INFORME DE LA COMISION DE HACIENDA RECAÍDO EN EL PROYECTO DE LEY QUE ESTABLECE UNA LEY MARCO SOBRE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA DE LA INFORMACIÓN.

Boletín N° 14.847-06(S)

HONORABLE CÁMARA:

La Comisión de Hacienda pasa a informar, en cumplimiento del inciso segundo del artículo 17 de la ley N° 18.918, Orgánica Constitucional del Congreso Nacional, y conforme a lo dispuesto en el inciso segundo del artículo 226 del Reglamento de la Corporación, el proyecto de ley mencionado en el epígrafe, originado en Mensaje del entonces Presidente de la República, don Sebastián Piñera Echenique, ingresado a tramitación el 15 de marzo de 2022.

La referida iniciativa se encuentra en segundo trámite constitucional y fue tratada en su primer informe reglamentario por la Comisión de Seguridad Ciudadana. Se encuentra con urgencia calificada de Suma

Asistió en representación del Ejecutivo, el Subsecretario del Ministerio del Interior señor Manuel Monsalve Benavides.

I.-CONSTANCIAS REGLAMENTARIAS

1.-Artículos que deben ser conocidos por esta Comisión de Hacienda.

La Comisión Técnica señaló en tal condición a los siguientes artículos por incidir en materias presupuestarias o financieras de la administración del Estado:

Artículo 8 inciso primero, en sus letras a), b) c), d), g), h) e i); artículo 10 inciso primero; articulo 11 letras f) e i); artículo 12; artículo 13; artículo 14 letra e); artículo 15; artículo 17 incisos cuarto, quinto, sexto, séptimo, octavo y final; artículo 23 inciso primero; artículo 24; artículo 29; artículo 36; artículo 40 incisos primero y segundo, y artículo 51 inciso segundo, permanentes, y artículos primero, segundo, tercero y sexto transitorios.

2.- Normas de quórum especial: No hubo nuevas normas que calificar en este trámite, en tal carácter.

3.- Artículos modificados: El artículo segundo transitorio está en tal condición en cuanto fue suprimido su inciso segundo con el siguiente texto:

“Con todo, conforme a este artículo no podrá ser nombrado en el cargo de Director o Directora de la Agencia, quien hubiere ejercido el cargo de Coordinador Nacional de Ciberseguridad, dependiente del. Ministerio del Interior y Seguridad Pública, los tres años previos a la publicación de esta ley en el Diario Oficial”.

4.- Artículos aprobados en los mismos términos propuestos por la Comisión Técnica:

Todos, con excepción de la disposición segunda transitoria.

5- Indicaciones declaradas inadmisibles: No hubo, en este trámite.

6.- Artículos nuevos: No hay

7.- Diputado Informante: Se designó al señor Miguel Mellado Suazo.

II.-SÍNTESIS DE LAS IDEAS MATRICES O FUNDAMENTALES

Resguardar a las personas en sus derechos, patrimonio y seguridad en relación con la información que reciben en el ciberespacio, mediante la implementación de la Política Nacional de Ciberseguridad, orientada hacia la protección de los derechos fundamentales de la sociedad en su conjunto, creando, por una parte, 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, respecto 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, y por la otra parte, promover la educación, formación y generación de capacidades en materia de ciberseguridad, en coordinación con los otros órganos que componen la Administración del Estado.

III.-CONTENIDO DEL PROYECTO DE LEY

El proyecto de ley consta de 55 artículos permanentes y seis transitorios mediante los cuales establece la Ley marco sobre Ciberseguridad con el siguiente contenido:[1]

- 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.

[1] Exposición efectuada en la comisión de Seguridad Ciudadana por el Subsecretario del Ministerio del Interior señor Manuel Monsalve

CSIRT Nacional: Equipo Nacional de Respuesta a Incidentes de Seguridad Informática

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

IV.-NORMAS DE COMPETENCIA DE LA COMISIÓN DE HACIENDA

La comisión técnica señaló en tal condición a los siguientes artículos, por incidir en materias presupuestarias o financieras de la administración del Estado:

Artículo 8 inciso primero, en sus letras a), b) c), d), g), h) e i); artículo 10 inciso primero; articulo 11 letras f) e i); artículo 12; artículo 13; artículo 14 letra e); artículo 15; artículo 17 incisos cuarto, quinto, sexto, séptimo, octavo y final; artículo 23 inciso primero; artículo 24; artículo 29; artículo 36; artículo 40 incisos primero y segundo, y artículo 51 inciso segundo, permanentes, y artículos primero, segundo, tercero y sexto transitorios.

