacional dentro de un plazo definido.

Asimismo, subrayó que se trata de una iniciativa que forma parte de la Política Nacional de Ciberseguridad y que se diseñó en el año 2017 durante el Gobierno de la ex Presidenta de la República, señora Michelle Bachelet, continuando, como parte de una política de Estado, en el Gobierno del ex Presidente de la República, señor Sebastián Piñera. Precisó que fue durante los últimos días de la Administración de este último mandatario que el proyecto de ley fue ingresado al Senado.

Relató que como actual Ejecutivo tomaron la decisión, considerando que se trataba de una política de Estado, de recoger la estructura que ya proponía el proyecto de ley e incluirle mejoras mediante indicaciones presentadas tanto por el Gobierno, como por los señores Senadores integrantes de las comisiones de Defensa Nacional y de Seguridad Pública, unidas.

Señaló que la iniciativa establece un modelo de gobernanza, creando la Agencia Nacional de Ciberseguridad como un órgano técnico a cargo de la ciberseguridad del país, con competencias sobre el sector público y privado, y con facultades normativas, fiscalizadoras y sancionadoras.

Refirió que también se incluyen otros ámbitos novedosos en la mencionada Agencia, como el de promover la educación, formación y generación de capacidades en materia de ciberseguridad, en coordinación con los otros órganos que componen la Administración del Estado.

Subrayó que uno de los cambios que se hicieron al modelo de gobernanza propuesto en su oportunidad es el de simplificarlo. Explicó que el proyecto de ley en su origen creaba mucha institucionalidad, no obstante, luego de que el actual Ejecutivo reuniese más información, tanto con el sector público como privado, se advirtió una carencia importante de profesionales o expertos en materia de ciberseguridad en el país. Precisó que son cerca de 38.000 especialistas los que faltan por año.

Por lo anterior, sostuvo que crear demasiada institucionalidad derivaría en un problema importante de dotación.

Finalmente, expresó que el consenso al que se arribó en las comisiones de Defensa Nacional y de Seguridad Pública, unidas, fue avanzar en un modelo organizacional como el que se propone tras los acuerdos alcanzados.

Luego, el **Subsecretario del Ministerio del Interior y Seguridad Pública, señor Manuel Monsalve**, en conjunto con el **señor Álvarez**, procedieron a efectuar una presentación, en formato ppt, del siguiente tenor:

Proyecto de ley marco sobre ciberseguridad e infraestructura crítica de la información (Boletín 14847)

IMPORTANCIA DE LA CIBERSEGURIDAD

- El Estado tiene el deber de proteger la información que las personas le entregan, cuidando así la confianza de la ciudadanía.

- Cuando el Estado no actúa en materia de ciberseguridad, las personas, sus derechos, patrimonio y seguridad se ven afectadas.

- Hoy es importante tener presente que **no estamos protegiendo computadores, estamos protegiendo a las personas y a la sociedad en su conjunto.**

- Los ataques al SERNAC, Estado Mayor Conjunto, Comisión Nacional de Acreditación, Ministerio de Justicia y al Poder Judicial dan cuenta de la urgencia e importancia legislar.

CIBERSEGURIDAD COMO POLÍTICA DE ESTADO

- La Política Nacional de Ciberseguridad, elaborada en el gobierno de la presidenta Michelle Bachelet**, fijó los lineamientos políticos del Estado de Chile para el resguardo de la seguridad de las personas y de sus derechos en el ciberespacio**.

- En el gobierno del presidente Sebastián Piñera, **se confirmó la PNCS como una política de Estado**, avanzando en su implementación, incluyendo la presentación de este proyecto de ley marco sobre ciberseguridad que hoy comenzamos a revisar.

- El programa del presidente Gabriel Boric **propuso la implementación robusta de la Política Nacional de**

Ciberseguridad, que debe necesariamente estar orientada hacia la protección de los derechos fundamentales de las personas.

PROYECTO DE LEY MARCO SOBRE CIBERSEGURIDAD

- Crea un modelo de gobernanza que promueve la **gestión de riesgos y la implementación de estándares de ciberseguridad**, para mejorar la prevención, contención, resolución y respuesta de incidentes y ciberataques.

- El modelo se basa en un sistema de **colaboración público-privada**, con obligaciones de ciberseguridad y sanciones diferenciadas por riesgos y tamaño.

- Crea la **Agencia Nacional de Ciberseguridad (ANCI)** con facultades regulatorias, fiscalizadoras y sancionatorias, y crea el **Consejo Multisectorial sobre Ciberseguridad**.

- Crea un Equipo Nacional de Respuesta a Incidentes de Seguridad Informática **(CSIRT Nacional**), habilita la creación de **CSIRT Sectoriales**, crea el **CSIRT de la Defensa Nacional**.

Agencia Nacional de Ciberseguridad (ANCI)

- Su función será **gestionar los incidentes de ciberseguridad, regular, fiscalizar y sancionar** las acciones de los organismos de la Administración del Estado y de las instituciones privadas en materia de ciberseguridad.

- Se relacionará con el Presidente de la República a través del Ministerio del Interior y Seguridad Pública.

- Dirección y administración superior a cargo de un Director o Directora Nacional, designado conforme a las normas del Sistema de Alta Dirección Pública.

- Personal se regirá por el Código del Trabajo, con aplicación de derechos, obligaciones y prohibiciones del Estatuto Administrativo, que sean pertinentes.

CSIRT Nacional

Organismo técnico creado al interior de la ANCI, responsable de:

- Responder a incidentes de seguridad informática cuando sean de impacto significativo;

- Coordinar a los CSIRT Sectoriales;

- Prestar colaboración o asesoría técnica a los CSIRT Sectoriales

- Supervisar incidentes a escala nacional;

- Realizar entrenamiento, educación y capacitación en materia de ciberseguridad;

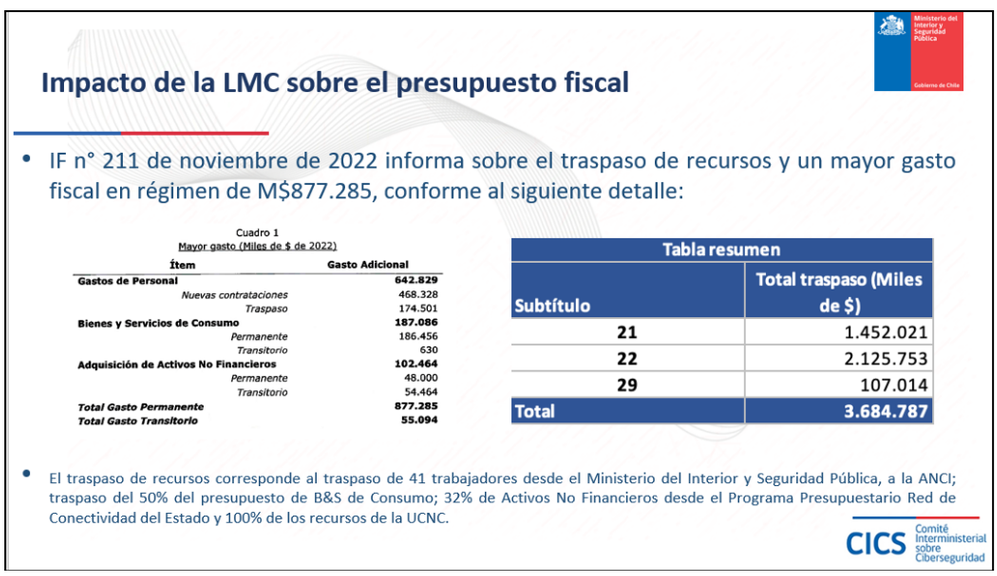
- Difundir alertas tempranas, avisos e información sobre riesgos e incidentes para la comunidad; entre otras.

Servicios esenciales – operadores de importancia vital

- LMC incorpora los conceptos de "**servicios esenciales**" y "**operadores de importancia vital**" para establecer un régimen de obligaciones de ciberseguridad y sanciones diferenciado según el riesgo para la vida de las personas y el impacto en el normal funcionamiento del país.

- Los **deberes específicos de alto estándar** se aplicarán a los organismos del Estado con competencias específicas sobre servicios esenciales y a las instituciones privadas calificadas como operadores de importancia vital.

- Los **demás protocolos y estándares** que establezca la ANCI, deberán ser diferenciados según el tipo de organización de que se trate y su relación con la prestación de servicios calificados como esenciales, teniendo especialmente en consideración las características y necesidades de las pequeñas y medianas empresas.



Impacto de la LMC sobre el presupuesto fiscal

- IF n° 211 de noviembre de 2022 informa sobre el traspaso de recursos y un mayor gasto fiscal en régimen de M$877.285, conforme al siguiente detalle:

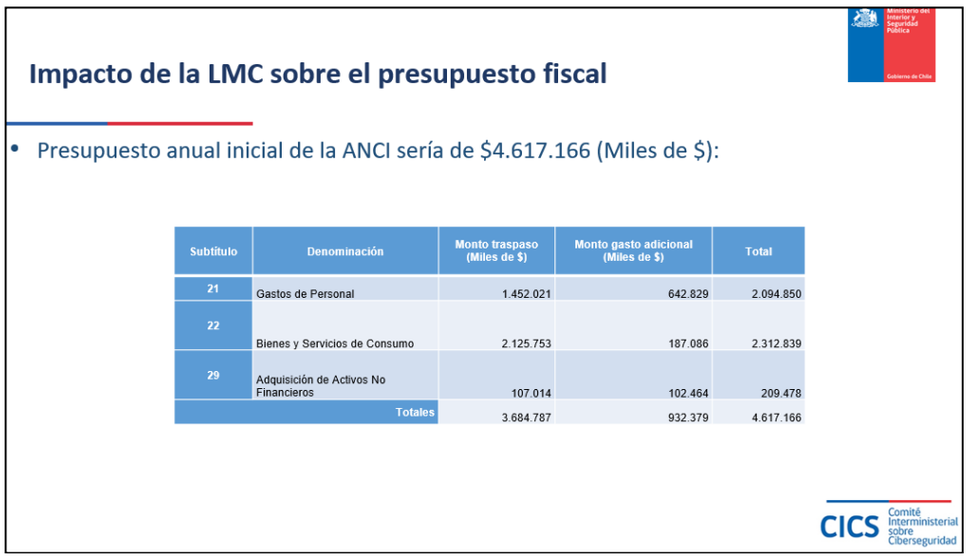
Cuadro 1
Mayor gasto (Miles de $ de 2022)

Ítem	Gasto Adicional
Gastos de Personal	**642.829**
Nuevas contrataciones	468.328
Traspaso	174.501
Bienes y Servicios de Consumo	**187.086**
Permanente	186.456
Transitorio	630
Adquisición de Activos No Financieros	**102.464**
Permanente	48.000
Transitorio	54.464
Total Gasto Permanente	**877.285**
Total Gasto Transitorio	**55.094**

Tabla resumen	
Subtítulo	Total traspaso (Miles de $)
21	1.452.021
22	2.125.753
29	107.014
Total	3.684.787

- El traspaso de recursos corresponde al traspaso de 41 trabajadores desde el Ministerio del Interior y Seguridad Pública, a la ANCI; traspaso del 50% del presupuesto de B&S de Consumo; 32% de Activos No Financieros desde el Programa Presupuestario Red de Conectividad del Estado y 100% de los recursos de la UCNC.

CICS Comité Interministerial sobre Ciberseguridad



Subtítulo	Denominación	Monto traspaso (Miles de $)	Monto gasto adicional (Miles de $)	Total
21	Gastos de Personal	1.452.021	642.829	2.094.850
22	Bienes y Servicios de Consumo	2.125.753	187.086	2.312.839
29	Adquisición de Activos No Financieros	107.014	102.464	209.478
	Totales	3.684.787	932.379	4.617.166

Al término de la presentación, el **Honorable Senador señor Edwards** manifestó que, si la Agencia Nacional de Ciberseguridad cuenta con facultades regulatorias, fiscalizadoras y sancionatorias, a su entender debiesen existir medios impugnatorios para los afectados, como podría ser reclamar ante alguna Corte de Apelaciones o ante la propia Agencia. Pidió aclarar este punto.

En segundo término, solicitó que se diera ejemplos de servicios esenciales y operadores de importancia vital, así como también de los deberes específicos que menciona la iniciativa legal.

Finalmente requirió mayor información sobre los recursos del Banco Interamericano de Desarrollo (BID) destinados a este proyecto de ley.

El **señor Subsecretario** se refirió a la última de las tres preguntas del Senador Edwards. Informó que en lo que respecta a la inversión inicial, que supone la dotación de equipamiento y tecnología para entregar respuestas ante incidentes de seguridad informática, una posibilidad para aquello es hacer uso de los recursos del crédito BID. Recordó que el mencionado crédito asciende a cerca de US$ 100 millones, que opera en un régimen mixto, ya que una mitad de los fondos es proporcionada por el BID y la otra mitad por el Estado.

Puntualizó que, pese a que se está pagando el crédito BID y tales recursos podrían ser utilizados para mejorar las capacidades informáticas, así como los equipamientos en materia de investigación policial, se trata de un crédito que ha tenido un muy bajo nivel de ejecución. Mencionó que en el año 2021 su ejecución fue cercana a cero, mientras que en el año 2022 fue de aproximadamente $5.000 millones.

Agregó que, en base a la historia de ejecución del crédito en los años anteriores, el Ministerio de Hacienda determinó para el año 2023, por concepto de gasto para el Ministerio del Interior y Seguridad Pública, la suma de $7.500 millones cargada al crédito BID, por lo que refirió que sigue subsistiendo un margen bastante amplio para poder hacer uso del mencionado crédito.

Reiteró que se trata de una inversión inicial, la que puede ser financiada mediante el uso del crédito BID.

El **señor Álvarez**, recogiendo las demás preguntas del señor Senador, informó que con ocasión de las sanciones se establece un procedimiento reglado en el proyecto de ley, el cual cuenta con mucho más detalle que otros procedimientos similares. Puso de relieve que en materia sancionatoria se consagra el principio *non bis in ídem*, considerando que se trata de una normativa que debe ser complementada con otras regulaciones, tanto sectoriales como generales.

En cuanto a las posibilidades de reclamación, observó que existe un recurso de reposición ante la misma autoridad que dicta la sanción, pero de igual manera se contempla un reclamo de ilegalidad ante la Corte de Apelaciones respectiva.

Enseguida, sobre ejemplos de operadores de importancia vital, refirió que originalmente el proyecto de ley utilizaba la expresión de “infraestructura crítica”, lo que estaba muy asociado a un elemento físico, no obstante, precisó que el énfasis debía estar puesto en los servicios digitales. Acotó que un ejemplo de estos operadores es lo que ocurre en el sector eléctrico, pues explicó que en la matriz eléctrica la generación, transporte y distribución están a cargo de grandes operadores, como son las hidroeléctricas. Con todo, señaló que también se encuentran los pequeños operadores, como podría ser una central solar o una central eólica.

Dicho lo anterior, informó que la ley establece criterios específicos para determinar cuáles de estos operadores deben ser considerados un servicio esencial que, por cierto, lo será el sector eléctrico, no obstante, expresó que será necesario distinguir, dentro de ese servicio esencial, cuáles de sus operadores son clave para que el país no deje de funcionar.

Resaltó que la gracia de este modelo, en contraposición al de infraestructura crítica que se consideró en su oportunidad, es que es dinámico, ya que pueden ir cambiando las condiciones y dar el espacio para detectar que un nuevo operador de importancia vital entró a funcionar.

Manifestó que esta lógica también aplica para el sector público. Al respecto explicó, siguiendo con el ejemplo del sector

eléctrico, que al determinarse aquel como servicio esencial y establecidas como operadoras de importancia vital las generadoras, transmisoras y distribuidoras de energía, las autoridades sectoriales vinculadas a esos servicios también serán consideradas operadoras de importancia vital.

