INFORME DE LA COMISIÓN DE SEGURIDAD CIUDADANA 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:[1]

La Comisión de Seguridad Ciudadana viene en informar el proyecto de ley referido en el epígrafe, de origen en un mensaje de S.E. el Presidente de la República, **en segundo trámite constitucional y primero reglamentario**, con urgencia calificada de **suma.**[2]

Durante la discusión de este mensaje se contó con la participación y colaboración de las siguientes personas, señoras y señores: El Subsecretario del Interior, Manuel Monsalve; el Coordinador Nacional de Ciberseguridad del Ministerio del Interior, Daniel Álvarez, quien concurrió junto a las asesoras, Michelle Bordachar, Lesly Covarrubias y Patricia Araya; la Comisionada de la Comisión para el Mercado Financiero, Bernardita Piedrabuena, quien concurrió junto al Director General de Regulación Prudencial, Luis Figueroa; el Director Ejecutivo de la ONG Derechos Digitales, Juan Carlos Lara, quien concurrió junto a la Analista de Políticas Públicas, Isidora Ruggeroni; el ingeniero Jorge Atton; el abogado señor Felipe Harboe; la abogada especialista en protección de datos personales y nuevas tecnologías, Romina Garrido; el profesor de la Universidad del Desarrollo, Juan Pablo González; la abogada especialista, Paulina Silva; el Presidente de la mesa legal de la Asociación Chilena de Empresas Tecnologías de Información A. G., ACTI, Claudio Magliona; el profesor del Departamento de Ciencias de la Computación de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile, Alejandro Hevia; el Presidente Ejecutivo de Chile Telcos, Alfie Ulloa; Puppy Rojas; el Coordinador de Asuntos Públicos de la Cámara Chilena Norteamericana de Comercio, AMCHAM, Marcelo Guajardo, quien asistió junto a los Secretarios Ejecutivos de la Mesa de Regulaciones Digitales, Carolina Cabrera y Felipe Álvarez; el Director de la Alianza Chilena de Ciberseguridad, Guillermo Carey; el Presidente de la Cámara Nacional de Comercio, José Pakomio; el Presidente de la Comisión de Economía y Productividad Digital, Cristóbal Aninat y el abogado y asesor legislativo, Juan Ignacio Gómez.

I. CONSTANCIAS REGLAMENTARIAS PREVIAS.

1.- IDEAS MATRICES O FUNDAMENTALES.

La idea matriz o fundamental del proyecto.

Establecer la institucionalidad indispensable con la finalidad de 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.

2.- NORMAS DE CARÁCTER ORGÁNICO CONSTITUCIONAL Y DE QUÓRUM CALIFICADO.

Compartiendo la calificación que en su oportunidad hizo el Senado de las normas que requieren ser aprobadas con quórum especial, la Comisión determinó la siguiente calificación de las disposiciones aprobadas en este segundo trámite constitucional:

---

[1]Participaron en la elaboración de este informe el abogado secretario de comisiones, don Álvaro Halabi Diuana, la abogada ayudante, doña Carolina Salas Prüsing y la secretaria ejecutiva, doña Luz Barrientos Rivadeneira.

[2] S.E. el Presidente de la República hizo presente la urgencia a este proyecto el 22 de noviembre de 2023, por lo que el plazo de su vencimiento legal es el 7 de diciembre de 2023.

A) Tienen el carácter de ley orgánica constitucional, debiendo aprobarse conforme al quórum establecido en el inciso segundo del artículo 66 de la Constitución Política e la República:

1) De conformidad con lo prescrito en el artículo 38 de la Carta Fundamental:

Los artículos 1° inciso segundo; 10; 11 letras a), b), c), d), e), i), m), n), ñ), v) y x); 12; 20 inciso tercero; 24; 29; 30; 47; 48; 49; 50; 53 y 54, permanentes, y el artículo segundo transitorio.

2) Según el artículo 77 de la Constitución Política de la República:

Artículos 11 incisos segundo y cuarto de la letra k); 37; 41; 42; 44 y 46.

B) Normas de quórum calificado, de conformidad al artículo 8°, inciso segundo de la Carta Fundamental:

Artículos 19; 21 inciso primero; 33; 34; 35 y 51.