V.-INCIDENCIA EN MATERIA FINANCIERA O PRESUPUESTARIA DEL ESTADO

El Ejecutivo adjuntó los siguientes informes financieros elaborados por la Dirección de Presupuestos del Ministerio de Hacienda: N° 043, de 10 de marzo de 2022 que acompañó al proyecto a su ingreso; y los informes que se señalan, algunos sustitutivos y otros que actualizan la estimación de costos reportados con motivo de la presentación de indicaciones tanto en el Senado como en este segundo trámite constitucional: IF complementario N° 204, de 11 de noviembre de 2022; IF sustitutivo de los anteriores N° 211, de 21 de noviembre de 2022; IF complementario N° 064, de 11 de abril de 2023, IF complementario N° 142, de 10 de julio de 2023, IF complementario N° 209 de 27 de septiembre de 2023, IF N° 218, de 11 de octubre de 2023, IF N° 228, de 18 de octubre de 2023 e IF N° 234, de 25 de octubre de 2023.

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.

Gasto asociado

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 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.

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.".

Informe financiero complementario

- 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:

Antecedentes

Mediante indicaciones, el Ejecutivo (N° 023-371) se incorpora 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.

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.

Gasto asociado

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).

Nuevas indicaciones acompañadas de informes financieros que indican que no irrogan gasto fiscal:

Informe financiero N°142 de 10 de julio de 2023

-Se elimina la excepción de aplicabilidad de las disposiciones de la ley a las empresas y sociedades del Estado o en que éste tenga participación accionaria superior al 50% o mayoría en el directorio, con lo que se les da un tratamiento similar a cualquier empresa privada.

-Se determinan en la ley los servicios esenciales, previamente sólo se consideraban el procedimiento y características que debían considerarse para calificar a servicios como tales, y, en consecuencia, se identifican los siguientes servicios esenciales: telecomunicaciones; infraestructura digital; ciberseguridad; generación, transmisión y distribución eléctrica; producción, transporte, almacenamiento y distribución de combustibles; sanitarios y de suministro de agua potable; servicios comerciales de transportes aéreos, ferroviarios y marítimos; portuarios; aeroportuarios; bancarios y financieros; de administración de fondos previsionales, de fondos de cesantía y los servicios de salud previsional; de prestaciones de salud. Asimismo, se indica que, mediante resolución, la Agencia Nacional de Ciberseguridad (ANCI) podrá calificar otros servicios como servicios esenciales considerando ciertos criterios establecidos en la ley.

-Se establece como obligación el requerimiento de informes a las autoridades sectoriales competentes y a las entidades que puedan ser calificadas como operadores de importancia vital.

-Se establece como obligación para los organismos del Estado e instituciones privadas el aplicar permanente las instrucciones generales y particulares dictadas por la ANCI y se determina que éstas deberán ser establecidas de manera proporcional en relación con los riesgos que presentan las redes y sistemas informáticos de que se trate, teniendo en cuenta el grado de progreso de dichas obligaciones y, en su caso, las normas nacionales o internacionales aplicables, así como el coste de su aplicación.

-Se realizan cambios en el proceso para reportar incidentes de ciberseguridad al CSIRT Nacional y se aplica la obligación de reportar a los organismos de la Administración del Estado, así como los operadores de servicios esenciales y los operadores de importancia vital, además de las instituciones privadas determinados por la ANCI.

-Se establece que la información a la que la ANCI tenga acceso, que incluya datos personales, deberá ser anonimizada, siempre que esto no entorpezca con sus funciones.

-Se profundiza en el alcance de la función fiscalizadora de la ANCI, al especificar las actividades y acciones que ésta podrá ejercer en el ejercicio de esta función.