En respuesta a la consulta de cuáles son los deberes específicos de los operadores de importancia vital y las medidas que deben adoptar, señaló que el artículo 6 del proyecto de ley se hace cargo de esta materia, mencionando, entre otras medidas, las de planificar su capacidad de ciberseguridad y que cuenten con un modelo de gestión de riesgos. Asimismo, agregó que deben mantener un registro de las acciones que hacen en materia de ciberseguridad, elaborar e implementar planes de continuidad operacional y ciberseguridad, entre otras.

Finalizó su intervención señalando que los estándares establecidos son los mismos que ya se fijaron en la regulación europea.

El **Honorable Senador señor Pugh** resaltó el trabajo realizado por las comisiones de Defensa Nacional y de Seguridad Pública, unidas, para incorporar la última normativa de la Directiva NIS2 y considerar la regulación belga sobre la materia. Puso de relieve que Chile, con el presente proyecto de ley, se sitúa en la vanguardia en temas de ciberseguridad y valoró que, tratándose de una política de Estado que trasciende a los gobiernos de turno, como país se avanza en acuerdos para contar con una institucionalidad con un nuevo ecosistema.

Manifestó su interés por la posibilidad de trasladar la institucionalidad tecnológica y de conocimiento fuera de Santiago hacia las regiones y, específicamente, a Valparaíso, pues refirió que es esencial no solo desarrollar conocimiento, sino que también descentralizarlo. Cito el caso de Rumania dentro de la Unión Europea y su posicionamiento en materia de ciberseguridad.

El **Honorable Senador señor Insulza** destacó la importancia y urgencia del proyecto de ley. Apuntó que lo normal es que un país cree la institucionalidad respectiva y luego suscriba los convenios internacionales y dicte leyes de delitos cibernéticos, pero advirtió que en el caso chileno se procedió a la inversa, en el entendido de que primero suscribieron el convenio de Budapest sobre Ciberdelincuencia, en un momento posterior se aprobó la ley de delitos cibernéticos y en esta instancia se está creando la Agencia Nacional de Ciberseguridad. Con todo, pidió agilizar la tramitación del proyecto de ley.

Recogiendo las inquietudes del Senador Edwards por los créditos del BID, sostuvo que los socios más cumplidores piden préstamos al BID para mejorar su ranking internacional. Agregó que es normal que se ocupen estos créditos, tal como se ha realizado en gobiernos anteriores.

Recordó que son pocos los países que pueden pedir créditos en materia de seguridad, lo que demuestra la confianza que el BID tiene respecto de Chile.

- - -

Como se señaló con anterioridad, de conformidad con su competencia, la Comisión de Hacienda se pronunció respecto de las siguientes disposiciones del proyecto de ley: artículo 6, inciso primero, en sus letras a), b) c), d), g) y h), artículo 8, inciso primero, artículo 9, letras f) e i), artículo 10, artículo 11, letra e), artículo 12, artículo 14, incisos quinto, sexto, séptimo, octavo noveno y final, artículo 19, inciso primero, artículo 21, inciso cuarto, artículo 25, artículo 32, artículo 33, incisos primero y quinto, artículo 36, incisos tercero y cuarto, y artículo 42, inciso segundo, permanentes; y artículos primero, segundo, tercero y séptimo transitorios.

A continuación, se da cuenta de las disposiciones del proyecto de ley, así como de los acuerdos adoptados por la Comisión.

Artículo 6

En su inciso primero, refiere que todos los organismos del Estado con competencias específicas sobre servicios esenciales y las instituciones privadas calificadas como operadores de importancia vital, tendrán los deberes que ahí se indican.

Letra a)

Dispone el deber de implementar un sistema de gestión de seguridad de la información continuo con el fin de determinar aquellos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y cuáles afectarían la continuidad operacional del servicio. Agrega que dicho sistema debe contar con la capacidad de estimar tanto la probabilidad como el impacto de las consecuencias de un incidente de ciberseguridad.

Letra b)

Establece el deber de mantener un registro de las acciones ejecutadas que compongan el sistema de seguridad de la información, 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.

Letra c)

Fija el deber de elaborar e implementar planes de continuidad operacional y ciberseguridad, certificados por un centro de certificación acreditado o por la Agencia, según sea el caso. Dichos planes deberán ser actualizados y certificados periódicamente.

Letra d)

Preceptúa el deber de realizar continuamente operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos 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.

Letra g)

Refiere al deber de informar a la comunidad sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente sus redes y sistemas informáticos, en los siguientes casos: cuando se vean expuestos datos personales y no exista otra ley que obligue su notificación; o cuando generar conciencia pública sea necesario para evitar un incidente o para gestionar uno que ya hubiera ocurrido. Todo lo anterior, conforme a las instrucciones generales y particulares que al efecto dicte la Agencia.

Letra h)

Establece el deber de contar con programas de capacitación, formación y educación continua de sus trabajadores y colaboradores, que incluyan campañas de ciberhigiene.

--En votación el artículo 6, inciso primero, en sus letras a), b), c), d), g) y h), fueron aprobadas por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Edwards, Insulza, Lagos, Núñez y Pugh.

Artículo 8

En su inciso primero, crea 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, velar por la protección, promoción y respeto del derecho a la seguridad informática, coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad.

--En votación el artículo 8, inciso primero, fue aprobado por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Edwards, Insulza, Lagos, Núñez y Pugh.

Artículo 9

Señala las atribuciones de la Agencia Nacional de Ciberseguridad para dar cumplimiento a su objetivo.

En su letra f) contempla la atribución de crear y administrar un Registro Nacional de Incidentes de Ciberseguridad.

En su letra i) considera la atribución de diseñar e implementar, en coordinación con el Ministerio de Educación, cuando corresponda, planes y acciones de educación, formación ciudadana, investigación, innovación, entrenamiento, fomento y difusión, destinados a promover el desarrollo nacional de una cultura de ciberseguridad.

--En votación el artículo 9 en sus letras f) e i), fueron aprobadas por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Edwards, Insulza, Lagos, Núñez y Pugh.

Artículo 10

Establece que la dirección y administración superior de la Agencia estará a cargo de un Director o Directora 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.

--En votación el artículo 10, fue aprobado por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Edwards, Insulza, Lagos, Núñez y Pugh.

Artículo 11

Fija las atribuciones del Director o Directora Nacional de la Agencia.

En su letra e) dispone la atribución de ejecutar los actos y celebrar los convenios necesarios para el cumplimiento de los fines de la Agencia. Añade que, en el ejercicio de esta facultad, podrá libremente administrar, adquirir y enajenar bienes de cualquier naturaleza

--En votación el artículo 11, letra e), fue aprobada por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Edwards, Insulza, Lagos, Núñez y Pugh.

Artículo 12

Prescribe, textualmente, lo siguiente:

“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.”.

--En votación el artículo 12, fue aprobado por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Edwards, Insulza, Lagos, Núñez y Pugh.

Artículo 14

Referente al personal de la Agencia.

En su inciso quinto establece que en el caso de cese de funciones de los trabajadores que hubieren ingresado a la Agencia en virtud de las disposiciones del título VI de la ley N° 19.882, sólo tendrán derecho a la indemnización contemplada en el artículo quincuagésimo octavo de dicha ley. Dichos trabajadores no tendrán derecho a las indemnizaciones establecidas en el Código del Trabajo.

En su inciso sexto prescribe que el Director o Directora de la Agencia, sin perjuicio de lo que establezca el contrato, tendrá la facultad para aplicar las normas relativas a las destinaciones, comisiones de servicio y cometidos funcionarios de los artículos 73 a 78 del decreto con fuerza de ley N° 29, promulgado en 2004 y publicado en 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo. Agrega que, para estos efectos, los viáticos se pagarán conforme al decreto con fuerza de ley N° 262, de 1977, del Ministerio de Hacienda, y al decreto supremo N° 1, de 1991, del Ministerio de Hacienda, o el texto que lo reemplace.

En su inciso séptimo dispone que la Agencia no podrá celebrar contratos de trabajo estableciendo el pago de indemnizaciones por causas distintas a las indicadas en los artículos 161, 162 y 163 del Código del Trabajo, y en caso alguno se podrá alterar el monto que entregue la base de cálculo dispuesta en dichas normas. Añade que, para el caso de evaluación deficiente de su desempeño, se podrá aplicar la causal del artículo 160 N° 7 del mismo cuerpo legal.

En su inciso octavo señala que una resolución dictada por el Director o la Directora de la Agencia, visada por la Dirección de Presupuestos, establecerá en forma anual la estructura de la dotación de trabajadores de la Agencia, indicando el número máximo de trabajadores que podrá ocupar según el régimen de remuneraciones.

En su inciso noveno refiere que un reglamento expedido por el ministerio encargado de la 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, promulgado en 2000 y publicado en 2001, del Ministerio Secretaría General de la Presidencia, con sujeción a la planta y dotación máxima del personal.

En su inciso final establece que la Agencia deberá cumplir con las normas establecidas en el decreto ley N° 1.263, de 1975, de administración financiera del Estado.

--En votación el artículo 14, incisos quinto, sexto, séptimo, octavo, noveno y final, fueron aprobados por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Edwards, Insulza, Lagos, Núñez y Pugh.

Artículo 19

En su inciso primero crea la Red de Conectividad Segura del Estado, que proveerá servicios de interconexión y conectividad a Internet a los organismos de la Administración del Estado señalados en el artículo 1 de la ley.

--En votación el artículo 19 inciso primero, fue aprobado por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Edwards, Insulza, Lagos, Núñez y Pugh.

Artículo 21

En su inciso cuarto preceptúa que el incumplimiento de las instrucciones que imparta la Agencia para la respuesta coordinada de incidentes acarreará responsabilidad funcionaria de la autoridad o jefatura del Equipo de Respuesta a Incidentes de Seguridad Informática Sectorial respectivo, la que podrá ser sancionada conforme lo dispuesto en los artículos 33 y 34.

--En votación el artículo 21 inciso cuarto, fue aprobado por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Edwards, Insulza, Lagos, Núñez y Pugh.

Artículo 25

Es del siguiente tenor:

“Artículo 25. Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional. Créase el Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional, en

adelante CSIRT de la Defensa Nacional, dependiente del Ministerio de Defensa Nacional, como el organismo responsable de la coordinación, protección y seguridad de las redes y sistemas del mencionado Ministerio y de los servicios esenciales y operadores vitales para la defensa nacional, además de cumplir aquellas tareas que le sean encomendadas, con el propósito de resguardar la defensa y la seguridad nacional.

El CSIRT de la Defensa Nacional dependerá del Estado Mayor Conjunto, del Ministerio de Defensa Nacional.

Para los efectos presupuestarios, el CSIRT a que se refiere este artículo dependerá del Ministerio de Defensa Nacional; se regirá por el reglamento que este Ministerio dicte al efecto y, en lo que le sea aplicable, por la presente ley.”.

--En votación el artículo 25, fue aprobado por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Edwards, Insulza, Lagos, Núñez y Pugh.

Artículo 32

Señala que la infracción a las obligaciones dispuestas en el Título VI de la ley, 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.

--En votación el artículo 32, fue aprobado por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Edwards, Insulza, Lagos, Núñez y Pugh.

Artículo 33

En su inciso primero se refiere a las sanciones a las infracciones cometidas por instituciones privadas.

En su letra a) dispone que las infracciones leves serán sancionadas con amonestación escrita o multa de 1 a 1.000 unidades tributarias mensuales. Añade que, en caso de que el infractor sea un operador de importancia vital, la multa podrá ser de hasta 5.000 unidades tributarias mensuales.

En su letra b) establece que las infracciones graves serán sancionadas con multa de 1.001 a 5.000 unidades tributarias mensuales. Agrega que, en caso de que el infractor sea un

operador de importancia vital, la multa podrá ser de hasta 10.000 unidades tributarias mensuales.

En su letra c) señala que las infracciones gravísimas serán sancionadas con multa de 10.001 a 20.000 unidades tributarias mensuales.

En su inciso quinto prescribe que 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 contados desde el momento en que se produjo el incidente y la capacidad económica del infractor.

El **Honorable Senador señor Edwards** consultó si el tipo de multa depende del tamaño de la institución privada que cometa la infracción.

El **señor Álvarez** aclaró que hay reglas que establecen un tratamiento diferenciador al momento de la fijación de la multa, como es el de atender a si se trata de pequeñas y medianas empresas.

--En votación el artículo 33, incisos primero y quinto, fueron aprobados por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Edwards, Insulza, Lagos, Núñez y Pugh.

Artículo 36

En su inciso tercero señala que las infracciones a los principios y obligaciones contenidos en los artículos 21 y 29 serán sancionadas con multa de veinte por ciento a cincuenta por ciento de la remuneración mensual del jefe superior del organismo público infractor. Añade que la cuantía de la multa se determinará considerando la gravedad de la infracción, la naturaleza del incidente y el número de personas afectadas, si las hubiere. Refiere que en la determinación de la sanción se deberán considerar también las circunstancias que atenúan la responsabilidad del infractor.

En su inciso cuarto dispone que, si el organismo público persiste en la infracción, se le aplicará al jefe superior del organismo público el duplo de la sanción originalmente impuesta y la suspensión en el cargo por un lapso de cinco días hábiles.

--En votación el artículo 36, incisos tercero y cuarto, fueron aprobados por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Edwards, Insulza, Lagos, Núñez y Pugh.

Artículo 42

En su inciso segundo preceptúa que la revelación de la información reservada será sancionada de conformidad al delito de violación de secretos contemplado en los artículos 246, 247 y 247 bis del Código Penal.

--En votación el artículo 42 inciso segundo, fue aprobado por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Edwards, Insulza, Lagos, Núñez y Pugh.

Disposiciones transitorias

Artículo primero

Dispone, textualmente, lo siguiente:

"Artículo primero. Entrada en vigencia y personal. 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 a través 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. Determinar la fecha para la iniciación de actividades de la Agencia, la cual podrá contemplar un período para su implementación y uno a contar del cual entrará en operaciones.

2. Fijar el sistema de remuneraciones del personal de la Agencia y las normas necesarias para la fijación de las remuneraciones variables, en su aplicación transitoria.

3. Fijar la planta de personal de Directivos de la Agencia, pudiendo al efecto fijar el número de cargos, los requisitos para el desempeño de los mismos, sus denominaciones y los cargos que se encuentren afectos al Título VI de la ley N° 19.882. Además, determinará la fecha de entrada en vigencia de dicha planta.

4. El personal que a la fecha de inicio de

actividades de la Agencia se encuentre prestando servicios a honorarios en la Subsecretaría del Interior y cuyo traspaso se determine de conformidad a los incisos tercero y cuarto de este numeral, podrá optar por modificar su estatuto laboral al Código del Trabajo, siempre que cumpla con los requisitos respectivos y otorgue previamente su consentimiento.

En la medida que el personal señalado en el inciso anterior cumpla con los requisitos respectivos y dé su consentimiento, las modificaciones de estatuto laboral señaladas en el inciso precedente deberán incluirse en la dotación máxima de personal del primer presupuesto que se fije para la Agencia.

En el respectivo decreto con fuerza de ley, se determinará la forma y el número de personas a honorarios a traspasar sin solución de continuidad, desde la Subsecretaría del Interior a la Agencia, además, el plazo en que se llevará a cabo este proceso. Conjuntamente con el traspaso del personal, se traspasarán los recursos presupuestarios que se liberen por este hecho y, a su vez, un número equivalente al de los honorarios traspasados deberá ser reducido del número máximo de personas a ser contratadas a honorarios fijado en las glosas presupuestarias correspondientes de la Subsecretaría del Interior.