3.- NORMAS QUE REQUIEREN TRÁMITE DE HACIENDA.

Las siguientes disposiciones aprobadas por esta Comisión deben ser conocidas por la Comisión de Hacienda, por incidir en materias presupuestarias y financieras:

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.

El Ejecutivo adjuntó los siguientes informes financieros: N° 043, de 10 de marzo de 2022, IF complementario N° 204, de 11 de noviembre de 2022, IF complementario 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.

4.- APROBACIÓN DEL PROYECTO.

En sesión N° 57, de fecha 14 de junio de 2023, el proyecto fue **aprobado** en general por **unanimidad** de votos.

Votan a favor las y los diputados señores Jorge Alessandri (presidente), Cristián Araya, José Miguel Castro, Maite Orsini, Alejandra Placencia, Gloria Naveillán y Diego Schalper. No hubo votos en contra. No hubo abstenciones. **(7x0x0)**

5.- DIPUTADO INFORMANTE.

Se designó como Diputado Informante al señor **JOSÉ MIGUEL CASTRO BASCUÑÁN**.

II. ANTECEDENTES.

A título de antecedentes, cabe resaltar que S.E. el Presidente de la República, por conducto de su mensaje, enfatiza que las tecnologías emergentes de la sociedad digital han generado un cambio cultural amplio, el que se ha acelerado y ahondado en el contexto de diversas medidas sanitarias -como el confinamiento-, producto de la pandemia del COVID-19. Así, previene, se ha alterado la forma de ser y estar en el mundo.

En esa situación asevera que ha sido menester que también el Estado profundice su transformación digital, la cual, sostiene se inició con la publicación de la ley Nº21.180, sobre transformación digital del Estado, publicada el 11 de noviembre de 2019 y ha continuado con el decreto supremo Nº4, de 09 de noviembre de 2020, del Ministerio Secretaría General de la Presidencia, el cual contiene el reglamento que regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos, en las materias que indica, según lo dispuesto en la referida ley. De la misma manera, con el decreto con fuerza de ley N° 1, de 2020, del Ministerio Secretaría General de la Presidencia, establece normas de aplicación del artículo 1° de la ley N° 21.180, respecto de los procedimientos administrativos regulados en leyes especiales que se expresan a través de medios electrónicos y determina la gradualidad para la aplicación de la misma ley, a los órganos de la Administración del Estado que indica y las materias que les resulten aplicables.

Esta modernización, precisa, es una tarea continua y permanente, enmarcada dentro del principio rector consagrado en el artículo 1° de la Constitución Política de la República, que reconoce que el Estado está al servicio de las personas. Se enfatiza que se ha avanzado en robustecer el acceso a diversos servicios públicos mediante canales digitales, además se hace necesario asegurar que dichas prestaciones sean entregadas con todos los resguardos y estándares de seguridad necesarios.

Así, destaca, se transita decididamente hacia un Estado que sea más integrador, ágil, innovador y más efectivo para cumplir su función de servir al bien común, para mejorar la calidad de vida de las personas, modernizar la función pública y potenciar el desarrollo económico, productivo, industrial y de servicios, fortaleciendo la integridad, disponibilidad de la información en el ciberespacio y la confidencialidad y seguridad en el tratamiento de los datos de los ciudadanos.

Acciones concretas de lo antes referido se encuentran en diversas plataformas que proveen acceso a trámites que tradicionalmente debían realizarse de forma presencial, como la Comisaría Virtual, o las solicitudes de beneficios estatales por medio de la Clave Única, incorporándose próximamente los procedimientos administrativos y la gestión documental electrónica.

Observa que esta evolución sociocultural implica enfrentar desafíos en distintos ámbitos, en el área de la tecnología y aquellos referidos a habilidades relacionales y al analfabetismo digital. A su vez, los desafíos en materia de ciberseguridad requieren una convergencia, coordinación y articulación público-privada, para la gestión de alertas preventivas y de incidentes de ciberseguridad.