-Se establece que la ANCI podrá homologar certificaciones técnicas internacionales o extranjeras sobre ciberseguridad mediante resolución fundada de su director o directora.

-Se incorpora dentro de los aspectos a determinar a través de decreto con fuerza de ley, el periodo para la vigencia de las normas establecidas por la presente ley, el cual no podrá ser inferior a seis meses desde su publicación.

Informe financiero N°209 de 27 de septiembre de 2023

-Se elimina la excepción de aplicabilidad de las disposiciones de la ley a las empresas y sociedades del Estado o en que éste tenga participación accionaria superior al 50% o mayoría en el directorio, con lo que se les da un tratamiento similar a cualquier empresa privada.

-Se determinan en la ley los servicios esenciales, previamente sólo se consideraban el procedimiento y características que debían considerarse para calificar a servicios como tales, y, en consecuencia, se identifican los siguientes servicios esenciales: telecomunicaciones; infraestructura digital; ciberseguridad; generación, transmisión y distribución eléctrica; producción, transporte, almacenamiento y distribución de combustibles; sanitarios y de suministro de agua potable; servicios comerciales de transportes aéreos, ferroviarios y marítimos; portuarios; aeroportuarios; bancarios y financieros; de administración de fondos previsionales, de fondos de cesantía y los servicios de salud previsional; de prestaciones de salud. Asimismo, se indica que, mediante resolución, la Agencia Nacional de Ciberseguridad (ANCI) podrá calificar otros servicios como servicios esenciales considerando ciertos criterios establecidos en la ley.

-Se establece como obligación el requerimiento de informes a las autoridades sectoriales competentes y a las entidades que puedan ser calificadas como operadores de importancia vital.

-Se establece como obligación para los organismos del Estado e instituciones privadas el aplicar permanente las instrucciones generales y particulares dictadas por la ANCI y se determina que éstas deberán ser establecidas de manera proporcional en relación con los riesgos que presentan las redes y sistemas informáticos de que se trate, teniendo en cuenta el grado de progreso de dichas obligaciones y, en su caso, las normas nacionales o internacionales aplicables, así como el coste de su aplicación.

-Se realizan cambios en el proceso para reportar incidentes de ciberseguridad al CSIRT Nacional y se aplica la obligación de reportar a los organismos de la

Administración del Estado, así como los operadores de servicios esenciales y los operadores de importancia vital, además de las instituciones privadas determinados por la ANCI.

-Se establece que la información a la que la ANCI tenga acceso, que incluya datos personales, deberá ser anonimizada, siempre que esto no entorpezca con sus funciones.

-Se profundiza en el alcance de la función fiscalizadora de la ANCI, al especificar las actividades y acciones que ésta podrá ejercer en el ejercicio de esta función.

-Se establece que la ANCI podrá homologar certificaciones técnicas internacionales o extranjeras sobre ciberseguridad mediante resolución fundada de su director o directora.

-Se incorpora dentro de los aspectos a determinar a través de decreto con fuerza de ley, el periodo para la vigencia de las normas establecidas por la presente ley, el cual no podrá ser inferior a seis meses desde su publicación.

Informe financiero N° 218, de 11 de octubre de 2023

a) En términos de información, se faculta a la Agencia para requerir a:

i. El CSIRT Nacional y a los demás organismos pertenecientes a la Administración del Estado la información que sea necesaria para el cumplimiento de sus fines;

ii. Las entidades obligadas por la presente ley que hayan visto afectados sus servicios por un incidente de ciberseguridad o ciberataque, que entreguen a los potenciales afectados información veraz, suficiente y oportuna sobre su ocurrencia;

iii. Los organismos de la Administración del Estado y a las instituciones privadas señaladas, la información necesaria para prevenir la ocurrencia de incidentes de ciberseguridad o para gestionar uno que ya hubiera ocurrido;

Además, la Agencia podrá requerir, mediante instrucción de su Director o Directora, el acceso a redes o sistemas informáticos en casos de incidentes de impacto significativo cuya gestión lo haga imprescindible. En caso de que la Agencia requiriera la restricción del acceso o uso de redes o sistemas informáticos deberá actuar conjuntamente con la autoridad sectorial correspondiente.