La individualización del personal traspasado conforme al inciso anterior, 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.

El personal a honorarios que pase a ser Código del Trabajo de acuerdo a lo señalado en este artículo, mantendrá una remuneración líquida mensualizada que le permita mantener su honorario líquido mensual.

5. Determinar la dotación máxima de personal de la Agencia.

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

--En votación el artículo primero transitorio, fue aprobado por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Edwards, Insulza, Lagos, Núñez y Pugh.

Artículo segundo

Su contenido es el que a continuación se transcribe:

“Artículo segundo. 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 o Directora de la Agencia Nacional de Ciberseguridad, quien asumirá de inmediato, por el plazo máximo de un año y en tanto se efectúa el proceso de selección pertinente que establece la señalada ley para los cargos del Sistema de Alta Dirección Pública. 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 o Directora, siempre que no se encuentre vigente la respectiva planta de personal. La remuneración del primer Director o Directora 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.”.

--En votación el artículo segundo transitorio, fue aprobado por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Edwards, Insulza, Lagos, Núñez y Pugh.

Artículo tercero

Señala que 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.

--En votación el artículo tercero transitorio, fue aprobado por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Edwards, Insulza, Lagos, Núñez y Pugh.

Artículo séptimo

Refiere que 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.

--En votación el artículo séptimo transitorio, fue aprobado por la unanimidad de los miembros de la Comisión, Honorables Senadores señores Edwards, Insulza, Lagos, Núñez y Pugh.

- - -

FINANCIAMIENTO

- El informe financiero **N° 43** elaborado por la Dirección de Presupuestos del Ministerio de Hacienda, de 10 de marzo de 2022, señala lo siguiente:

"**I. Antecedentes**

El presente proyecto de ley tiene por objeto establecer la institucionalidad, principios y el marco general que estructure, regule y coordine la ciberseguridad en Chile; regular la responsabilidad y deberes de los órganos de la Administración del Estado y de las instituciones privadas que posean infraestructura crítica de la información; disponer de los mecanismos de control y supervisión a los que se verán sometidos; y, establecer los requisitos mínimos para prevención y resolución de incidentes de ciberseguridad.

En particular, las principales materias abordadas por el proyecto de ley son:

a. Definiciones técnicas y específicas de ciberseguridad.

b. Principios rectores para la aplicación e interpretación de la ley.

c. La creación de la Agencia Nacional de Ciberseguridad, como un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propio, de carácter técnico y especializado, cuyas principales funciones serán:

- Asesorar al Presidente de la República, en el análisis y definiciones de la política nacional de ciberseguridad, que contiene las medidas, planes y programas de acción específicos que se aplican para

su ejecución y cumplimiento, así como en temas relativos a estrategias de avance en su implementación.

- Dictar normas técnicas de carácter general y los estándares mínimos de ciberseguridad e impartir instrucciones particulares para los organismos 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.

- Coordinar a los Equipos de Respuesta a Incidentes Informáticos (CSIRT por sus siglas en inglés) Sectoriales y a aquellos que pertenezcan a organismos públicos o privados y al CSIRT Nacional, en lo relativo a los estándares y tiempos de comunicación de incidentes de ciberseguridad o vulnerabilidades informáticas.

- Administrar el Registro Nacional de Incidentes de Ciberseguridad.

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

- 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.

- 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.

- Suscribir convenios con organismos públicos y privados destinados a facilitar la colaboración y la transferencia de información que permita el cumplimiento de los fines de la Agencia.

- Cooperar con organismos nacionales e internacionales, en materias propias de su competencia, en coordinación con el Ministerio de Relaciones Exteriores, cuando corresponda.

- Prestar asesoría técnica a organismos públicos y privados cuya infraestructura de la información haya sido calificada como crítica, que estén o se hayan visto afectadas por un incidente de seguridad informática 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 19.628.

- 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.

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

- Diseñar planes y acciones que fomenten la investigación, innovación y desarrollo de la industria de ciberseguridad local en conjunto con el Ministerio de Ciencias, Tecnología, Conocimiento e Innovación.

d. Se crea el Registro Nacional de Incidentes de Ciberseguridad. En este registro se ingresarán los datos técnicos y antecedentes necesarios para describir la ocurrencia de incidentes de ciberseguridad, con su análisis y estudio, así como para realizar las respetivas investigaciones y comunicar las alertas respectivas a CSIRT Sectoriales y a los organismos que posean infraestructura crítica de la información que corresponda al caso.

e. Se crea el Comité Interministerial de Ciberseguridad, cuya función será asesorar al Ministro del Interior y Seguridad Pública en materias de ciberseguridad relevantes para el funcionamiento de la Administración Pública y de servicios esenciales.

f. Se crea el Consejo Técnico de la Agencia Nacional de Ciberseguridad, que tendrá por 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 hacerles frente.

g. Se crea el Equipo Nacional de Respuesta a Incidentes Informáticos (CSIRT Nacional), el CSIRT Sectorial de Gobierno y el CSIRT Sectorial de Defensa.

h. Establece determinadas multas a los organismos que no entreguen información requerida por la autoridad, no la entreguen en los plazos requeridos u otras infracciones determinadas por la ley.

II. Efecto del proyecto de ley sobre el Presupuesto Fiscal

Los efectos del Proyecto de Ley sobre el Presupuesto Fiscal se originan de la creación de la Agencia Nacional de Ciberseguridad, que estará conformada por el Consejo Técnico de la Agencia Nacional de Ciberseguridad, el Equipo Nacional de Respuesta a Incidentes Informáticos y el Equipo de Respuesta a Incidentes Informáticos

Sectorial de Gobierno.

Se contempla un traspaso de recursos desde la División de Redes y Seguridad informática de la Subsecretaría del Interior, hacia nueva la Agencia Nacional de Ciberseguridad. Se traspasa el 50% del presupuesto 2022 aprobado para esta división en Bienes y Servicios de consumo. A su vez, se considera el traspaso del 100% del presupuesto 2022 aprobado para esta división correspondiente a Adquisición de Activos no Financieros ya que se requiere adquirir el equipamiento necesario para la puesta en marcha de la Agencia y seguir cumpliendo con las renovaciones de software que son ocupados actualmente. En términos de traspaso de personal, se contempla el traspaso de 41 personas desde la División de Redes y Seguridad Informática y de la Unidad de Coordinación de Ciberseguridad de la Subsecretaría de Interior.

El mayor gasto fiscal que irrogará la aplicación del presente proyecto de ley se desprende de la contratación de 19 personas para integrar las nuevas divisiones de la Agencia, División Jurídica, División de Administración y Finanzas y División de Concientización y Normalización. Para lo anterior se estima un gasto de $ 578.784 miles de pesos anuales. También se contempla un gasto atribuible a Arriendos y Servicios Básicos con un costo anual de $ 200.000 miles de pesos.

Tabla 1: Mayor gasto fiscal por la aplicación del proyecto de ley (miles de pesos de 2022)

Concepto	Personal	Año 1	Año 2	Año 3 (Régimen)
Gasto en Personal	19	578.784	578.784	578.784
Bienes y Servicios de Consumo		200.000	200.000	200.000
Total		**778.784**	**778.784**	**778.784**

De esta manera, el mayor gasto fiscal que implicará la aplicación del presente proyecto de ley es de $778.784 miles en régimen, de acuerdo al detalle presentado en la tabla 1.

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 del Ministerio del Interior y Seguridad Pública. No obstante, el Ministerio de Hacienda con cargo a la partida presupuestaria del 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 que determinen las respectivas leyes de Presupuestos del Sector Público para cada año.

Los restantes Equipos de respuesta Sectoriales, deberán ser cubiertos (en forma y plazo) por financiamiento propio de cada

entidad reguladora o fiscalizadora, según corresponda.

III. Fuentes de Información.

- Mensaje de S.E. el Presidente de la República, con el que inicia Proyecto de Ley Marco sobre Ciberseguridad y de Infraestructura Crítica de la Información.

- Antecedentes financieros Proyecto de Ley Marco de Ciberseguridad y de Infraestructura Crítica de la Información - División de Redes y Seguridad Informática.

- Ley de Presupuestos del Sector Público, año 2022.”.

- Luego, se acompañó el informe financiero complementario **N° 204,** elaborado por la Dirección de Presupuestos del Ministerio de Hacienda, de 11 de noviembre de 2022, que señala lo siguiente:

“**I. Antecedentes**

Las presentes indicaciones (N° 183-370) incorporan nuevos conceptos, principios, y obligaciones; además de realizar cambios al funcionamiento de la Agencia Nacional de Ciberseguridad (ANC) y otros ajustes que apuntan a una mejor coordinación institucional. En concreto, las principales modificaciones corresponden a:

- Se incorpora el término "operadores de importancia vital" para aquellos servicios cuya afectación o interrupción podría tener efectos en la defensa nacional o en el mantenimiento de actividades sociales y económicas fundamentales.

- Se incorporan dos nuevos principios rectores: el de respuesta responsable, y el de igualdad y no discriminación.

- Se delimitan los organismos que quedarán sometidos al cumplimiento de las obligaciones de ciberseguridad más estrictas.

- Se establece que las facultades regulatorias, fiscalizadoras y sancionatorias de la Agencia sean de alcance general, en lugar de limitar su aplicación a los sectores regulados como lo hacía el proyecto original.

- Se simplifican las funciones del CSIRT Nacional, concentrándose en éste las funciones que se entregaban a los CSIRT Sectoriales. Además, se elimina el CSIRT de Gobierno. Por otra parte, se

establece que el CSIRT de Defensa será responsable de la coordinación, protección y seguridad de las redes y sistemas del Ministerio de Defensa Nacional y de los servicios esenciales y operadores vitales para la defensa nacional, además de cumplir aquellas tareas que le sean encomendadas, con el propósito de resguardar la Defensa y Seguridad Nacional.

- Se reemplaza el Consejo Técnico de la Agencia por un Consejo Multisectorial sobre Ciberseguridad, ad honorem y paritario.

- Se realizan ajustes a las infracciones, de forma de facilitar su aplicación.

- Se establece la existencia legal de la Red de Conectividad Segura del Estado (antes, Red de Conectividad del Estado), que provee de servicios de internet a organismos públicos y se entrega ia administración de dicha red a la ANC.

II. Efecto de las Indicaciones sobre el Presupuesto Fiscal

Considerando los cambios introducidos y particularmente el traspaso de la administración de la Red de Conectividad Segura del Estado a la ANC, se plantea una distribución del presupuesto de dicho programa presupuestario que contempla la transferencia del 50% del presupuesto de Bienes y Servicios de Consumo y un 32% de Activos No Financieros, levemente distinto al I.F. N° 43 de 2022[1]. También se considera el traspaso a la ANC de los recursos de la Unidad de Coordinación de Ciberseguridad de la Subsecretaría del Interior. En tanto, no se observan diferencias en el traspaso de personal respecto de lo indicado en dicho Informe Financiero. Por otra parte, las nuevas funciones del CSIRT de Defensa serán cubiertas con el presupuesto y dotación vigentes del respectivo Ministerio.

De acuerdo a lo señalado anteriormente, **las presentes indicaciones no irrogarán un mayor gasto fiscal** respecto del Informe Financiero antecedente.

III. Fuentes de información

- Mensaje de S.E. el Presidente de la República, mediante el cual realiza indicaciones al Proyecto de Ley que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.

- Ley de Presupuestos del Sector Público, 2022.

---

[1] En el Informe Financiero N° 43 de 2022, se habla de un traspaso de recursos de la División de Redes y Seguridad Informática de la Subsecretaría del Interior, que en la práctica corresponden al Programa Presupuestario de la Red de Conectividad del Estado.

En el Informe Financiero N° 43 de 2022, se habla de un traspaso de recursos de la División de Redes y Seguridad Informática de la Subsecretaría del Interior, que en la práctica corresponden al Programa Presupuestario de la Red de Conectividad del Estado.”.

- Posteriormente, se acompañó el informe financiero sustitutivo **N° 211,** elaborado por la Dirección de Presupuestos del Ministerio de Hacienda, de 21 de noviembre de 2022, que señala lo siguiente:

“**I. Antecedentes**

El presente Informe Financiero sustituye a los anteriores e incorpora el efecto de las indicaciones 207-370. Este proyecto de ley establece un marco sobre la ciberseguridad, definiendo los principios rectores y los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad. Así también, se definen obligaciones y atribuciones para los operadores de importancia vital, referidos a aquellos en que un incidente de seguridad informática pueda tener una repercusión importante en la seguridad nacional, en la provisión de servicios esenciales o en el efectivo cumplimiento de las funciones del Estado.

El proyecto también crea una nueva institucionalidad pública a cargo de la ciberseguridad, la Agencia Nacional de Ciberseguridad (ANC), 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, velar por la protección, promoción y respeto del derecho a la seguridad informática, regular y fiscalizar las acciones de los órganos de la Administración del Estado y de las instituciones privadas y particulares.

El personal de la ANC se regirá por el código del trabajo y estará afecto al Sistema de Alta Dirección Pública hasta el segundo nivel jerárquico.

Dentro de la ANC se crea el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática, CSIRT Nacional encargado de responder a incidentes de seguridad informática cuando sean de impacto significativo. También se establece el CSIRT Defensa, responsable de la coordinación, protección y seguridad de las redes y sistemas del Ministerio de Defensa Nacional y también se contemplan CSIRT Sectoriales, los que deberán coordinarse con el CSIRT nacional.

Por otra parte, se establece la existencia legal de la Red de Conectividad Segura del Estado (antes, Red de Conectividad del Estado), que provee de servicios de internet a organismos públicos y se

entrega la administración de dicha red a la ANC.

Finalmente, se crea el Consejo Multisectorial de Ciberseguridad, que estará compuesto por el Director de la ANC y seis consejeros de alta experiencia en la materia, ad honorem, de carácter consultivo y que tendrá por función asesorar y formular recomendaciones a la ANC. También se crea el Comité Interministerial sobre Ciberseguridad, que tendrá por objeto asesorar al Presidente de la República en materias de ciberseguridad relevantes para el funcionamiento del país.

II. Efecto del Proyecto de Ley sobre el Presupuesto Fiscal

El principal efecto en el presupuesto fiscal se origina con la creación de la Agencia Nacional de Ciberseguridad. Para la conformación de dicha institución se contempla el traspaso de 41 trabajadores desde el Ministerio del Interior y Seguridad Pública, que actualmente se desempeñan en funciones delegadas a la nueva ANC. También se considera el traspaso del 50% del presupuesto de Bienes y Servicios de Consumo y un 32% de Activos No Financieros desde el Programa Presupuestario Red de Conectividad del Estado y de los recursos de la Unidad de Coordinación de Ciberseguridad de la Subsecretaría del Interior.

El mayor gasto fiscal que irrogará la aplicación de este proyecto de ley corresponde a la contratación de 15 nuevos trabajadores, que se desempeñarán en CSIRT y unidades de Administración y Servicios Generales. Debido a que el personal a traspasar se encuentra contratado en calidad de honorarios, se proyecta además un gasto que permitirá mantener sus remuneraciones liquidas.

Finalmente, también se contemplan mayores gastos en Bienes y Servicios de Consumo y Adquisición de Activos No Financieros, tanto permanentes como transitorios. Respecto de los gastos permanentes considera arriendo de oficinas, adquisición de software y servicios básicos asociado al nuevo personal, en tanto el gasto transitorio contempla principalmente habilitación de oficinas y equipamiento.

El detalle del mayor gasto fiscal que representa el presente proyecto de ley se detalla en el siguiente cuadro.