Acota que, para el adecuado funcionamiento de la ciberseguridad en el país, se deben gestionar los riesgos e implementar los más exigentes estándares que otorguen confianza y seguridad, en las instituciones públicas como privadas. Para esto, se requiere planificación, implementación, seguimiento y evaluación constante en el desarrollo de la ciberseguridad, con un marco completamente integrado que considere una nueva visión de lo multisectorial y transectorial, enfatizando el trabajo conjunto de los sectores público y privado, para beneficio mutuo y general.

Es necesario dar prioridad a la colaboración y la coordinación, permitiendo un trabajo conjunto con todos los actores, tanto locales como globales, valorando el importante rol de la ciencia, la tecnología y la investigación en la ciberseguridad.

El vertiginoso desarrollo de la sociedad digital conlleva un mayor riesgo de vulnerabilidad en todas las estructuras digitales de la sociedad, pero especialmente en aquellos sectores estratégicos donde existe infraestructura de la información que resulta crítica, la regulación sobre ciberseguridad resulta un elemento lógico y necesario.

Por lo referido se sostiene que esta iniciativa permitirá establecer el marco regulatorio necesario para el desarrollo robusto de la ciberseguridad, tanto en su dimensión operativa como regulatoria.

Luego, al fundamentar la pertinencia del proyecto, el Ejecutivo establece una serie de lineamientos que se deben tener presentes al momento de abordar esta materia, a saber:

1.- La relevancia de la ciberseguridad.

Precisa que la ciberseguridad es un tema recurrente en la discusión pública, pues en una sociedad que ha comenzado a transitar desde los soportes físicos hacia la infraestructura de la información, el permanente riesgo de incidentes de ciberseguridad y ciberataques comienza a formar parte de los elementos que deben considerarse. En este sentido, la gestión del riesgo y el control de la vulnerabilidad, son elementos de suyo relevantes.

Así la ciberseguridad es clave en todo el proceso de adaptabilidad a la sociedad digital, para la aplicación y desarrollo de tecnologías como la inteligencia artificial, en los diversos procesos socio-relacionales, en la generación de servicios y los procesos productivos. Sin embargo, toda esa potencialidad se puede transformar en riesgo, si no se adoptan los procesos y estándares de una cultura de ciberseguridad, con enfoque colaborativo y sistémico.

Señala que el Gobierno del Presidente Sebastián Piñera asumió el compromiso de abordar esta temática en el horizonte de su mandato, en su programa de gobierno, en materia de ciencia, innovación y emprendimiento para embarcarnos en la revolución tecnológica, y estableció dentro de sus objetivos la creación de condiciones para que Chile pueda insertarse exitosamente y de manera protagónica en la cuarta revolución industrial. Para ello se propuso adaptar las regulaciones a los desafíos que impone la revolución digital, considerando el desarrollo de políticas de ciberseguridad. De esta forma, con el presente proyecto de ley, se procura justamente llevar adelante esas políticas, y al mismo tiempo, se da cumplimiento a las medidas que dispone la Política Nacional de Ciberseguridad.

2. La relevancia de la institucionalidad en materia de ciberseguridad.

Señala que Chile necesita con urgencia una institucionalidad en ciberseguridad, para coordinar esfuerzos que permitan enfrentar los nuevos desafíos de seguridad pública, dado por el uso masivo y extensivo de las tecnologías. Este es un problema de creciente importancia que se mantendrá y agudizará en el futuro próximo, atendido el vertiginoso despliegue de infraestructura digital en el ámbito público y privado.

Aclara que en el país se requiere un órgano encargado de la seguridad en el ciberespacio, que proteja los bienes y activos de la sociedad digital. En los sectores productivos del mundo privado se concentra una gran cantidad de iniciativas digitales y virtuales, que se constituyen en las nuevas infraestructuras críticas de la información de la sociedad digital.

En ese escenario Chile necesita una institucionalidad pública que se coordine con el sector privado de manera permanente, para garantizar la seguridad en el ciberespacio, que ayude a prevenir los delitos informáticos y proteja la infraestructura crítica de la información.

Adicionalmente, esta institucionalidad necesita una gobernanza clara y una orgánica definida en sus roles, con amplias competencias, tecnológicamente robusta, confiable para las instituciones públicas y privadas, de interacción nacional y global, altamente profesional, eficiente en su gestión y experimentada.