b) Modificar la atribución de la Agencia para cooperar con organismos internacionales, restringiéndola a servir como punto de contacto con las autoridades nacionales de ciberseguridad extranjeras o sus homólogos, y con los organismos internacionales con competencia en materia de ciberseguridad, y cooperando con dichas organizaciones sujeta a la coordinación con el Ministerio de Relaciones Exteriores.

c) Para el cumplimiento de la función fiscalizadora de la Agencia:

i. Se permite instruir de manera particular auditorías por sí o mediante terceros autorizados, y análisis de seguridad basados en criterios de evaluación de riesgos objetivos. Además, establece que la entidad fiscalizada deberá cooperar en todo momento con los funcionarios de la Agencia o con los terceros autorizados por ella, según corresponda.

ii. Facultar a esta para instruir de manera particular a los sujetos obligados que realicen pruebas que demuestren la implementación de los planes de continuidad operacional y ciberseguridad.

iii. Exceptuar de la obligación de concurrir a declarar respecto de hechos cuyo conocimiento estime necesario para el cumplimiento de sus funciones, a las personas

indicadas en el artículo 361 del Código de Procedimiento Civil, las cuales deberán pedir declarar por escrito.

d) Establecer estándares de ciberseguridad y deberes de información al público sobre riesgos de seguridad de dispositivos digitales disponibles a consumidores finales.

e) Determinar que los operadores de importancia vital deben obtener las certificaciones de ciberseguridad que señala la ley y las que determine la Agencia mediante reglamento a través de organismos que sean parte del registro de entidades certificadoras autorizadas, a cargo de la Agencia. Además, la Agencia podrá homologar certificaciones técnicas internacionales o extranjeras sobre ciberseguridad mediante resolución fundada de su director o directora.

f) Especificar que, en caso de un procedimiento sancionatorio iniciado por la Agencia, esta deberá abstenerse cuando existiera un procedimiento administrativo en curso, o dejar de conocer si se iniciare uno por la autoridad sectorial correspondiente dentro de los plazos legales. Igualmente, en caso de que la Agencia tome conocimiento de un supuesto hecho infractor cuya fiscalización y sanción corresponda a una autoridad sectorial, deberá informar entregando todos los antecedentes pudiendo iniciarlo transcurridos tres meses desde recibida dicha comunicación sin que la autoridad sectorial hubiere iniciado un procedimiento sancionatorio. El plazo podrá ampliarse hasta por 3 meses adicionales, a solicitud de la autoridad sectorial, en caso de que ésta informe a la Agencia del inicio de un proceso de fiscalización que pudiere resultar en un procedimiento sancionatorio.

Informe financiero N°228 de 18 de octubre de 2023

-Se especifica el requerimiento para dar acceso a la Agencia a redes o sistemas informáticos de instituciones que son parte del ámbito de aplicación de la ley en casos de incidentes de impacto significativo cuya gestión lo haga imprescindible. A ello se agrega que en el caso de que el requerido fuese una institución privada, ésta podrá oponerse como lo señala el proyecto de ley. Por el contrario, de no existir oposición, la Agencia podrá acceder a la información objeto del requerimiento.

-En la misma línea, en el escenario que se requiriese una gestión urgente y el requerido se opusiere, la Agencia podrá acceder a redes o sistemas informáticos sin que proceda recurso, siempre que sea autorizado por un Ministro de la Corte de Apelaciones de Santiago, el cual deberá conocer el requerimiento en casos de urgencia, y se especifica el procedimiento.

-Se agregan especificaciones a la norma conjunta que debe dictar la Agencia con una autoridad sectorial cuando esta última emita normativas generales, técnicas e instrucciones necesarias para fortalecer la ciberseguridad en las instituciones de su sector. Estas señalan que la norma conjunta deberá precisar las instituciones supervisadas que quedarán sujetas a las disposiciones dictadas, además de identificar la autoridad competente para ejercer funciones de fiscalización y aplicar sanciones de conformidad con la legislación respectiva.