Cuadro 1
Mayor gasto (Miles de $ de 2022)

Ítem	Gasto Adicional
Gastos de Personal	**642.829**
Nuevas contrataciones	468.328
Traspaso	174.501
Bienes y Servicios de Consumo	**187.086**
Permanente	186.456
Transitorio	630
Adquisición de Activos No Financieros	**102.464**
Permanente	48.000
Transitorio	54.464
Total Gasto Permanente	**877.285**
Total Gasto Transitorio	**55.094**

De acuerdo a lo señalado anteriormente el proyecto de ley **irrogará un mayor gasto fiscal en régimen de M$877.285**.

III. Fuentes de información

• Mensaje de S.E. el Presidente de la República (N° 469-369), con el cual inicia al Proyecto de Ley que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.

• Mensaje de S.E. el Presidente de la República (N° 183-370), mediante el cual realiza indicaciones al Proyecto de Ley que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.

• Mensaje de S.E. el Presidente de la República (N° 207-370), mediante el cual realiza indicaciones al Proyecto de Ley que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.

• Ley de Presupuestos del Sector Público, 2022.

• Minuta Gastos ANC, Ministerio del Interior y Seguridad Pública, Noviembre 2022.”.

- Enseguida, se acompañó el informe financiero complementario **N° 64,** elaborado por la Dirección de Presupuestos del Ministerio de Hacienda, de 11 de abril de 2023, que señala lo siguiente:

“**I. Antecedentes**

Mediante las presentes indicaciones (N° 023-371)

se incorporan nuevos conceptos, principios y obligaciones y regulaciones extras al personal de la Agencia Nacional de Ciberseguridad; se establecen prohibiciones a los órganos de la Administración del Estado e instituciones privadas involucradas en la ley realizar pagos de cualquier tipo por rescate ante ataques de secuestro digital y se generan regímenes de medidas especiales para una serie de instituciones señaladas en la ley. En concreto, las principales modificaciones corresponden a:

- Se incorpora el principio de igualdad y no discriminación dentro de los principios rectores de la institución.

- Se incorpora el principio de actualización de programas computacionales, el cual señala que los organismos públicos e instituciones privadas adoptarán medidas necesarias para la instalación de actualizaciones de seguridad de los sistemas informáticos que usen o administren.

- Se prohíbe a los organismos e instituciones señalados en la ley, realizar pagos por cualquier tipo de rescate ante ataques de secuestro digital.

- Se incluye como atribución para la Agencia el fiscalizar el cumplimiento de las disposiciones de esta ley, sus reglamentos, protocolos, estándares técnicos y las instrucciones generales y particulares que emita la Agencia en ejercicio de las atribuciones conferidas en la ley.

- Se establece que al personal de la Agencia también le serán aplicables normas generales sobre obligaciones y derechos funcionarios, del decreto con fuerza de ley N° 29, del Ministerio de Hacienda, del año 2004.

- Se establece la prohibición al personal de la Agencia, así como también para sus cónyuges y parientes consanguíneos, de prestar por sí o a través de otras personas naturales o jurídicas, servicios personales a personas o a entidades sometidas a la fiscalización de la Agencia.

- Se establecen las funciones de los CSIRT Sectoriales.

- Se establece que las autoridades sectoriales podrán dictar las normas de carácter general y las normas técnicas que consideren necesarias para la ciberseguridad de la institución de su sector. En el ejercicio de estas facultades normativas, las autoridades sectoriales deberán considerar los protocolos y estándares técnicos y las instrucciones generales y particulares dictados por la Agencia.

- Se indica que la Comisión para el Mercado Financiero podrá establecer normas de carácter general y normas técnicas

sobre ciberseguridad aplicables al sector respectivo, sin necesidad de solicitar la aprobación de la Agencia, siempre y cuando tengan un alcance distinto a las normas dictadas por esta última.

- Se realizan modificaciones al régimen especial establecido para: el Congreso Nacional, el Poder Judicial, la Contraloría General de la República, el Ministerio Público, el Tribunal Constitucional, el Banco Central, el Servicio Electoral y la Justicia Electoral y el Consejo Nacional de Televisión. Principalmente, se establece que deberán acordar mecanismos de coordinación, cooperación, reporte de incidentes e intercambio de información sobre ciberseguridad, respecto de la Agencia o demás instancias previstas en la ley y que esta deberá contar con autorización previa para acceder a sus sistemas informáticos, en caso de ser requerido.

III. Efecto del Proyecto de Ley sobre el Presupuesto Fiscal

Estas indicaciones no modifican aspectos esenciales que impliquen un mayor gasto respecto de los informes financieros previos. Respecto de la constitución de los CSIRT Sectoriales y las funciones que desarrollarán, deberán ser cubiertos por financiamiento propio de cada entidad reguladora o fiscalizadora, según corresponda, y en el intertanto, de acuerdo a lo indicado en el artículo quinto transitorio, el CSIRT Nacional tendrá, para todos los efectos legales, la calidad de CSIRT Sectorial correspondiente, con todas sus atribuciones y facultades.

Por lo tanto, estas indicaciones, **no irrogarán mayor gasto fiscal** respecto de lo indicado en los Informes Financieros antecedentes (N°s 43, 204 y 211, de 2022).

III. Fuentes de información

• Mensaje de S.E. el Presidente de la República, mediante el cual realiza indicaciones al Proyecto de Ley que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.”.

Se deja constancia de los precedentes informes financieros en cumplimiento de lo dispuesto en el inciso segundo del artículo 17 de la Ley Orgánica Constitucional del Congreso Nacional.

- - -

TEXTO DEL PROYECTO

En mérito de los acuerdos precedentemente expuestos, vuestra Comisión de Hacienda tiene el honor de proponeros la aprobación del proyecto de ley en informe, en los mismos términos en que

fue despachado por las comisiones de Defensa Nacional y de Seguridad Pública, unidas, cuyo texto 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 permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre estos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones privadas, y los mecanismos de control, supervisión y de responsabilidad ante infracciones.

Para los efectos de esta ley, se entenderá por Administración del Estado a los ministerios, las delegaciones presidenciales regionales y provinciales, los gobiernos regionales, las municipalidades, las Fuerzas Armadas, de Orden y Seguridad Pública, y los órganos y servicios públicos creados para el cumplimiento de la función administrativa. Los órganos autónomos constitucionales se ajustarán a las disposiciones de esta ley que así lo señalen. No se aplicarán las disposiciones de esta ley a las empresas públicas creadas por ley y a las empresas del Estado y sociedades en que este tenga participación accionaria superior al 50% o mayoría en el directorio, salvo que sean calificadas como operadores de importancia vital.

La institucionalidad de la ciberseguridad velará por la protección, promoción y respeto del derecho a la seguridad informática de las personas y sus familias, que comprende la adopción de las medidas necesarias e idóneas para garantizar la integridad, confidencialidad, disponibilidad y resiliencia de la información que contengan sus redes y sistemas informáticos, incluyendo las herramientas de cifrado.

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

1. Activo informático: toda información almacenada en una red y sistema informático que tenga valor para una persona u organización.

2. Agencia: la Agencia Nacional de Ciberseguridad, que se conocerá en forma abreviada como ANCI.

3. Auditorías de seguridad: procesos de control destinados a revisar el cumplimiento de las políticas y procedimientos que se derivan del Sistema de Gestión de la Seguridad de la Información.

4. Autenticación: propiedad de la información que da cuenta de su origen legítimo.

5. Autoridad sectorial: aquellos servicios públicos que cuentan con facultades regulatorias, fiscalizadoras y eventualmente sancionatorias respecto de sus regulados.

6. Ciberataque: un incidente de ciberseguridad en el que una persona o grupo de ellas, conocidas o no, intenta destruir, exponer, alterar, deshabilitar, exfiltrar, hacer uso o acceder de manera no autorizada a un activo de información, y en el que puedan verse afectados también activos físicos de forma eléctrica o mecánica.

7. Ciberespacio: ambiente formado por la interconexión e interrelación compleja entre las redes y sistemas informáticos, los componentes lógicos de la información, los datos almacenados, procesados o transmitidos, y las interacciones sociales que ocurren en aquel.

Los componentes lógicos de la información son los diferentes programas computacionales que permiten el funcionamiento, administración y uso de la red.

8. Ciberhigiene o higiene digital: conjunto de prácticas habituales de las personas para mejorar la gestión segura de datos y proteger redes y sistemas informáticos, que incluyen, entre otros, el cuidado de claves de acceso, la gestión de vulnerabilidades y la actualización de programas y aplicaciones.

9. Ciberseguridad: preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad.

10. Confidencialidad: propiedad que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados.

11. Disponibilidad: propiedad que consiste en que la información está disponible y es utilizable cuando es requerida por un individuo, entidad o proceso autorizado.

12. Equipo de Respuesta a Incidentes de Seguridad Informática o CSIRT: centros multidisciplinarios que tienen por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos.

13. Estándares mínimos de ciberseguridad: corresponde al conjunto de reglas y procedimientos técnicos básicos sobre ciberseguridad, dictados por la Agencia o por la autoridad sectorial competente de conformidad con la presente ley.

14. Gestión de incidentes de ciberseguridad: conjunto ordenado de acciones enfocadas a prevenir la ocurrencia de incidentes de ciberseguridad y, en caso de que ocurran, restaurar los niveles de operación lo antes posible.

15. Incidente de ciberseguridad: todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación o no-repudio de los procesos ejecutados o implementados en las redes y sistemas informáticos.

16. Integridad: propiedad que consiste en que la información no ha sido modificada o destruida sin autorización.

17. Interagencialidad: coordinación que permite que dos o más agencias o instituciones actúen de forma conjunta, sinérgica y coherente para alcanzar objetivos comunes, imposibles de lograr de forma independiente.

18. Interoperabilidad: capacidad de los sistemas informáticos de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos en tiempo real.

19. No repudio: propiedad de la información que permite probar su origen.

20. Operadores de importancia vital: institución pública o privada, identificada como tal por la Agencia de conformidad con esta ley, por prestar algún servicio esencial para el mantenimiento de actividades sociales o económicas cruciales, que depende de las redes y sistemas informáticos, y cuya afectación, interceptación, interrupción o destrucción pueda 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.

21. Red y sistema informático: conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales.

22. Resiliencia: capacidad de las redes y sistemas informáticos para seguir operando luego de un incidente de ciberseguridad, aunque sea en un estado degradado, debilitado o segmentado, y la capacidad de las redes y sistemas informáticos para recuperar sus funciones después de un incidente de ciberseguridad.

23. Riesgo: posibilidad de ocurrencia de un incidente de ciberseguridad; la magnitud de un riesgo es cuantificada en términos de la probabilidad de ocurrencia del incidente y del impacto de las consecuencias del mismo.

24. Sector regulado: aquel sector de la actividad económica que se encuentra sometido a la supervigilancia de un órgano público con facultades suficientes para regular, fiscalizar y eventualmente sancionar.

25. Servicios esenciales: todo servicio cuya afectación o interrupción tendría un impacto perturbador en el normal funcionamiento de la defensa nacional, la sociedad o la economía.

26. Sistema de gestión de seguridad de la información: conjunto de políticas, procedimientos, guías técnicas, y las actividades y recursos asociados, gestionados colectivamente por una organización para proteger sus activos de información.

27. 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 actualización de programas computacionales: los organismos públicos e instituciones privadas adoptarán las medidas necesarias para la instalación de las actualizaciones de seguridad de los sistemas informáticos que usen o administren, dando prioridad a aquellas que solucionen vulnerabilidades graves.

2. Principio de confidencialidad de los sistemas informáticos: la información almacenada o transmitida por redes y sistemas informáticos deberá ser conocida y accedida exclusivamente

por personas o entidades autorizadas a tal efecto, las que se encontrarán sujetas a las responsabilidades y obligaciones que señalen las leyes.

3. Principio de control de daños: frente a un ciberataque o a un incidente de ciberseguridad, todos los organismos del Estado, así como las instituciones privadas, deberán siempre actuar diligentemente, adoptando las medidas necesarias para evitar la escalada del ciberataque o del incidente de ciberseguridad y su posible propagación a otros sistemas informáticos.

4. Principio de cooperación con la autoridad: los organismos 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.

5. Principio de disponibilidad de los sistemas informáticos: la información almacenada o transmitida por redes y sistemas informáticos, y las redes y sistemas informáticos deberán estar accesibles para su uso a demanda.

6. Principio de igualdad y no discriminación: todas las personas tienen derecho a participar de un espacio digital seguro y libre de violencia. El Estado desarrollará acciones de prevención, promoción, reparación y garantía de este derecho, otorgando especial protección a mujeres, niñas, niños, jóvenes, personas de la tercera edad y disidencias sexogenéricas.

7. Principio de integridad de los sistemas informáticos y de la información: la información almacenada o transmitida por redes y sistemas informáticos, incluida la configuración de estos, solo podrá ser modificada por personas autorizadas en el ejercicio de sus funciones o por sistemas que cuenten con la autorización respectiva.

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

9. Principio de responsabilidad: aquel en cuya virtud la seguridad de las redes, sistemas y datos es de responsabilidad de aquel que las provee, ofrece u opera, con independencia de la naturaleza pública o privada del organismo.

10. Principio de respuesta responsable: la aplicación de medidas para responder a incidentes de ciberseguridad o ciberataques en ningún caso podrá significar la realización de, o el apoyo a, operaciones ofensivas.

11. Principio del cifrado: toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere necesarias, incluyendo el cifrado. Ninguna persona ni autoridad podrá afectar, restringir o impedir el ejercicio de este derecho.

TÍTULO II
Obligaciones de ciberseguridad

Párrafo 1°
Servicios esenciales y operadores de importancia vital

Artículo 4. Determinación de los servicios esenciales e identificación de los operadores de importancia vital. En el ejercicio de la facultad establecida en el artículo 9 letra g) de esta ley, la Agencia determinará aquellos servicios que sean considerados esenciales para los efectos de esta ley, y dentro de estos identificará a los operadores de importancia vital, de conformidad con los criterios y el procedimiento dispuesto en el presente artículo.

A fin de determinar qué servicios resultan esenciales, se deberá atender a la entidad del impacto cuya afectación o interrupción podría tener en la defensa nacional o en el mantenimiento de actividades sociales y económicas fundamentales.

Los criterios para la identificación de los operadores de importancia vital serán los siguientes:

a) Se trata de un operador que presta un servicio calificado como esencial de conformidad con esta ley;

b) La prestación de dicho servicio depende de las redes y sistemas informáticos, y

c) Un incidente de ciberseguridad tendría un impacto perturbador en la prestación de dicho servicio.

Para determinar si el impacto de un incidente de ciberseguridad podría ser perturbador, se deberán tener en consideración, al menos, los siguientes factores:

a) La cantidad de usuarios potencialmente afectados;

b) La interdependencia de otros sectores calificados como servicios esenciales;

c) La potencial afectación de la vida, integridad física o salud de las personas;

d) La repercusión que podrían tener los incidentes, en términos de grado y duración, en las actividades económicas y sociales, en la seguridad nacional o en el ejercicio de la soberanía;

e) La extensión geográfica que podría verse afectada por un incidente;

f) La importancia del operador para el mantenimiento de un nivel suficiente del servicio, teniendo en cuenta la disponibilidad de alternativas para la prestación de ese servicio;

g) La afectación relevante del funcionamiento del Estado y sus organismos, y

h) El daño reputacional que pueda ocasionarse.

La Agencia requerirá a la Agencia Nacional de Inteligencia un informe fundado sobre los servicios que deban calificarse como esenciales e identifique, para cada uno de estos, aquellos operadores que resultan de importancia vital para su provisión. De igual manera, la Agencia podrá requerir informes similares a otros organismos públicos o instituciones privadas. El órgano requerido deberá dar respuesta al requerimiento de la Agencia dentro del plazo de sesenta días contados desde su recepción. Se exceptúan de esta obligación los servicios esenciales y operadores vitales exclusivos de la defensa nacional, quienes responderán a los requerimientos del CSIRT de la Defensa Nacional.