Finalmente expone que el propósito de este proyecto es establecer la institucionalidad necesaria para robustecer la ciberseguridad, ampliar y fortalecer el trabajo preventivo, la formación de una cultura pública en materia de seguridad digital, enfrentar las contingencias en el sector público y privado, y resguardar la seguridad de las personas en el ciberespacio.

III. RESUMEN DEL CONTENIDO DEL PROYECTO APROBADO POR EL SENADO.

Conforme lo dispone el número 2° del artículo 304 del reglamento, el texto aprobado por el Senado pretende, en suma, mediante la creación de un nuevo texto jurídico y de diversas modificaciones legales consagrar la institucionalidad indispensable para robustecer la ciberseguridad. Para cumplir esa finalidad se hace nacer a la vida del derecho una nueva normativa para sustentarla y para complementar dicha legislación se modifican diversos textos legales

Dicha iniciativa en el Senado tuvo una exhaustiva tramitación, debido a que fue informada primeramente por la Comisión de Defensa Nacional, la que lo aprobó en general; luego fue estudiada por la Comisión de Seguridad Pública, para que acto seguido de haber sido aprobada en general por la Sala del Senado, la informara las Comisiones Unidas de Defensa Nacional y Seguridad Pública, quienes la aprobaron en particular, para finalmente ser informada por la Comisión de Hacienda, respecto de los artículos de su competencia.

Cabe consignar que el proyecto consta de cuarenta y ocho artículos permanentes, que contiene diez títulos, como asimismo ocho artículos transitorios.

El Título I de las Disposiciones generales, que contempla el artículo 1º que se refiere al objeto de esta ley, el artículo 2º aborda las definiciones y el artículo 3º trata de los principios rectores.

El Título II de las Obligaciones de ciberseguridad, trata las siguientes disposiciones: el artículo 4º sobre la determinación de los servicios esenciales e identificación de los operadores de importancia vital; el artículo 5º se refiere a los deberes generales; el artículo 6° aborda los deberes específicos y el artículo 7º señala el deber de reportar.

El Título III de la Agencia Nacional de Ciberseguridad se refiere a las siguientes normas: el artículo 8º crea el Agencia Nacional de Ciberseguridad como un servicio público, 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; y los artículos 9º al artículo 14 abordan la dirección de esta Agencia; las atribuciones, el patrimonio, nombramiento de autoridades y personal de la citada Agencia. A su turno, el artículo 15 informa de las prohibiciones e inhabilidades; el artículo 16 crea el Consejo Multisectorial sobre Ciberseguridad; el artículo 17 trata del funcionamiento del Consejo; el artículo 18 contiene

las causales de cesación; el artículo 19 crea la Red de Conectividad Segura del Estado y el artículo 20 el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática.

El Título IV de las otras instituciones intervinientes, contempla el artículo 21 que consagra que las autoridades sectoriales deberán constituir Equipos de Respuesta a Incidentes de Seguridad Informática Sectoriales (CSIRT sectoriales)¸ el artículo 22 trata de las facultades especiales de las autoridades sectoriales¸ el artículo 23 se refiere a los Incidentes de ciberseguridad de efecto significativo y el artículo 24 aborda los Centros de Certificación Acreditados como los únicos organismos autorizados para certificar el cumplimiento de los estándares de ciberseguridad

El Título V del Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional está compuesto del artículo 25, por el que crea el Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional. del artículo 26 establece sus funciones, del artículo 27 señala que deben establecerse los Equipos de Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional y del artículo 28, sobre el deber de reporte al CSIRT.

El Título VI de la reserva de información en el sector público en materia de ciberseguridad, contempla el artículo la reserva de información y de circulación restringida, el artículo 30, referido a la extensión de la obligación de reserva, el artículo 31. que consagra el deber de reserva de la Agencia y el artículo 32, que estipula sanciones por infracción a las obligaciones dispuestas en este Título,

El Título VII de las infracciones y sanciones, contiene el artículo 33 aborda las sanciones a las infracciones de esta ley cometidas por instituciones privadas, el artículo 34 que contiene el procedimiento administrativo por infracción de ley, el artículo 35 trata del procedimiento de reclamación judicial, el artículo 36 se refiere a la responsabilidad administrativa del jefe superior del organismo público, el artículo 37 apunta a la responsabilidad del funcionario o funcionaria infractor y el artículo 38 prescribe una agravante especial. Si por la perpetración de un delito resultare afectada gravemente la continuidad operativa de un operador de importancia vital.