-Se crea el cargo de subdirector o subdirectora nacional de la Agencia, el cual estará afecto al Sistema de Alta Dirección Pública, y subrogará al Director o Directora Nacional en caso de ausencia o impedimento, y quién además ejercerá de manera exclusiva las funciones de fiscalización y de instruir el inicio de procedimientos sancionatorios y sancionar las infracciones e incumplimientos en que incurran las instituciones obligadas por la presente ley.

Informe financiero N°234 de 25 de octubre de 2023

a) Restringir el diseño e implementación de planes y acciones a los ámbitos de formación ciudadana, capacitación, fortalecimiento, difusión y promoción de la cultura en ciberseguridad.

b) Permitir a la Agencia requerir a los organismos de la Administración del Estado y a las instituciones privadas señaladas en la ley acceso a la información estrictamente necesaria para prevenir la ocurrencia de incidentes de ciberseguridad o para gestionar uno que ya hubiera ocurrido. En la misma línea, cuando la información referida anteriormente pudiera incluir datos personales, no se considerará la dirección IP como tal.

c) El procedimiento para acceder a las redes y sistemas informáticos en casos de incidentes de impacto significativo cuya gestión lo haga imprescindible señalado en esta ley también será aplicable cuando la Agencia requiera el acceso a sistemas informáticos, datos, documentos y demás información que fuere necesaria para el desempeño de sus funciones de supervisión y fiscalización.

INCIDENCIA PRESUPUESTARIA

De conformidad con los informes financieros señalados anteriormente, el proyecto de ley irrogará un mayor gasto fiscal en régimen de M$877.285.

VI.-ACUERDOS ADOPTADOS EN ESTE TRÁMITE

La Comisión recibió previo a la votación de la iniciativa al subsecretario del Interior, señor Manuel Monsalve.

Señaló que el país progresivamente es víctima de ataques cibernéticos, que afectan diversas entidades del Estado. Es por esto que se vuelve esencial contar con organismos rectores y prácticas que prevengan estos ataques.

Precisó que el proyecto de ley marco sobre Ciberseguridad (LMC) fue presentado por el presidente Sebastián Piñera, en cumplimiento de la Política Nacional de Ciberseguridad (PNCS) y forma parte de la agenda de seguridad pública suscrita por el Ejecutivo y el Congreso Nacional. El proyecto establece un modelo de gobernanza de la ciberseguridad basado en la gestión de riesgos y la implementación de estándares de seguridad digital para el sector público, los servicios esenciales y los operadores de importancia vital del sector privado.

El proyecto propone la creación de una Agencia Nacional de Ciberseguridad, como el organismo rector de la ciberseguridad del país, dotada de las funciones y atribuciones necesarias para cumplir su cometido, tales como la gestión de incidentes de ciberseguridad, la coordinación interinstitucional, la función normativa técnica, la función fiscalizadora y, eventualmente, la sancionatoria, entre otras. El proyecto de ley, en segundo trámite constitucional, fue despachado por la Comisión de Seguridad Ciudadana de la Cámara de Diputados, el pasado miércoles 22 de octubre. En su primer trámite constitucional, fue aprobado unánimemente por el Senado en abril de 2023.

Detalló el contenido de los artículos sometidos a la competencia de la Comisión de Hacienda:

Artículo 8, inciso primero, en sus letras a), b) c), d), g), h) e i), que establecen las obligaciones que deberán implementar las organizaciones públicas y privadas que sean consideradas operadores de importancia vital para la ciberseguridad del país.

Artículo 10, inciso primero, que crea la Agencia Nacional de Ciberseguridad como un servicio público funcionalmente descentralizado, con personalidad jurídica y patrimonio propio, de carácter técnico y especializado, que se relaciona con el Presidente de la República a través del ministerio encargado de la seguridad pública.

Artículo 11, letras f) e i), que establecen las atribuciones de crear un Registro Nacional de Incidentes de Ciberseguridad y de diseñar e implementar planes y acciones de formación ciudadana, capacitación, fortalecimiento, difusión y promoción en materia de ciberseguridad, respectivamente.

Artículo 12, que fija la dirección de la Agencia que estará a cargo de un o una Directora Nacional, quien será la jefa superior del servicio y será designada por el sistema de Alta Dirección Pública.