Transcurrido este plazo, con los antecedentes que hubiere recibido, la Agencia propondrá una lista actualizada de servicios esenciales y de operadores de importancia vital al Comité Interministerial de Ciberseguridad para que, dentro del plazo de treinta días, se pronuncie fundadamente, pudiendo aprobar o sugerir las enmiendas que considere necesarias para su aprobación, las que serán comunicadas a la Agencia.

Dentro de los treinta días siguientes a la recepción de la decisión del Comité Interministerial de Ciberseguridad, el Ministerio encargado de la seguridad pública, mediante la dictación de un decreto supremo bajo la fórmula "Por orden del Presidente de la República", determinará aquellos servicios que serán considerados esenciales y a los operadores de importancia vital. Este decreto quedará exento del trámite de toma de razón de la Contraloría General de la República.

Párrafo 2°
Obligaciones de ciberseguridad

Artículo 5. Deberes generales. Será obligación de los organismos del Estado y de las instituciones privadas aplicar de manera permanente las medidas necesarias para prevenir, reportar y resolver incidentes de ciberseguridad. Estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso.

Asimismo, estas medidas tendrán por objeto la gestión de riesgos asociados a la ciberseguridad y la contención y mitigación del impacto que los incidentes puedan tener sobre la continuidad operacional, la confidencialidad y la integridad del servicio prestado, de conformidad con lo prescrito en la presente ley.

En el caso de los organismos de la Administración del Estado e instituciones privadas que presten servicios esenciales, el cumplimiento de estas obligaciones exige, al menos, la debida implementación de los protocolos y estándares establecidos por la Agencia, así como de los estándares particulares de ciberseguridad dictados de conformidad a la regulación sectorial respectiva, de ser el caso.

La Agencia deberá establecer protocolos y estándares diferenciados según el tipo de organización de que se trate y su relación con la prestación de servicios calificados como esenciales, teniendo especialmente en consideración las características y necesidades de las pequeñas y medianas empresas, tal como se definen en la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño.

Para efectos de emitir los protocolos y estándares a los que se refiere el inciso anterior, la Agencia deberá solicitar informe previo de la autoridad sectorial competente, el que deberá ser evacuado a más tardar dentro el plazo de treinta días hábiles, sin perjuicio de lo dispuesto en el artículo 22 respecto de las instituciones financieras fiscalizadas por la Comisión para el Mercado Financiero.

Se prohíbe a los organismos e instituciones señalados en el inciso primero, realizar pagos de cualquier tipo por rescate ante ataques de secuestro digital o ransomware, ya sea que dichos ataques causen la inoperatividad de los sistemas o amenacen con exponer la información exfiltrada.

Artículo 6. Deberes específicos de los operadores de importancia vital y para la protección de los servicios esenciales. Todos los organismos del Estado con competencias

específicas sobre servicios esenciales y las instituciones privadas calificadas como operadores de importancia vital, deberán:

a) Implementar un sistema de gestión de seguridad de la información continuo con el fin de determinar aquellos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y cuáles afectarían la continuidad operacional del servicio. Dicho sistema debe contar con la capacidad de estimar tanto la probabilidad como el impacto de las consecuencias de un incidente de ciberseguridad.

b) Mantener un registro de las acciones ejecutadas que compongan el sistema de seguridad de la información, 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, certificados por un centro de certificación acreditado o por la Agencia, según sea el caso. Dichos planes deberán ser actualizados y certificados periódicamente.

d) Realizar continuamente operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos 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 de forma oportuna y expedita 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.

g) Informar a la comunidad sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente sus redes y sistemas informáticos, en los siguientes casos: cuando se vean expuestos datos personales y no exista otra ley que obligue su notificación; o cuando generar conciencia pública sea necesario para evitar un incidente o para gestionar uno que ya hubiera ocurrido. Todo lo anterior, conforme a las instrucciones generales y particulares que al efecto dicte la Agencia.

h) Contar con programas de capacitación, formación y educación continua de sus trabajadores y colaboradores, que incluyan campañas de ciberhigiene.

i) Designar un delegado de ciberseguridad, quien será la contraparte de la Agencia y dependerá directamente de la máxima autoridad de la institución a la que pertenece.

Un reglamento expedido por el Ministerio encargado de la seguridad pública identificará los organismos del Estado con competencias específicas sobre servicios esenciales.

Artículo 7. Deber de reportar. Todas las instituciones, sean públicas o privadas, e independiente de si son o no operadores de servicios esenciales, con la sola excepción de aquellos que la Agencia hubiere eximido expresamente en sus instrucciones generales o particulares, tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos, de conformidad con el artículo 23. Ello, sin perjuicio de las excepciones dispuestas en el Título V de la presente ley.

La obligación de reportar deberá cumplirse en un plazo inferior a tres horas contadas desde que se tuvo conocimiento del evento respectivo. La entidad informante podrá solicitar la prórroga de dicho plazo por una sola vez y mientras se encuentre este vigente, con la sola finalidad de recabar mayores antecedentes.

Adicionalmente, todos los operadores de servicios esenciales, sean de importancia vital o no, deberán informar al CSIRT Nacional su plan de acción tan pronto lo hubieren adoptado. El plazo para la adopción de un plan de acción en ningún caso podrá ser superior a siete días corridos, de ocurrido alguno de los hechos a que refiere el inciso primero.

Para el cumplimiento del deber establecido en este artículo, los jefes de servicio deberán exigir a los proveedores de servicios de tecnologías de la información, que compartan la información sobre vulnerabilidades e incidentes que puedan afectar a las redes y sistemas informáticos de los organismos del Estado. Con el objeto de cumplir con lo anterior, deberán eliminar cualquier restricción, especialmente las contractuales, que pudiera dificultar la comunicación de información sobre amenazas entre el Gobierno y el sector privado.

La Agencia dictará las instrucciones que sean necesarias para la debida realización y recepción de los reportes a que se refiere el presente artículo.

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, velar por la protección, promoción y respeto del derecho a la seguridad informática, coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad.

La Agencia deberá regular, fiscalizar y sancionar las acciones de los organismos de la Administración del Estado y de las instituciones privadas en materia de ciberseguridad, incluida la facultad de impartir instrucciones generales y particulares.

En el ejercicio de sus funciones, la Agencia deberá siempre velar por la coherencia normativa, buscando que sus acciones se inserten de manera armónica en el ordenamiento regulatorio y sancionatorio nacional.

La Agencia se relacionará con el Presidente de la República por intermedio del Ministerio encargado de la seguridad pública.

La Agencia tendrá domicilio en la ciudad de Santiago, sin perjuicio de contar con oficinas en otras macrozonas 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 la elaboración y aprobación de la Política Nacional de Ciberseguridad, y de los planes y programas de acción específicos para su implementación, ejecución y evaluación.

b) Dictar las disposiciones para la aplicación y el cumplimiento de las leyes y reglamentos y, en general, dictar protocolos y estándares técnicos, instrucciones generales y particulares de carácter obligatorias a las instituciones públicas y privadas, con el objeto de

regular los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad.

c) Aplicar e interpretar administrativamente las disposiciones legales y reglamentarias en materia de ciberseguridad; los protocolos y estándares técnicos, y las instrucciones generales y particulares que dicte al efecto.

d) Coordinar y supervisar a los CSIRT Sectoriales existentes; a aquellos que pertenezcan a organismos de la Administración del Estado; a instituciones privadas y al CSIRT Nacional, en la forma que establece esta ley.

e) Establecer una coordinación con el CSIRT de la Defensa Nacional, en lo relativo a los estándares y tiempos de comunicación de incidentes de ciberseguridad o vulnerabilidades, así como respecto a las materias que serán objeto de intercambio de información.

f) Crear y administrar un Registro Nacional de Incidentes de Ciberseguridad.

g) Elaborar y actualizar la lista de servicios esenciales y operadores de importancia vital, en la forma prevista en el artículo 4 de la presente ley.

h) Requerir de los CSIRT Sectoriales la información que sea necesaria para el cumplimiento de sus fines y que se encuentre en posesión de estas instituciones.

i) Diseñar e implementar, en coordinación con el Ministerio de Educación, cuando corresponda, planes y acciones de educación, formación ciudadana, investigación, innovación, entrenamiento, fomento y difusión, destinados a promover el desarrollo nacional de una cultura de ciberseguridad.

j) Requerir a los organismos del Estado y a las instituciones privadas cualquier documento, antecedente o información que sea necesario para el cumplimiento de sus fines, incluyendo el acceso a redes y sistemas informáticos, observando de manera estricta el deber de reserva que esta ley impone, así como los consagrados por la ley N° 19.628.

k) Cooperar con organismos públicos, instituciones privadas y organismos internacionales, en materias propias de su competencia, sin perjuicio de las atribuciones de otros organismos del Estado. La Agencia servirá de punto de contacto con las Agencias Nacionales de Ciberseguridad extranjeras o sus equivalentes y con los

organismos internacionales con competencia en materia de ciberseguridad.

l) Prestar asesoría técnica a los organismos del Estado e instituciones privadas afectados por un incidente de ciberseguridad que haya comprometido sus activos informáticos críticos o afectado el funcionamiento de su operación, cautelando siempre los deberes de reserva de información que esta ley le impone, así como los consagrados por la ley N° 19.628.

m) Coordinar y colaborar interagencialmente con los organismos integrantes del Sistema de Inteligencia del Estado en la identificación de amenazas y la gestión de incidentes o ciberataques que puedan representar un riesgo para la seguridad nacional.

n) Fiscalizar el cumplimiento de las disposiciones de esta ley, sus reglamentos, protocolos, estándares técnicos y las instrucciones generales y particulares que emita la Agencia en ejercicio de las atribuciones conferidas en la ley.

La Agencia contará con todas las facultades que fueren necesarias para el cumplimiento de su función fiscalizadora; entre otras, las de realizar inspecciones, auditorías, análisis de seguridad o evaluar un sistema de gestión de seguridad de la información; requerir el acceso a sistemas informáticos, datos, documentos e información para el desempeño de sus funciones de supervisión, y citar a declarar a los socios, directores, administradores, representantes, empleados y personas que, a cualquier título, presten o hayan prestado servicios para las personas o entidades fiscalizadas y a toda otra persona que hubiere ejecutado y celebrado con ellas actos y convenciones de cualquier naturaleza, respecto de algún hecho cuyo conocimiento estime necesario para el cumplimiento de sus funciones.

ñ) Ordenar la realización de procedimientos sancionatorios a las entidades fiscalizadas, procediendo a sancionar las infracciones e incumplimientos en que incurran las instituciones públicas y privadas respecto de las disposiciones de esta ley, reglamentos, obligaciones e instrucciones generales y particulares que emita la Agencia. Para tales efectos, y de manera fundada, podrá citar a declarar, entre otros, a los representantes legales, administradores, asesores y dependientes de la institución de que se trate, así como a toda persona que haya tenido participación o conocimiento respecto de algún hecho que sea relevante para resolver el procedimiento sancionatorio. Asimismo, podrá tomar las declaraciones por otros medios que aseguren su integridad y fidelidad.

o) Fomentar la investigación, innovación, capacitación y entrenamiento frente a amenazas, vulnerabilidades e incidentes de ciberseguridad y, en conjunto con los ministerios de

Economía, Fomento y Turismo, y de Ciencia, Tecnología, Conocimiento e Innovación, diseñar planes y acciones que fomenten el desarrollo o fortalecimiento de la industria de ciberseguridad local.

p) Realizar el seguimiento y evaluación de las medidas, planes y acciones elaborados en el ejercicio de sus funciones.

q) Informar al CSIRT de la Defensa Nacional y a los CSIRT Sectoriales los reportes o alarmas de incidentes de ciberseguridad y de vulnerabilidades existentes, conocidas o detectadas en su sector, que considere relevantes, pudiendo sugerir determinados planes de acción.

r) Determinar, conforme al informe técnico que el CSIRT Nacional elabore para estos efectos, las categorías de incidentes o vulnerabilidades de ciberseguridad que estarán eximidas de notificación.

s) Certificar el cumplimiento de los estándares de ciberseguridad correspondientes por parte de los organismos de la Administración del Estado.

t) Otorgar y revocar las acreditaciones correspondientes a los centros de certificación, en los casos y bajo las condiciones que establezca esta ley y el reglamento respectivo.

u) Establecer los estándares que deberán cumplir las instituciones que provean bienes o servicios al Estado, y las normas de seguridad para el desarrollo de los sistemas y programas informáticos que sean utilizados por los organismos del Estado.

v) Regular, en coordinación con el Servicio Nacional del Consumidor, estándares de ciberseguridad y deberes de información al público sobre riesgos de seguridad de dispositivos digitales disponibles a consumidores finales, cubriendo tanto la publicidad del producto como la obligación de incluir etiquetas en estos, pudiendo consistir en fechas de expiración, indicadores de riesgo, u otros indicadores similares.

w) Administrar la Red de Conectividad Segura del Estado (RCSE).

x) Coordinar anualmente durante el mes de octubre, un ejercicio nacional de comprobación de capacidades de ciberseguridad, en cumplimiento de la ley N° 21.113.

y) 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 **o Directora** 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 o Directora Nacional. Corresponderá especialmente al Director o Directora 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 los funcionarios y funcionarias que indique;

g) Instruir la apertura de procedimientos administrativos sancionadores, designar a los funcionarios y funcionarias a cargo y determinar las sanciones e imponerlas, y

h) Ejercer la representación judicial y extrajudicial de la Agencia, sin perjuicio de las atribuciones que pudieran corresponder al Consejo de Defensa del Estado.

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, hasta el segundo nivel jerárquico.

Artículo 14. Del personal de la Agencia. El personal de la Agencia se regirá por las normas del Código del Trabajo.

Con todo, serán aplicables a este personal las normas de probidad contenidas en la ley N° 20.880, sobre Probidad en la Función Pública y Prevención de los Conflictos de Intereses, y las disposiciones del Título III de la ley N° 18.575, orgánica constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto con fuerza de ley Nº 1, promulgado en 2000 y publicado en 2001, del Ministerio Secretaría General de la Presidencia, debiendo dejarse constancia en los contratos respectivos de una cláusula que así lo disponga.

Al personal de la Agencia también le serán aplicables los artículos 61, 62, 63, 64, 90 y 90 A según corresponda, del decreto con fuerza de ley N° 29, promulgado en 2004 y publicado en 2005,

del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo.

Asimismo, el personal estará sujeto a responsabilidad administrativa, sin perjuicio de la responsabilidad civil o penal que pudiere afectarle por los actos realizados en el ejercicio de sus funciones. La responsabilidad disciplinaria del personal de la Agencia por los actos realizados en el ejercicio de sus funciones podrá hacerse efectiva por la autoridad respectiva, de acuerdo al procedimiento establecido en el título V "De la Responsabilidad Administrativa" del decreto con fuerza de ley N° 29, promulgado en 2004 y publicado en 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo.

En el caso de cese de funciones de los trabajadores que hubieren ingresado a la Agencia en virtud de las disposiciones del título VI de la ley N° 19.882, sólo tendrán derecho a la indemnización contemplada en el artículo quincuagésimo octavo de dicha ley. Dichos trabajadores no tendrán derecho a las indemnizaciones establecidas en el Código del Trabajo.