El Título VIII del Comité Interministerial de Ciberseguridad, contiene el artículo 39 que crea el Comité Interministerial sobre Ciberseguridad, que asesorará al Presidente de la República en materias de ciberseguridad relevantes para el funcionamiento del país, el artículo 40 establece quiénes serán los miembros permanentes que integrarán el Comité, el artículo señala que el Comité contará con una Secretaría Ejecutiva radicada en la Agencia, el artículo 42 establece que 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 el artículo 43 consagra un reglamento, que fijará las normas de funcionamiento del Comité.

El Título IX aborda los órganos autónomos constitucionales, que contempla el artículo el artículo 45 precisa regímenes especiales. para estos órganos, y señala que les 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.

El Título X de las modificaciones a otros cuerpos legales, a través de los artículos 45 a 48, con el objeto de armonizar las materias tratadas en esta ley, con la ley N° 20.424, Estatuto Orgánico del Ministerio de Defensa Nacional, 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; la ley N° 19.974, sobre el sistema de inteligencia del Estado y crea la Agencia Nacional de Inteligencia y la

ley N° 7.401, que reprime las actividades que vayan contra la seguridad exterior del Estado.

Los artículos primero al octavo, todos transitorios, abordan, entre otros aspectos, la entrada en vigencia de esta nueva ley, del personal, de la autorización al Presidente de la República a nombrar, a partir de la publicación de la esta ley, al primer Director o Directora de la Agencia Nacional de Ciberseguridad, la autorización al Presidente de la República, para conformar el primer presupuesto de la Agencia Nacional de Ciberseguridad, la dictación dentro del plazo de ciento ochenta días posteriores a la publicación de la ley de los reglamentos señalados en esta ley por el Ministerio del Interior y Seguridad Pública, la renovación parcial de los miembros del Consejo Multisectorial sobre Ciberseguridad, se aborda el financiamiento del mayor gasto fiscal que represente la aplicación de esta ley durante su primer año presupuestario de vigencia y señala como se calificarán los servicios esenciales mientras no se dicten los respectivos decretos

Cabe destacar que en el transcurso de este proyecto hubo temas centrales y básicos que fueron discutidos latamente en el Senado, como la debida armonía que debe guardar este proyecto de ley con la ley N° 21.459 sobre delitos informáticos y el proyecto de ley sobre datos personales que se encuentra en discusión en tercer trámite constitucional, boletines N°11.144-07 y 11.092-07, refundidos; la creación de una institucionalidad pública a cargo de la ciberseguridad, con funciones y atribuciones tanto respecto al sector público como al sector privado; la rigidez del concepto de infraestructura crítica, y ciertos cuestionamientos a la definición de servicios esenciales; el carácter supletorio de la presente iniciativa de ley en cuanto a sus facultades normativas y principios, y específicamente en lo que refiere a la Agencia Nacional de Ciberseguridad y la intención por parte del Ejecutivo de simplificar el proyecto de ley, especialmente en cuanto a su estructura orgánica, con el propósito de que la Agencia Nacional de Ciberseguridad sea una institución rectora en esta materia tanto para el sector público como privado.

Se consigna que entre los hechos más relevantes que se dieron en la tramitación de esta iniciativa legal en el Senado, referidos principalmente a las enmiendas introducidas al texto original por el Senado, están los siguientes:

1.- Fue aprobada en general por el Senado, en octubre de 2022, por unanimidad. En dicha ocasión se determinó que fuera informada, en particular, por las Comisiones de Defensa Nacional y de Seguridad Pública, unidas.

2.- Las instancias legislativas referidas dieron inicio a su cometido el 29 de noviembre del mismo año, recibiendo en audiencia a la Ministra del Interior y Seguridad Pública, señora Carolina Tohá, y al Coordinador Nacional de Ciberseguridad, señor Daniel Álvarez, quienes anunciaron y explicaron los cambios propuestos por el Ejecutivo al proyecto de ley despachado por la Sala de esta Corporación, mediante las correspondientes indicaciones.