Artículo 13, que crea la figura de Subdirector o Subdirectora de la Agencia, que también será designado por el sistema de Alta Dirección Pública.

Artículo 14, letra e), que entrega al Director o Directora la facultad de ejecutar actos y celebrar contratos.

Artículo 15, que determina el patrimonio de la Agencia.

Artículo 17, incisos cuarto, quinto, sexto, séptimo, octavo y final, que fijan las reglas sobre el personal de la Agencia, a quienes se le aplicarán las disposiciones del Código del Trabajo y las normas pertinentes del Estatuto Administrativo y de la ley sobre Probidad en la Función Pública, entre otras.

Artículo 23, inciso primero, que reconoce legalmente la Red de Conectividad Segura del Estado, que ya provee servicios de interconexión y conectividad a los OAE

Artículo 24, que crea el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática, CSIRT Nacional.

Artículo 29, que crea el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional, CSIRT de la Defensa Nacional.

Artículo 36, que dispone el régimen de sanciones aplicables a quienes infrinjan el deber de reserva que la ley establece respecto de cierta información que mantenga la Agencia.

Artículo 40, incisos primero y segundo, que fija el régimen de sanciones aplicables a quienes incumplan las obligaciones establecidas en la ley, determinando los hechos y las sanciones a aplicar.

Artículo 51, inciso segundo, que dispone el régimen de sanciones aplicables a los miembros del Comité Interministerial sobre Ciberseguridad que infrinjan el

deber de reserva que la ley establece respecto de cierta información que mantenga la Agencia.

Artículo primero transitorio, que delega en el Presidente de la República la facultad de dictar uno o más DFLs, para determinar la entrada en vigencia de la ley y las reglas sobre la dotación de personal de la Agencia y el traspaso de funcionarios desde la Subsecretaría del Interior a la Agencia.

Artículo segundo transitorio, que autoriza al Presidente para nombrar al primer director o directora de la Agencia, que durará un año en su cargo, estableciendo algunas restricciones a ese primer nombramiento.

Artículo cuarto transitorio, determina la regla sobre mayor gasto fiscal que represente la aplicación de la ley durante su primer año presupuestario.

VOTACIÓN

Puestos en votación todos los artículos, **con excepción del artículo segundo transitorio,** respecto del cual el diputado señor Sáez solicitó votación separada, resultaron aprobados por la unanimidad de los doce diputadas y diputados presentes señores Aedo, Barrera, señora Cid, señores Mellado, Naranjo, Ramírez, Romero, Sáez, Sepúlveda, Soto (en reemplazo del diputado Bianchi), Von Mühlenbrock y Yeomans (Presidenta).

Respecto a la votación del inciso segundo del artículo segundo transitorio, el subsecretario Monsalve reconoció que el punto es cuestión es si el actual Coordinador de Ciberseguridad puede o no puede ser nombrado en el cargo de director de la Agencia Nacional de Ciberseguridad. La norma hace que quien haya ocupado el cargo de coordinador en los últimos 3 años no pueda nunca ser director de la Agencia. Consideró que es una norma muy específica y dirigida que no parece sana como precedente. Llamó a la Comisión a rechazar esta disposición.

El texto del artículo segundo transitorio es el siguiente:

“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 sólo efecto en un cargo su dotación máxima de personal, siempre que no se encuentre vigente la respectiva planta de personal. El primer Director de la Agencia Nacional de Ciberseguridad no podrá participar del primer proceso de selección por Alta Dirección Pública para la provisión de su cargo.

Con todo, conforme a este artículo no podrá ser nombrado en el cargo de Director o Directora de la Agencia, quien hubiere ejercido el cargo de Coordinador Nacional

de Ciberseguridad, dependiente del. Ministerio del Interior y Seguridad Pública, los tres años previos a la publicación de esta ley en el Diario Oficial".

La Secretaría explicó que este inciso fue agregado en la comisión técnica mediante la aprobación de una indicación presentada por los diputados señores Cristián Araya y Henry Leal.