El Director o Directora de la Agencia, sin perjuicio de lo que establezca el contrato, tendrá la facultad para aplicar las normas relativas a las destinaciones, comisiones de servicio y cometidos funcionarios de los artículos 73 a 78 del decreto con fuerza de ley N° 29, promulgado en 2004 y publicado en 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo. Para estos efectos, los viáticos se pagarán conforme al decreto con fuerza de ley N° 262, de 1977, del Ministerio de Hacienda, y al decreto supremo N° 1, de 1991, del Ministerio de Hacienda, o el texto que lo reemplace.

La Agencia no podrá celebrar contratos de trabajo estableciendo el pago de indemnizaciones por causas distintas a las indicadas en los artículos 161, 162 y 163 del Código del Trabajo, y en caso alguno se podrá alterar el monto que entregue la base de cálculo dispuesta en dichas normas. Para el caso de evaluación deficiente de su desempeño, se podrá aplicar la causal del artículo 160 N° 7 del mismo cuerpo legal.

Una resolución dictada por el Director o la Directora de la Agencia, visada por la Dirección de Presupuestos, establecerá en forma anual la estructura de la dotación de trabajadores de la Agencia, indicando el número máximo de trabajadores que podrá ocupar según el régimen de remuneraciones.

Un reglamento expedido por el ministerio encargado de la 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, promulgado en 2000 y publicado en 2001, del Ministerio Secretaría General de la Presidencia, con sujeción a la planta y dotación máxima del personal.

La Agencia deberá cumplir con las normas establecidas en el decreto ley N° 1.263, de 1975, de administración financiera del Estado.

Artículo 15. Prohibiciones e inhabilidades. Prohíbese al personal de la Agencia prestar por sí o a través de otras personas naturales o jurídicas, servicios personales a personas o a entidades sometidas a la fiscalización de la Agencia, o a los directivos, jefes o empleados de ellas, sean estas públicas o privadas.

El personal de la Agencia no podrá intervenir, en razón de sus funciones, en asuntos en que tenga interés él o ella, su cónyuge, su conveniente civil, sus parientes consanguíneos del primero a cuarto grado inclusives, o por afinidad de primero y segundo grado.

Asimismo, les está prohibido actuar por sí o a través de sociedades de que formen parte, como lobbistas o gestores de intereses de terceras personas ante cualquier institución sometida a la fiscalización de la Agencia.

En todo caso, quedarán exceptuados de estas prohibiciones e inhabilidades el ejercicio de derechos que atañan personalmente al funcionario o funcionaria, o que se refieran a la administración de su patrimonio. El desempeño de funciones en la Agencia será de dedicación exclusiva y será incompatible con todo otro empleo o servicio retribuido con fondos fiscales o municipales, y con las funciones, remuneradas o no, de consejero, director o trabajador de instituciones fiscales, semifiscales, organismos autónomos nacionales o extranjeros, empresas del Estado y, en general, de todo servicio público creado por ley. No obstante, será compatible con cargos docentes en instituciones públicas o privadas reconocidas por el Estado hasta un máximo de doce horas semanales, para lo cual deberá prolongar su jornada para compensar las horas durante las cuales no haya podido desempeñar su cargo.

Igualmente, quedará exceptuada la atención no remunerada prestada a sociedades de beneficencia, instituciones de carácter benéfico y, en general, a instituciones sin fines de lucro. Con todo, para que operen estas excepciones, será necesario obtener autorización previa y expresa del jefe superior del servicio.

Al personal de la Agencia le serán aplicables los literales a), e), f), g), h), i), j), k), l) y m) del artículo 84 del decreto con fuerza de ley N° 29, promulgado en 2004 y publicado en 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo.

Párrafo 3°
Consejo Multisectorial sobre Ciberseguridad

Artículo 16. Consejo Multisectorial sobre Ciberseguridad. Créase el Consejo Multisectorial sobre Ciberseguridad, en adelante el Consejo, de carácter consultivo y que tendrá por función asesorar y formular recomendaciones a la Agencia en el análisis y revisión periódica de la situación de ciberseguridad del país, en el estudio de las amenazas existentes y potenciales en el ámbito de ciberseguridad, y proponer medidas para abordarlas.

El Consejo estará integrado por el Director o Directora Nacional de la Agencia, quien lo presidirá, y seis consejeros ad honorem designados por el Presidente de la República, escogidos entre personas de destacada labor en el ámbito de la ciberseguridad o de las políticas públicas vinculadas a la materia, provenientes dos del sector industrial o comercial, dos del ámbito académico y dos de las organizaciones de la sociedad civil, quienes permanecerán en su cargo durante seis años, renovándose en tríos 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 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 N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.

Artículo 17. Funcionamiento del Consejo. El Consejo sesionará a lo menos cuatro veces al año; sus recomendaciones serán de carácter público, y deberán recoger la diversidad de opiniones existentes en él cuando no haya unanimidad respecto de las mismas. Excepcionalmente y mediante decisión fundada, el Director o Directora podrá decretar secreta o reservada una parte o toda una sesión del Consejo, de lo cual se deberá dejar constancia en el acta respectiva. En este caso, se aplicará lo dispuesto en el artículo 42.

El Consejo sesionará todas las veces que sea necesario para el cumplimiento de sus funciones. La Agencia prestará el

apoyo técnico y administrativo indispensable para el adecuado funcionamiento del Consejo.

Un reglamento expedido por el Ministerio encargado de la seguridad pública determinará las demás normas necesarias para el correcto funcionamiento del Consejo.

Artículo 18. 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.

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

d) Fallecimiento.

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

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

i. Inasistencia injustificada a cuatro 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, cuando correspondiere. Respecto de la causal de la letra f), la concurrencia de dichas circunstancias facultará al Presidente de la República para decretar la remoción.

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 solo por el tiempo que falte para completar el período del consejero reemplazado.

Párrafo 4°
Red de Conectividad Segura del Estado

Artículo 19. Red de Conectividad Segura del Estado. Créase la Red de Conectividad Segura del Estado, en adelante RCSE, que proveerá servicios de interconexión y conectividad a Internet a los organismos de la Administración del Estado señalados en el artículo 1 de la presente ley.

La Agencia podrá suscribir los convenios de interconexión con instituciones públicas y privadas que considere necesarios para el mejor funcionamiento de la RCSE y de los servicios adicionales que preste.

Un reglamento expedido por el Ministerio encargado de la seguridad pública y visado por el Ministro de Hacienda regulará al funcionamiento de la RCSE y las obligaciones especiales de los organismos de la Administración del Estado.

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

Artículo 20. Equipo Nacional de Respuesta a Incidentes de Seguridad Informática. Créase dentro de la Agencia Nacional de Ciberseguridad el Equipo Nacional de Respuesta **a Incidentes** de Seguridad Informática, en adelante "CSIRT Nacional", el que tendrá las siguientes funciones:

a) Responder ante ciberataques o incidentes de ciberseguridad, cuando estos sean de efecto significativo.

b) Coordinar a los CSIRT Sectoriales frente a ciberataques o incidentes de ciberseguridad de efecto significativo. La misma coordinación deberá establecer con el CSIRT de la Defensa Nacional. En el ejercicio de esta función, el CSIRT Nacional podrá realizar todas las acciones necesarias para asegurar una respuesta rápida por parte de los CSIRT Sectoriales, incluida la supervisión de las medidas adoptadas por estos.

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) Supervisar incidentes a escala nacional.

f) Efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación.

g) Realizar entrenamiento, educación y capacitación en materia de ciberseguridad.

h) Requerir a las instituciones afectadas o a los CSIRT correspondientes, información anonimizada de incidentes de ciberseguridad y vulnerabilidades encontradas y los planes de acción respectivos para mitigarlos.

i) Difundir alertas tempranas, avisos e información sobre riesgos e incidentes para la comunidad.

j) Elaborar un informe con los criterios técnicos para la determinación de las categorías de incidentes o vulnerabilidades de ciberseguridad que estarán eximidas de notificación.

TÍTULO IV
Otras instituciones intervinientes

Artículo 21. CSIRT Sectoriales. Las autoridades sectoriales deberán constituir Equipos de Respuesta a Incidentes de Seguridad Informática Sectoriales, en adelante CSIRT Sectoriales, los que tendrán por finalidad contribuir al desarrollo de capacidades, confianza y seguridad de las redes y sistemas informáticos y proporcionar asistencia para la gestión de incidentes de ciberseguridad en sus respectivos sectores.

Los CSIRT Sectoriales tendrán las siguientes funciones:

a) Responder ante ciberataques o incidentes de ciberseguridad, dando prioridad a aquellos que puedan tener efecto significativo.

b) Colaborar e interoperar con los otros CSIRT Sectoriales, frente a ciberataques o incidentes de ciberseguridad de efecto significativo, bajo la coordinación y supervisión de la Agencia.

c) Establecer relaciones de cooperación e interoperabilidad con los otros CSIRT Sectoriales.

d) Supervisar la gestión de incidentes de ciberseguridad que afecten a su sector.

e) Efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación que afecten a su sector.

f) Realizar capacitación en materia de ciberseguridad, debiendo para ello seguir las instrucciones que al efecto pudiera dictar la Agencia.

g) Requerir a las instituciones de su sector información sobre los incidentes de ciberseguridad y vulnerabilidades encontradas y los planes de acción respectivos para mitigarlos, la que deberá ser remitida al CSIRT Nacional. La información que se remita deberá excluir datos personales.

h) Difundir alertas tempranas, avisos e información sobre riesgos e incidentes de ciberseguridad, conforme las instrucciones que dicte al efecto la Agencia.

i) Poner en conocimiento de la Agencia toda información relevante, en especial aquella referida a incidentes de ciberseguridad de efecto significativo.

j) Colaborar con la Agencia en los casos y en la forma que esta lo solicite.

En el ejercicio de sus funciones, los CSIRT Sectoriales deberán dar cumplimientos a todas aquellos protocolos y estándares técnicos, instrucciones generales y particulares, que la Agencia pudiera dictar con el objeto de lograr un nivel común de ciberseguridad y respuestas coordinadas ante la ocurrencia de incidentes de ciberseguridad. En el caso del CSIRT del sector financiero sujeto a la fiscalización de la Comisión para el Mercado Financiero, bastará con dar cumplimiento a los protocolos y estándares técnicos que la Agencia comunique ante la ocurrencia de incidentes de ciberseguridad, salvo en los casos de incidentes que pudieran tener un efecto sistémico en las redes y sistemas informáticos del país.

El incumplimiento de las instrucciones que imparta la Agencia para la respuesta coordinada de incidentes acarreará responsabilidad funcionaria de la autoridad o jefatura del CSIRT respectivo, la que podrá ser sancionada conforme lo dispuesto en los artículos 33 y 34.

Un reglamento expedido por el Ministerio encargado de la seguridad pública establecerá las instancias de

coordinación entre la Agencia y las autoridades sectoriales y sus respectivos CSIRT.

Artículo 22. Facultades especiales. Las autoridades sectoriales podrán dictar las normas de carácter general y las normas técnicas que consideren necesarias para la ciberseguridad de las instituciones de su sector, de conformidad con la regulación respectiva, las que deberán ser sometidas a aprobación previa de la Agencia, quien deberá pronunciarse en el plazo de treinta días hábiles.

Asimismo, las autoridades sectoriales deberán dictar las instrucciones, circulares y órdenes necesarias para la implementación de los protocolos y estándares técnicos establecidos por la Agencia.

En el ejercicio de estas facultades normativas, las autoridades sectoriales deberán considerar, a lo menos, los protocolos y estándares técnicos y las instrucciones generales y particulares dictados por la Agencia Nacional de Ciberseguridad. Lo anterior, sin perjuicio de que estos últimos serán obligatorios para todos los regulados aun cuando la autoridad sectorial omita referirse a ellos.

Tratándose de sus instituciones fiscalizadas, la Comisión para el Mercado Financiero podrá establecer las normas de carácter general y técnicas sobre ciberseguridad sin necesidad de solicitar la aprobación de la Agencia, siempre y cuando tengan un alcance distinto a las normas dictadas por ella. En caso de que la Comisión para el Mercado Financiero emita normativa que regule elementos contenidos en normas, protocolos o instrucciones generales dictados por la Agencia, deberá informarle previamente, remitiendo la norma, protocolo o instrucción, con una anticipación de, al menos, treinta días hábiles a su emisión por parte de la Comisión para el Mercado Financiero.

Artículo 23. Incidentes de efecto significativo. Se considerará que un incidente de ciberseguridad tiene efecto significativo si es capaz de interrumpir la continuidad de un servicio esencial o afectar la integridad física o la salud de las personas, así como en el caso de afectar sistemas informáticos que contengan datos personales. Para determinar la importancia de los efectos de un incidente, se tendrán especialmente en cuenta los siguientes criterios:

a) El número de personas afectadas.

b) La duración del incidente.

c) La extensión geográfica con respecto a la zona afectada por el incidente.

Los CSIRT Sectoriales tendrán la obligación de tomar las providencias necesarias para apoyar en el restablecimiento del servicio afectado, bajo la coordinación del CSIRT Nacional.

Deberá 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.

Artículo 24. Centros de Certificación Acreditados. Sin perjuicio de las funciones y atribuciones de la Agencia, los únicos organismos autorizados para certificar el cumplimiento de los estándares de ciberseguridad exigidos por la autoridad competente serán aquellos que cuenten con una acreditación vigente otorgada por la Agencia Nacional de Ciberseguridad, de conformidad con lo dispuesto en esta ley y en su reglamento. En el caso de los organismos de la Administración del Estado que estén sujetos a las obligaciones del artículo 6, será la Agencia la encargada de certificar el cumplimiento de dichos estándares.

Estos centros serán los únicos habilitados para certificar que un determinado ente cumple con los estándares y normas de seguridad que se exijan para la prestación de servicios al Estado, y el desarrollo de los sistemas y programas informáticos que sean utilizados por las instituciones públicas.

Una vez contratados o comprados los servicios o programas informáticos, será responsabilidad de los jefes de servicio velar por el cumplimiento de dichos estándares y normas.

Los organismos públicos en la celebración de sus contratos deberán evaluar de mejor manera y dar preferencia a los productos y servicios calificados con un nivel adecuado de seguridad por un centro certificador.

Lo establecido en este artículo no será aplicable a la defensa nacional, sector que no requerirá de la acreditación de la Agencia ni de certificación para prestar servicios a otros organismos del Estado. Asimismo, el responsable por el cumplimiento de los estándares

y normas de seguridad del sector defensa será el Estado Mayor Conjunto, del Ministerio de Defensa Nacional.

TÍTULO V
Del Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional

Artículo 25. Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional. Créase el Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional, en adelante CSIRT de la Defensa Nacional, dependiente del Ministerio de Defensa Nacional, como el organismo responsable de la coordinación, protección y seguridad de las redes y sistemas del mencionado Ministerio y de los servicios esenciales y operadores vitales para la defensa nacional, además de cumplir aquellas tareas que le sean encomendadas, con el propósito de resguardar la defensa y la seguridad nacional.

El CSIRT de la Defensa Nacional dependerá del Estado Mayor Conjunto, del Ministerio de Defensa Nacional.

Para los efectos presupuestarios, el CSIRT a que se refiere este artículo dependerá del Ministerio de Defensa Nacional; se regirá por el reglamento que este Ministerio dicte al efecto y, en lo que le sea aplicable, por la presente ley.

Artículo 26. De las funciones del CSIRT de la Defensa Nacional. Las funciones principales del CSIRT de la Defensa Nacional serán las siguientes:

a) Conducir y asegurar la protección y defensa de los riesgos y amenazas presentes en el ciberespacio, que permitan preservar la confidencialidad, integridad y disponibilidad de las redes de información, los servicios esenciales y operadores vitales para la defensa nacional. Para ello, estará a cargo de la coordinación y será enlace entre los diferentes CSIRT Institucionales de la Defensa Nacional.

b) Asumir el rol de coordinador y enlace entre la Agencia y su CSIRT Nacional con los CSIRT Institucionales de la Defensa Nacional, 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, detección, contención, protección, recuperación de los sistemas y respuesta dependientes de las Fuerzas Armadas y del Estado Mayor Conjunto, considerando los lineamientos establecidos por la Agencia.

d) Prestar colaboración o asesoría técnica en la implementación de las políticas de ciberseguridad nacionales a los CSIRT Institucionales de la Defensa Nacional.