3.- Las Comisiones unidas dedicaron once sesiones al examen de las 199 indicaciones formuladas al texto aprobado en general.

4.- Se precisa que, para facilitar la tramitación de esta iniciativa de ley, se conformó una mesa de trabajo prelegislativo -constituida por asesores de integrantes de las Comisiones unidas y del Ejecutivo-, la que permitió alcanzar amplio consenso en las modificaciones incorporadas. En efecto, casi la totalidad de las indicaciones fueron aprobadas por unanimidad.

5.-. En lo que a las enmiendas atañe, el proyecto aprobado en particular pone en el centro y releva la protección de los derechos de las personas. Así lo señala expresamente el nuevo inciso final del artículo 1.

6.- Otra innovación radica en la sustitución de la expresión “infraestructura crítica” por “operadores de importancia vital y servicios esenciales” La razón de tal decisión descansa en que, actualmente, aquel término ha quedado circunscrito a las de orden físico, mientras

que para los demás se recurre a la locución “servicios esenciales”. La Agencia Nacional de Ciberseguridad, siguiendo el procedimiento previsto en el artículo 4, determinará aquellos que sean considerados como tales y, dentro de estos, identificará a los operadores de importancia vital de conformidad a los criterios establecidos en la ley.

7.- Otro aspecto modificado dice relación con el ámbito de aplicación. El texto sugerido a la Sala obligará a todos los organismos del Estado y a las instituciones privadas a dar cumplimiento a ciertos deberes generales; a saber, a adoptar medidas necesarias para prevenir, reportar y resolver incidentes de ciberseguridad; a gestionar los riesgos asociados, y a contener y mitigar sus impactos. Para ello, la Agencia establecerá protocolos y estándares diferenciados según el tipo de organización de que se trate, y tendrá especial consideración con las características y necesidades de las pequeñas y medianas empresas.

Asimismo, todas las entidades, sean públicas o privadas, con excepción de aquellas eximidas por la Agencia Nacional de Ciberseguridad, reportarán, en un plazo de tres horas, al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos. Asimismo, informarán su plan de acción tan pronto como lo hubieren adoptado. Adicionalmente, se les prohíbe expresamente realizar pagos de cualquier tipo por rescate ante ataques de secuestro de datos, de equipos o de dispositivos.

8.- A su vez, los organismos del Estado con competencias específicas sobre servicios esenciales, incluidas las empresas públicas creadas por ley y las empresas del Estado y sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio, y las instituciones privadas calificadas como operadores de importancia vital tendrán mayores exigencias, debiendo observar los deberes específicos del artículo 6.

9.- La Agencia Nacional de Ciberseguridad regulará, fiscalizará y sancionará las acciones de seguridad informática de los organismos de la Administración del Estado y de las instituciones privadas.

10.- Las entidades autónomas constitucionales, en tanto, por medio de sus órganos internos, tendrán la obligación de adoptar las medidas especiales de ciberseguridad contempladas en el artículo 6, dictando para ello las políticas, normas e instrucciones necesarias para dar cumplimiento a los principios y obligaciones de este texto legal, pudiendo requerir la asistencia de la Agencia Nacional de Ciberseguridad. Si bien estos órganos no estarán sujetos a la fiscalización, regulación ni supervigilancia de esta última, deberán acordar mecanismos de coordinación, cooperación, reporte de incidentes e intercambio de información sobre seguridad informática, incluyendo la conformación de equipos de respuestas.

11.- Otra innovación radica en la sustitución del Consejo Técnico de la Agencia Nacional de Ciberseguridad, aprobado en general, cuyos miembros eran remunerados, por el Consejo Multisectorial de Ciberseguridad, cuyos integrantes se desempeñarán ad honorem y tendrán la misión de asesorar a la Agencia en diversas materias relacionadas con la seguridad informática. En este punto, cabe hacer presente que el texto propuesto por las Comisiones de Defensa Nacional y de Seguridad Pública unidas no incluye una disposición que precise sus funciones. La razón de tal decisión se encuentra en la conveniencia de contar con un espacio de diálogo público privado que, de manera permanente y amplia, apoye al Jefe de Estado en este tipo de asuntos.