El señor Subsecretario del Interior, don Manuel Monsalve, expresó en esa oportunidad que la indicación le pareció perseguir un objetivo personal y discriminatorio, ya que todo funcionario que ingresó a trabajar al Ministerio del Interior y Seguridad Pública nunca se imaginó, ni le informaron, que no podría en un futuro participar para ser parte de un proceso de alta dirección pública.

El diputado Romero, don Agustín preguntó por qué se incorporó esta norma.

El diputado Sáez estimó que una discusión tan sustantiva para el país no puede ser infectada por una *vendetta* personal.

El diputado Von Mühlenbrock consultó de qué se trata esta venganza.

El subsecretario Monsalve señaló que el coordinador actual envuelto en la polémica ha sido cuestionado por una publicación realizada en una red social en la que denostó la institución de Carabineros de Chile. Ha manifestado personal y públicamente sus disculpas con el General Director de Carabineros.

La diputada Cid consideró que esta persona difícilmente podrá tener una buena relación con Carabineros, la que resulta necesaria para el cargo en cuestión.

El diputado Ramírez manifestó que en virtud de la confianza que tienen que tener las instituciones de parte de la ciudadanía es necesario hacerse cargo de las expresiones que se profieren.

El diputado Mellado, don Miguel estimó que difícilmente esta persona ha cambiado de pensamiento, sólo ha moderado su discurso por ocupar hoy una posición de poder. Así las cosas, él no puede asumir este cargo.

El diputado Romero expresó que resulta incomprensible que no exista en el gobierno otra persona que pueda asumir este cargo.

El diputado Aedo indicó que es legítimo cambiar de opinión de un momento a otro de la vida. Llamó a quienes traen consigo la doctrina cristiana a recordar el concepto de la transformación positiva de mente y corazón que es la metanoia.

El diputado Naranjo señaló que existe en la vida un derecho sagrado a la equivocación e instó a sus colegas a no discutir con liviandad esta importante materia. Agregó que lo único relevante es la evaluación profesional que de esta persona se tiene entre quienes están en condiciones de nominarlo al cargo.

El subsecretario Monsalve expresó que la persona en cuestión es un profesional y académico con vasta experiencia en ciberseguridad. En este sentido, la

evaluación del Ejecutivo es positiva, sin perjuicio de reconocer que cometió un error en el pasado por el cual presentó las debidas excusas.

Votación

Puesto en votación el inciso segundo del artículo segundo transitorio, resultó rechazado por no alcanzar el quórum de aprobación. Votaron en contra los diputados Aedo, Barrera, Naranjo, diputada Rojas, diputados Sáez, Sepúlveda, Soto, don Raúl (en reemplazo del diputado Bianchi) y diputada Yeomans (Presidenta). Votaron a favor los diputados Cid, Mellado, Ramírez, Romero y Von Mühlenbrock.

Puesto en votación el inciso primero del artículo segundo transitorio, resultó aprobado por la unanimidad de los trece diputados y diputadas presentes señores Aedo, Barrera, Cid, Mellado, Naranjo, Ramírez, Rojas, Romero, Sáez, Sepúlveda, Soto (en reemplazo del diputado Bianchi), Von Mühlenbrock y Yeomans.

****

Por las razones señaladas y consideraciones que expondrá el Diputado Informante, la Comisión de Hacienda recomienda aprobar las normas sometidas a su consideración, con incidencia en materia financiera o presupuestaria del Estado, en la forma explicada.

******

Tratado y acordado en la sesión ordinaria de miércoles 29 de noviembre del año en curso, con la asistencia presencial de los diputados señores, Eric Aedo Jeldres, Boris Barrera Moreno, Miguel Mellado Suazo, Jaime Naranjo Ortiz, Guillermo Ramírez Diez, Agustín Romero Leiva, Jaime Sáez Quiroz, Alexis Sepúlveda Soto, Gastón Von Mühlenbrock Zamora y diputadas señoras Sofía Cid Versalovic, y señoritas Camila Rojas Valderrama y Gael Yeomans Araya (Presidenta). El diputado Carlos Bianchi Chelech fue reemplazado por el diputado Raúl Soto Mardones.

Sala de la Comisión, a 4 de diciembre de 2023.

MARÍA EUGENIA SILVA FERRER
Abogado Secretaria de la Comisión