Artículo 27. De los Equipos de Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional. En el sector de la defensa nacional se constituirán Equipos de Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional, en adelante CSIRT Institucionales de la Defensa Nacional, los que tendrán por finalidad dar respuesta, en el marco de sus competencias, a vulnerabilidades e incidentes de ciberseguridad que pongan en riesgo las instalaciones, redes, sistemas, servicios y equipos físicos y de tecnología de la información de las respectivas instituciones de la defensa nacional.

Se podrán constituir CSIRT Institucionales, conforme a los lineamientos entregados por el CSIRT de la Defensa Nacional.

Las funciones de los CSIRT Institucionales de la Defensa Nacional serán determinadas por la reglamentación que el Ministerio de Defensa Nacional dicte al efecto, de conformidad a la política de ciberdefensa y a los lineamientos generales que entregue la Agencia.

Artículo 28. Deber de reporte al CSIRT de la Defensa Nacional. Todas las instituciones de la defensa nacional deberán reportar los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos al CSIRT de la Defensa Nacional. El CSIRT de la Defensa Nacional reportará a la Agencia todos los incidentes identificados cuando no se ponga en riesgo la seguridad y la defensa nacional.

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 la Agencia, de los CSIRT, sean Nacional, de Defensa o Sectoriales, o de su personal, cualquiera que sea su cargo o la naturaleza de su vinculación jurídica con estos. Asimismo, tendrán dicho carácter aquellos otros antecedentes respecto de los cuales el personal de tales organismos del Estado tome conocimiento en el desempeño de sus funciones o con ocasión de estas.

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

Los funcionarios y funcionarias de la Agencia y del CSIRT Nacional, de Defensa o de los 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 seguridad de la información y los registros previstos en el artículo 6, 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, y

iii. Los planes de acción y mitigación de riesgos de ciberseguridad.

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

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. Las sanciones a las infracciones de la presente ley cometidas por instituciones privadas serán las siguientes:

a) Las infracciones leves serán sancionadas con amonestación escrita o multa de 1 a 1.000 unidades tributarias mensuales. En caso de que el infractor sea un operador de importancia vital, la multa podrá ser de hasta 5.000 unidades tributarias mensuales.

b) Las infracciones graves serán sancionadas con multa de 1.001 a 5.000 unidades tributarias mensuales. En caso de que el infractor sea un operador de importancia vital, la multa podrá ser de hasta 10.000 unidades tributarias mensuales.

c) Las infracciones gravísimas serán sancionadas con multa de 10.001 a 20.000 unidades tributarias mensuales.

Se consideran infracciones leves el incumplimiento de las obligaciones señaladas en esta ley que no tenga señalada una sanción especial.

Se consideran infracciones graves, las siguientes:

a) Entregar fuera de plazo la información a la autoridad u organismo de la Administración del Estado habilitado por ley para requerirla.

b) Incumplir la obligación de reportar establecida en el artículo 7.

c) Incumplir los deberes previstos en los artículos 5 y 6 de la presente ley, cuando el infractor sea un operador de servicios esenciales.

Las siguientes infracciones se consideran gravísimas, cuando el infractor sea un operador de servicios esenciales:

a) Negar injustificadamente información a la autoridad u organismo de la Administración del Estado habilitado para requerirla.

b) Entregar información falsa o manifiestamente errónea a la autoridad u organismo de la Administración del Estado habilitado para requerirla.

c) Incumplir la obligación de reportar establecida en el artículo 7.

d) Incumplir los deberes previstos en los artículos 5 y 6 de la presente ley, cuando el infractor tenga, además, la calidad de operador de importancia vital.

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 contados desde el momento en que se produjo el incidente y la capacidad económica del infractor.

Cuando por unos mismos hechos y fundamentos jurídicos, el infractor pudiese ser sancionado con arreglo a esta ley y a otra u otras leyes, de las sanciones posibles, se le impondrá la de mayor gravedad.

En ningún caso se podrá aplicar al infractor, por los mismos hechos y fundamentos jurídicos, dos o más sanciones administrativas.

Las infracciones previstas en esta ley prescribirán a los tres años de cometidas, plazo que se interrumpirá con la notificación de la formulación de cargos por los hechos constitutivos de las mismas.

Artículo 34. Procedimiento administrativo por infracción de ley. La determinación de las infracciones que cometan las instituciones privadas por vulneración de las leyes, reglamentos, estatutos y demás normas que las rijan, o por incumplimiento de las instrucciones y órdenes que les imparta la Agencia, así como la aplicación de las sanciones correspondientes se sujetará a las siguientes reglas especiales:

a) El procedimiento sancionatorio será instruido por la Agencia.

b) La Agencia podrá iniciar un procedimiento sancionatorio, de oficio o a petición de parte, o como resultado de un proceso de fiscalización. Junto con la apertura del expediente, la Agencia deberá designar un funcionario o una funcionaria responsable de la

instrucción del procedimiento, que recibirá el nombre de instructor o instructora. En el evento de que producto de una denuncia se iniciare un procedimiento administrativo sancionador, el denunciante tendrá la calidad de interesado, para todos los efectos legales.

c) La Agencia podrá formular cargos en contra de la institución privada, señalando tanto una descripción clara y precisa de los hechos que se estimen constitutivos de infracción y la fecha de su verificación, así como las normas que se estimen infringidas, la sanción y cualquier otro antecedente que sirva para sustentar la formulación.

d) La formulación de cargos deberá notificarse a la institución privada mediante carta certificada dirigida a su domicilio postal o mediante comunicación al correo electrónico que haya registrado en la Agencia.

e) La institución privada tendrá un plazo de quince días hábiles para presentar sus descargos. En esa oportunidad, la institución privada podrá acompañar todos los antecedentes que estime pertinentes para desacreditar los hechos imputados. Junto con los descargos, la institución privada deberá fijar una dirección de correo electrónico a través de la cual se realizarán todas las demás comunicaciones y notificaciones, si no lo hubiere hecho previamente.

f) Recibidos los descargos o transcurrido el plazo otorgado para ello, la Agencia examinará el mérito de los antecedentes y podrá ordenar la realización de las pericias e inspecciones que sean pertinentes. En el caso de que existan hechos sustanciales, pertinentes y controvertidos, la Agencia podrá ordenar la recepción de los demás medios probatorios que procedan, para lo cual deberá abrir un término probatorio de diez días hábiles.

g) La Agencia dará lugar a las medidas o diligencias probatorias que solicite la institución privada en sus descargos, siempre que sean pertinentes y necesarias. En caso contrario, la rechazará mediante resolución fundada.

h) Los hechos investigados y las responsabilidades de los presuntos infractores podrán acreditarse mediante cualquier medio de prueba admisible en derecho, los que se apreciarán de acuerdo a las reglas de la sana crítica.

i) La Agencia tendrá amplias facultades para solicitar antecedentes o informes que contribuyan a su resolución.

j) Cumplidos los trámites señalados en los literales anteriores, el instructor o instructora emitirá, dentro de diez días hábiles, un dictamen en el cual propondrá la absolución o la sanción que a su juicio corresponda aplicar. Dicho dictamen deberá contener la

individualización del o de los infractores; la relación de los hechos investigados y la forma como se ha llegado a comprobarlos, y la proposición al Director o Directora de las sanciones que estimare procedente aplicar o de la absolución de uno o más de los infractores.

k) Emitido el dictamen, el instructor o instructora elevará los antecedentes al Director o Directora, quien resolverá en el plazo de quince días hábiles, dictando al efecto una resolución fundada en la cual absolverá al infractor o aplicará la sanción, en su caso. No obstante, el Director o Directora podrá ordenar la realización de nuevas diligencias o la corrección de vicios de procedimiento, fijando un plazo para tales efectos, dando audiencia al investigado. Ninguna persona podrá ser sancionada por hechos que no hubiesen sido materia de cargos.

l) La resolución que ponga fin al procedimiento sancionatorio deberá ser fundada y resolver todas las cuestiones planteadas en el expediente, pronunciándose sobre cada una de las alegaciones y defensas formuladas por la institución privada, y contendrá la declaración de haberse configurado por la institución privada la infracción a la normativa aplicable, o su absolución, según corresponda. En caso de que la Agencia considere que se ha verificado la infracción, en la misma resolución ponderará las circunstancias que agravan o atenúan la responsabilidad del infractor e impondrá la sanción, de acuerdo a la gravedad de la infracción cometida.

m) La resolución que establezca la infracción a la normativa sobre ciberseguridad y aplique la sanción correspondiente deberá ser fundada. Esta resolución deberá indicar los recursos administrativos y judiciales que procedan contra ella en conformidad a esta ley, los órganos ante los que deben presentarse y los plazos para su interposición. La resolución de la Agencia que resuelve el procedimiento por infracción de ley será reclamable mediante recurso de reposición que se podrá interponer en el plazo de cinco días hábiles contados desde la notificación, el que deberá ser resuelto por el Director o Directora dentro del plazo de treinta días hábiles.

n) El procedimiento administrativo de infracción de ley no podrá superar los seis meses contados desde la notificación a que se refiere el literal d) anterior.

Artículo 35. Procedimiento de reclamación judicial. Las personas que estimen que un acto administrativo que paraliza el procedimiento, o una resolución final o de término emanado de la Agencia, sea ilegal y les cause perjuicio, podrán deducir un reclamo de ilegalidad ante la Corte de Apelaciones de Santiago o la del lugar donde se encuentre domiciliado el reclamante, a elección de este último. El

reclamo deberá interponerse dentro de los quince días hábiles siguientes a la notificación de la resolución impugnada, según las siguientes reglas:

a) El reclamante señalará en su escrito, con precisión, la resolución objeto del reclamo, la o las normas legales que se suponen infringidas, la forma en que se ha producido la infracción y, cuando procediere, las razones por las cuales el acto le causa agravio.

b) La Corte podrá declarar inadmisible la reclamación si el escrito no cumple con las condiciones señaladas en la letra a) anterior. Asimismo, podrá decretar orden de no innovar cuando la ejecución del acto impugnado le produzca un daño irreparable al recurrente.

c) Recibida la reclamación, la Corte requerirá el informe de la Agencia, concediéndole un plazo de diez días hábiles al efecto.

d) Evacuado el traslado o teniéndosele por evacuado en rebeldía, la Corte podrá abrir un término de prueba, si así lo estima necesario, el que se regirá por las reglas de los incidentes que contempla el Código de Procedimiento Civil.

e) Vencido el término de prueba, se ordenará traer los autos en relación. La vista de esta causa gozará de preferencia para su inclusión en la tabla.

f) Si la Corte da lugar al reclamo, en su sentencia decidirá si existió agravio y ordenará, cuando sea procedente, la rectificación del acto impugnado y la dictación de la respectiva resolución, según corresponda.

g) Tratándose de reclamaciones en contra de una resolución que resuelve un procedimiento sancionatorio, la Corte podrá rechazar o acoger la resolución impugnada, establecer o desechar la comisión de la infracción, según corresponda, y mantener, dejar sin efecto o modificar la sanción impuesta al responsable o su absolución, según sea el caso.

h) Contra la resolución de la Corte de Apelaciones no procederá recurso alguno.

i) En todo aquello no regulado por el presente artículo, regirán las normas establecidas en el Código Orgánico de Tribunales y en el Código de Procedimiento Civil, según corresponda.

Artículo 36. Responsabilidad administrativa del jefe superior del organismo público. El jefe superior de un organismo

público deberá velar porque el organismo respectivo aplique las medidas idóneas y necesarias para prevenir, reportar y resolver incidentes de ciberseguridad con arreglo a los principios y obligaciones establecidos en los Títulos I y II de esta ley, respectivamente.

Asimismo, los organismos de la Administración del Estado deberán someterse a las medidas tendientes a subsanar o prevenir las infracciones que indique la Agencia.

Las infracciones a los principios y obligaciones contenidos en los artículos 21 y 29 serán sancionadas con multa de veinte por ciento a cincuenta por ciento de la remuneración mensual del jefe superior del organismo público infractor. La cuantía de la multa se determinará considerando la gravedad de la infracción, la naturaleza del incidente y el número de personas afectadas, si las hubiere. En la determinación de la sanción se deberán considerar también las circunstancias que atenúan la responsabilidad del infractor.

Si el organismo público persiste en la infracción, se le aplicará al jefe superior del organismo público el duplo de la sanción originalmente impuesta y la suspensión en el cargo por un lapso de cinco días hábiles.

Las infracciones en que incurra un organismo público serán determinadas por la Agencia, de acuerdo al procedimiento establecido en el artículo 34.

Habiéndose configurado la infracción, las sanciones administrativas señaladas en este artículo serán aplicadas por la Agencia. Con todo, la Contraloría General de la República, a petición de la Agencia podrá, de acuerdo a las normas de su ley orgánica, incoar los procedimientos administrativos y proponer las sanciones que correspondan.

En contra de las resoluciones de la Agencia se podrá deducir el reclamo de ilegalidad establecido en el artículo 35.

Las sanciones previstas en este artículo deberán ser publicadas en el sitio web de la Agencia y del organismo o servicio de que se trate dentro del plazo de cinco días hábiles contados desde que la respectiva resolución quede firme.

Artículo 37. Responsabilidad del funcionario o funcionaria infractor. Sin perjuicio de lo dispuesto en el artículo anterior, si en el procedimiento administrativo correspondiente se determina que existen responsabilidades individuales de uno o más funcionarios o funcionarias del organismo público, la responsabilidad administrativa se

hará efectiva con sujeción a las normas estatutarias que rijan al organismo en que se produjo la infracción.

En caso de que el procedimiento administrativo correspondiente determine que cualquiera de los funcionarios o funcionarias involucrados es responsable de alguna de las infracciones gravísimas señaladas en el artículo 33 de esta ley, esta conducta se considerará una contravención grave a la probidad administrativa.

Artículo 38. Agravante especial. Si como consecuencia de la perpetración de un delito resultare afectada gravemente la continuidad operativa de un operador de importancia vital, 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 informáticos relevantes del operador de importancia vital o en la obstaculización del acceso o la alteración perjudicial del funcionamiento de su sistema informático.

TÍTULO VIII
Del Comité Interministerial de Ciberseguridad

Artículo 39. Comité Interministerial sobre Ciberseguridad. Créase el Comité Interministerial sobre Ciberseguridad, en adelante el Comité, que tendrá por objeto asesorar al Presidente de la República en materias de ciberseguridad relevantes para el funcionamiento del país.

En el ejercicio de sus funciones, el Comité deberá:

a) Asesorar al Presidente de la República en el análisis y definición de la Política Nacional de Ciberseguridad, que contendrá las medidas, planes y programas de acción específicos que se aplicarán para su ejecución y cumplimiento.

b) Proponer al Presidente de la República cambios a la normativa constitucional, legal o reglamentaria vigente cuando esta incida en materias de ciberseguridad.

c) Coordinar la implementación de la Política Nacional de Ciberseguridad.

d) Aprobar la lista de servicios esenciales propuesto por la Agencia, y sus modificaciones.

e) Aprobar la lista de operadores de importancia vital propuesto por la Agencia, y sus modificaciones.

f) Apoyar las funciones de la Agencia Nacional de Ciberseguridad en lo que resulte necesario.

g) Revisar y tener en consideración las recomendaciones del Consejo Multisectorial sobre Ciberseguridad.