12.- En relación con el texto aprobado por la Sala del Senado, otra novedad se aprecia en el régimen aplicable al personal de la Agencia. En efecto, recogiendo las observaciones realizadas durante la discusión en general; las peculiaridades de este organismo; las materias abordadas, y la necesidad de contratar en ciertos casos a expertos sin título profesional, se concluyó que la mejor opción es que quienes se desempeñen en la entidad encargada de la seguridad informática queden sujetos a las disposiciones del Código del Trabajo, con ciertas modificaciones. Entre ellas se encuentra la aplicación de las normas de probidad contenidas en la ley N° 20.880; las disposiciones del Título III de la ley orgánica

constitucional de Bases Generales de la Administración del Estado, y los artículos 61, 62, 63, 64, 90 y 90 A, según corresponda, del Estatuto Administrativo.

Además, se precisa que dichos trabajadores estarán 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.

13.- Por otro lado, el Director de la Agencia, no obstante 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 Estatuto Administrativo.

14.- También es posible observar un cambio, respecto del proyecto de ley aprobado en general, en la creación de la red de conectividad segura del Estado, la que proveerá servicios de interconexión y conectividad a los organismos de la Administración del Estado.
15.- En lo que atañe a las enmiendas introducidas al precepto que regula los CSIRT Sectoriales, el artículo 21 propuesto dispone que las autoridades sectoriales deberán constituir Equipos de Respuesta a Incidentes de Seguridad Informática, a fin de contribuir al desarrollo de capacidades, confianza y seguridad de las redes y sistemas informáticos y proporcionar asistencia para la gestión de incidentes en sus respectivas áreas. En el ejercicio de sus funciones, deberán dar cumplimiento a los protocolos, estándares técnicos e instrucciones que la Agencia pudiera dictar, con el objeto de lograr un nivel común de ciberseguridad y respuestas coordinadas. En el caso del CSIRT sujeto a la fiscalización de la Comisión para el Mercado Financiero, sin embargo, bastará con dar cumplimiento a los protocolos y estándares que la Agencia comunique ante la ocurrencia de incidentes que pudieran tener un efecto sistémico en el país. Con todo, no se afectarán las facultades fiscalizadoras, las normativas ni las de supervisión del citado servicio público.

16.- Además, se faculta a las autoridades sectoriales a dictar normas de carácter general y técnicas que consideren necesarias para la ciberseguridad de las instituciones de su sector. Ellas deberán ser sometidas a la aprobación previa de la Agencia. Asimismo, deberán dictar las instrucciones, circulares y órdenes necesarias para la implementación de los protocolos y estándares técnicos establecidos por el organismo encargado de la seguridad informática.

17.- En el ejercicio de estas facultades normativas, deberán considerar, a lo menos, los protocolos y estándares técnicos y las instrucciones generales y particulares dictados por la Agencia Nacional de Ciberseguridad.

18.- Tratándose de sus instituciones fiscalizadas, la Comisión para el Mercado Financiero podrá dictar las disposiciones de carácter general y técnico sobre ciberseguridad, sin necesidad de solicitar la aprobación de la Agencia, siempre y cuando tengan un alcance distinto a las elaboradas por ella. De lo contrario, deberá informar previamente a la Agencia, por razones de coordinación.

19.- Otro cambio radica en la inclusión de un título referido al Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional. En él se crea el CSIRT de la Defensa Nacional, se señalan sus funciones, se faculta la creación de CSIRT Institucionales de la Defensa Nacional y se obliga a reportar los ciberataques e incidentes de ciberseguridad de efectos significativos al CSIRT de dicha área. Este, a su vez, los reportará a la Agencia Nacional de Ciberseguridad, siempre que no pongan en riesgo la seguridad y la defensa nacional.

20.- Supone también una mejora el perfeccionamiento del procedimiento administrativo aplicable en caso de infringirse este futuro texto normativo. Así, se introduce una norma que regula el procedimiento de reclamación judicial, un precepto que alude a la responsabilidad administrativa del jefe superior del órgano público y otra relativa a la del funcionario infractor.