Artículo 40. De los integrantes del Comité. El Comité estará integrado por los siguientes miembros permanentes:

a) Por el Subsecretario del Interior o quien este designe.

b) Por el Subsecretario de Defensa o quien este designe.

c) Por el Subsecretario de Relaciones Exteriores o quien este designe.

d) Por el Subsecretario General de la Presidencia o quien este designe.

e) Por el Subsecretario de Telecomunicaciones o quien este designe.

f) Por el Subsecretario de Hacienda o quien este designe.

g) Por el Subsecretario de Ciencia, Tecnología, Conocimiento e Innovación o quien este designe.

h) Por el Director o Directora Nacional de la Agencia Nacional de Inteligencia.

i) Por el Director o Directora Nacional de la Agencia Nacional de Ciberseguridad, quien lo presidirá.

Con todo, el Comité podrá invitar a participar de sus sesiones a funcionarios o funcionarias 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 41. 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.

Al Director o Directora Nacional de la Agencia le corresponderá, entre otras funciones, convocar, dirigir y registrar las sesiones e implementar los acuerdos que se adopten.

Artículo 42. De la información reservada. Constituido el Comité en sesión secreta, los funcionarios **o funcionarias** 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 43. Del reglamento. Un reglamento expedido por el **Ministerio encargado de la seguridad pública** fijará las normas de funcionamiento del Comité.

Título IX
Órganos autónomos constitucionales

Artículo 44. Regímenes especiales. Corresponderá a las autoridades superiores de los órganos internos del Congreso Nacional, el Poder Judicial, la Contraloría General de la República, el Ministerio Público, el Tribunal Constitucional, el Banco Central, el Servicio Electoral y la Justicia Electoral y el Consejo Nacional de Televisión adoptar las medidas especiales de ciberseguridad señaladas en el artículo 6 de la presente ley, debiendo dictar para ello las políticas, normas e instrucciones necesarias para dar cumplimiento a los principios y obligaciones establecidos en esta ley, pudiendo requerir para ello la asistencia técnica de la Agencia Nacional de Ciberseguridad. En este caso, las referencias al reglamento contenidas en el artículo 6, se entenderán efectuadas a las normas que adopten los respectivos órganos internos.

Asimismo, las autoridades de estos órganos ejercerán la potestad disciplinaria respecto de sus funcionarios y funcionarias, en relación a las infracciones a esta ley que se produzcan y, del mismo modo, les corresponderá ejercer las demás funciones y adoptar las decisiones que esta ley encomienda a la Agencia, para fines de dar cumplimiento a lo previsto en este artículo.

Las instituciones y órganos señalados en este artículo no estarán sujetos a la regulación, fiscalización o supervigilancia de la Agencia. Sin perjuicio de ello, deberán acordar mecanismos de coordinación, cooperación, reporte de incidentes e intercambio de información sobre ciberseguridad, respecto de la Agencia y las demás autoridades o instancias previstas en esta ley, incluyéndose la conformación o participación en equipos de respuesta a incidentes de ciberseguridad. En este contexto, si además fuere requerido el acceso por parte de la Agencia a redes y sistemas informáticos de los referidos órganos, deberá contarse con su autorización previa, debiendo cautelarse para ello la continuidad de sus operaciones. En caso de que los antecedentes que se soliciten o la información a la que se acceda sean confidenciales o reservados, la Agencia deberá conservarlos en ese carácter.

Corresponderá a los señalados órganos determinar e informar a la Agencia sobre su carácter de operador de importancia vital, en los términos del artículo 4, e informarle, con la periodicidad que se acuerde, las infraestructuras, servicios o funciones específicos que se identifiquen en esta condición.

Asimismo, si el órgano autónomo constitucional revistiere además el carácter de autoridad sectorial, deberá considerarse su opinión previa en relación con las personas o entidades reguladas o supervisadas por ella, que pudieren calificarse como operadores de importancia vital.

TÍTULO X

De las modificaciones a otros cuerpos legales

Artículo 45. Incorpórase, en el artículo 25 de la ley N° 20.424, Estatuto Orgánico del Ministerio de Defensa Nacional, la siguiente letra k), nueva:

"k) Conducir al Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional en coordinación con la Subsecretaría de Defensa.".

Artículo 46. Introdúcense las siguientes enmiendas a la 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:

1. Incorpórase, en el artículo 2°, los siguientes incisos finales, nuevos:

“No será objeto de sanción penal el que, realizando labores de investigación en seguridad informática, hubiere incurrido en los hechos tipificados en el inciso primero, siempre que se cumplan las siguientes condiciones:

1) Haber reportado el acceso y las vulnerabilidades de seguridad detectadas en su investigación al responsable de las redes y sistemas informáticos afectados, en forma inmediata y a más tardar en el momento en que alerte a la Agencia Nacional de Ciberseguridad;

2) Haber dado cumplimiento a las demás condiciones sobre comunicación responsable de vulnerabilidades que al efecto hubiere dictado la Agencia Nacional de Ciberseguridad;

3) Que el acceso no haya sido realizado con el ánimo de apoderarse o de usar la información contenida en el sistema informático, ni con intención fraudulenta. Tampoco podrá haber actuado más allá de lo que era necesario para comprobar la existencia de una vulnerabilidad, ni utilizado métodos que pudieran conducir a denegación de servicio, a pruebas físicas, utilización de código malicioso, ingeniería social y alteración, eliminación, ex filtración o destrucción de datos, y

4) No haber divulgado públicamente la información relativa a la potencial vulnerabilidad.

Tampoco será objeto de sanción penal la persona que comunique a la Agencia información una vulnerabilidad potencial de la que haya tomado conocimiento en su contexto laboral o con ocasión de la prestación de sus servicios, ni se considerará que ha incumplido con ello su obligación de secreto profesional.”.

2. Derógase el artículo 16.

Artículo 47. Incorpórase, en el artículo 8° de la ley N° 19.974, sobre el sistema de inteligencia del Estado y crea la Agencia Nacional de Inteligencia, el siguiente literal h), nuevo:

“h) Elaborar, a requerimiento de la Agencia Nacional de Ciberseguridad, un informe fundado sobre los servicios que deban calificarse como esenciales para el mantenimiento de las actividades sociales o económicas cruciales para el país, que dependan de las redes y sistemas informáticos, cuya afectación, interceptación, interrupción o destrucción pueda 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. Asimismo, el informe se pronunciará sobre los

operadores que resultan de importancia vital para la provisión de esos servicios esenciales.”.

Artículo 48. Derógase la letra a) del artículo 8° de la ley N° 7.401, que reprime las actividades que vayan contra la seguridad exterior del Estado.

TÍTULO XI

Disposiciones transitorias

Artículo primero. Entrada en vigencia y personal. 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 a través 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. Determinar la fecha para la iniciación de actividades de la Agencia, la cual podrá contemplar un período para su implementación y uno a contar del cual entrará en operaciones.

2. Fijar el sistema de remuneraciones del personal de la Agencia y las normas necesarias para la fijación de las remuneraciones variables, en su aplicación transitoria.

3. Fijar la planta de personal de Directivos de la Agencia, pudiendo al efecto fijar el número de cargos, los requisitos para el desempeño de los mismos, sus denominaciones y los cargos que se encuentren afectos al Título VI de la ley N° 19.882. Además, determinará la fecha de entrada en vigencia de dicha planta.

4. El personal que a la fecha de inicio de actividades de la Agencia se encuentre prestando servicios a honorarios en la Subsecretaría del Interior y cuyo traspaso se determine de conformidad a los incisos tercero y cuarto de este numeral, podrá optar por modificar su estatuto laboral al Código del Trabajo, siempre que cumpla con los requisitos respectivos y otorgue previamente su consentimiento.

En la medida que el personal señalado en el inciso anterior cumpla con los requisitos respectivos y dé su consentimiento, las modificaciones de estatuto laboral señaladas en el inciso precedente deberán incluirse en la dotación máxima de personal del primer presupuesto que se fije para la Agencia.

En el respectivo decreto con fuerza de ley, se determinará la forma y el número de personas a honorarios a traspasar sin solución de continuidad, desde la Subsecretaría del Interior a la Agencia, además, el plazo en que se llevará a cabo este proceso. Conjuntamente con el traspaso del personal, se traspasarán los recursos presupuestarios que se liberen por este hecho y, a su vez, un número equivalente al de los honorarios traspasados deberá ser reducido del número máximo de personas a ser contratadas a honorarios fijado en las glosas presupuestarias correspondientes de la Subsecretaría del Interior.

La individualización del personal traspasado conforme al inciso anterior, 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.

El personal a honorarios que pase a ser Código del Trabajo de acuerdo a lo señalado en este artículo, mantendrá una remuneración líquida mensualizada que le permita mantener su honorario líquido mensual.

5. Determinar la dotación máxima de personal de la Agencia.

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

Artículo segundo. 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 **o Directora** de la Agencia Nacional de Ciberseguridad, quien asumirá de inmediato, por el plazo máximo de un año y en tanto se efectúa el proceso de selección pertinente que establece la señalada ley para los cargos del Sistema de Alta Dirección Pública. 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 **o Directora**, siempre que no se encuentre vigente la respectiva planta de personal. La remuneración del primer Director **o Directora** 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. 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. 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. En el tiempo intermedio en que los ministerios, subsecretarías, superintendencias y demás organismos 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 estos, de conformidad a lo dispuesto en el artículo 21, el CSIRT Nacional tendrá, para todos los efectos legales, la calidad de CSIRT Sectorial correspondiente, con todas sus atribuciones y facultades.

Artículo sexto. Renovación de los miembros del Consejo Multisectorial sobre Ciberseguridad. Para los efectos de la renovación parcial de los miembros del Consejo Multisectorial sobre Ciberseguridad a que se refiere el inciso segundo del artículo 16, 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) Tres consejeros durarán en sus cargos un plazo de tres años.

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

Artículo séptimo. 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.

Artículo octavo. Sobre los servicios esenciales. Hasta que no se dicten los respectivos decretos señalados en el artículo 4 de la ley, serán calificados como servicios esenciales para los efectos de esta ley, los servicios públicos de telecomunicaciones, incluyendo los servicios de transmisión de datos; los servicios de generación,

transmisión y distribución eléctrica; los servicios sanitarios y de suministro de agua potable, excluyendo los servicios sanitarios rurales; los servicios bancarios y financieros; las prestaciones de salud, incluyendo cualquier institución pública o privada que realice tratamiento de datos personales de salud, salvo aquellos prestados por municipios o corporaciones municipales; los órganos de la administración del Estado, excluyendo a las municipalidades y gobernaciones provinciales y regionales; el Poder Judicial, y el Poder Legislativo. La Agencia identificará, mediante resolución exenta, los operadores de importancia vital que quedarán sujetos a las obligaciones establecidas en el artículo 6 de esta ley.".

- - -

Acordado en sesión celebrada el día 25 de abril de 2023, con asistencia de los Honorables Senadores señores Juan Antonio Coloma Correa (José Manuel Rojo Edwards Silva), José Miguel Insulza Salinas, Ricardo Lagos Weber (Presidente), Daniel Núñez Arancibia (Presidente accidental) y Kenneth Pugh Olavarría.

A 25 de abril de 2023.

MARÍA SOLEDAD ARAVENA
Secretaria de la Comisión

RESUMEN EJECUTIVO

INFORME DE LA COMISIÓN DE HACIENDA, 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: todas las normas de competencia de la Comisión fueron aprobadas, en los mismos términos, por la unanimidad de sus integrantes (5x0).

III. ESTRUCTURA DEL PROYECTO APROBADO POR LA COMISIÓN: consta de 48 artículos permanentes y de ocho artículos transitorios.

IV. NORMAS DE QUÓRUM ESPECIAL: En lo relativo a las normas de quórum especial, la Comisión de Hacienda se remite a lo consignado en el segundo informe de las comisiones de Defensa Nacional y de Seguridad Pública, unidas.

V. URGENCIA: “discusión inmediata”.

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

VII. TRÁMITE CONSTITUCIONAL: primer trámite.

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

IX. TRÁMITE REGLAMENTARIO: informe de la Comisión de Hacienda.

X. NORMAS QUE SE MODIFICAN O QUE SE RELACIONAN CON LA MATERIA: 1.- Constitución Política de la República. 2.- Código del Trabajo. 3.- Código Penal. 4.- Decreto con fuerza de ley N° 29, promulgado en 2004 y publicado en 2005, del Ministerio de Hacienda, que fija texto refundido, coordinado y sistematizado de la ley Nº 18.834, sobre Estatuto Administrativo. 5.- Decreto con fuerza de ley N° 1, promulgado en 2000 y publicado en 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. 6.- Ley N° 20.502, que crea el Ministerio del Interior y Seguridad Pública y el Servicio Nacional para la

Prevención y Rehabilitación del consumo de drogas y alcohol, y modifica diversos cuerpos legales. 7.- Decreto 2.421, de 1964, del Ministerio de Hacienda, que fija el texto refundido de la ley de organización y atribuciones de la Contraloría General de la República. 8.- Ley N° 20.416, que fija normas especiales para las empresas de menor tamaño. 9.- Ley N° 21.000, que crea la Comisión para el Mercado Financiero. 10.- Ley N° 21.105, que crea el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación. 11.- Ley N° 20.424, Estatuto Orgánico del Ministerio de Defensa Nacional. 12.- Ley N° 21.180, sobre transformación digital del Estado. 13.- Ley N° 20.285, sobre acceso a la información pública. 14.- Ley N° 19.882, que regula nueva política de personal a los funcionarios públicos que indica. 15.-Ley N° 19.628, sobre protección de la vida privada. 16.- Ley N° 19.974, sobre el sistema de inteligencia del Estado y crea la Agencia Nacional de Inteligencia. 17.- Ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado. 18.- Ley N° 20.880, sobre probidad en la función pública y prevención de los conflictos de intereses. 19.- Ley N° 7.401, que reprime las actividades que vayan contra la seguridad exterior del estado. 20.- Decreto con fuerza de ley N° 1, de 1993, del Ministerio de Hacienda, fija el texto refundido, coordinado y sistematizado de la ley orgánica del Consejo de Defensa del Estado. 21.- Decreto con fuerza de ley N° 262, de 1977, del Ministerio de Hacienda, que aprueba el reglamento de viáticos para el personal de la administración pública. 22.- Decreto supremo N° 1, de 1991, del Ministerio de Hacienda, que fija monto de viáticos en dólares para el personal que debe cumplir comisiones de servicio en el extranjero. 23.- Decreto ley N° 1.263, de 1975, de administración financiera del Estado. 24.- Decreto N° 83, de 2017, del Ministerio de Relaciones Exteriores, que promulga el Convenio sobre la Ciberdelincuencia (Convenio de Budapest). 25.- 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. 26.- Ley N° 21.113, que declara el mes de octubre como el de la ciberseguridad. 27.- Ley N° 18.168, general de telecomunicaciones. 28.- Decreto N° 533, de 2015, del Ministerio del Interior y Seguridad Pública, que crea el Comité Interministerial sobre Ciberseguridad. 29.- Instructivo Presidencial 1/2017, de 27 de abril de 2017, que aprueba e instruye la implementación de la Política Nacional de Ciberseguridad. 30.- Decreto N° 3, de 2018, del Ministerio de Defensa Nacional, que aprueba la Política de Ciberdefensa. 31.- Ley N° 21.130, que moderniza la legislación bancaria. 32.- Ley N° 20.453, que consagra el principio de neutralidad en la red para los consumidores y usuarios de internet. 33.- 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. 34.- Decreto supremo N° 83, promulgado en 2004 y publicado en 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.

Valparaíso, 25 de abril de 2023.