21.- Otra relevante innovación se aprecia en el artículo 46 del texto sugerido, el que enmienda el artículo 2° de la ley N° 21.459, que establece normas sobre delitos informáticos, permitiendo brindar resguardo legal a las labores de investigación en seguridad

informática, vale decir al hacking ético, lo que es significativamente beneficioso para la sociedad.

22.- Finalmente, es necesario poner de relieve que el texto propuesto por las Comisiones unidas recoge los últimos estándares en materia de ciberseguridad. Entre ellos, los de la Directiva NIS2, de la Unión Europea; las prácticas incorporadas recientemente en Israel y Bélgica, y las reformas introducidas en la legislación dominicana.

IV. SÍNTESIS DE LA DISCUSIÓN GENERAL EN LA COMISIÓN Y ACUERDOS ADOPTADOS.

A.- DISCUCIÓN GENERAL.

El Coordinador Nacional de Ciberseguridad del Ministerio del Interior, señor Daniel Álvarez, con ayuda de una presentación en power pinta, expuso que la iniciativa fue presentada por el entonces Presidente de la República, don Sebastián Piñera y forma parte de la Política Nacional de Ciberseguridad 2018-2022, el que fue aprobado de manera unánime por la sala del Senado y por las Comisiones Unidas de Defensa Nacional y Seguridad Pública, y por la Comisión de Hacienda de esa corporación.

Manifestó que el proyecto de ley es de consenso, forma parte de la agenda de seguridad pública y del acuerdo suscrito entre el Gobierno y el Congreso Nacional en esta materia. 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. Además, indicó que crea la Agencia Nacional de Ciberseguridad (ANCI) con facultades regulatorias, fiscalizadoras y sancionatorias, y crea el Consejo Multisectorial sobre Ciberseguridad, como asimismo 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.

Detalló que la Agencia Nacional de Ciberseguridad (ANCI), tendrá la función de 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. Además, se relacionará con el Presidente de la República a través del Ministerio del Interior y Seguridad Pública.

Agregó que el proyecto de ley, 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. Y 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.

Por último, expresó que se perfeccionó las normas relativas a la obligación de reportar vulnerabilidades e incidentes de ciberseguridad, tanto en el sector público como privado, incluyendo la protección del hacking ético. Se establecen obligaciones específicas al Estado y al sector privado en materia de ciberseguridad, incorporando la dimensión de la educación, capacitación, buenas prácticas e higiene digital, entre muchos otros temas. Y con todo buscan generar un ecosistema normativo en materia de ciberseguridad y sectores regulados, manteniendo las facultades normativas sectoriales, bajo coordinación con la Agencia Nacional de Ciberseguridad.

El **Director Ejecutivo de la ONG Derechos Digitales, señor Juan Carlos Lara,** con apoyo de una minuta señaló que el proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información 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 nuevos órganos administrativos, consultivos y asesores, como también crea y facilita la creación de equipos de respuesta a incidentes o CSIRT.

Agregó que este proyecto de ley representa un avance significativo en la capacidad operativa del Estado en materia de seguridad digital, integrando expresamente al sector privado. Es parte importante de una serie de iniciativas legislativas y de política pública en la materia, incluyendo la Política Nacional de Ciberseguridad 2023-2028, la nueva ley Nº21.459 sobre delitos informáticos, y el proyecto que reforma la Ley de Protección de Datos Personales que fuera recientemente aprobado en esta Cámara.

Consideró relevante y positiva la incorporación de los principios, establecidos en el artículo 3, como aspecto clave del carácter de ley marco para guiar un conjunto de acciones regulatorias y fiscalizadoras. Celebramos la inclusión de un principio de igualdad y no discriminación; a la vez, consideramos necesario expandir el principio de cooperación con la autoridad a uno de colaboración, que en reconocimiento del carácter multisectorial del ecosistema de ciberseguridad además estimule la participación ciudadana con características de diversidad e inclusión; también ponemos bajo cuestionamiento el principio de cifrado. Si bien el cifrado de la información, tanto almacenada como en tránsito, es promovido activamente por Derechos Digitales como medida de privacidad y seguridad, considera que el principio subyacente es el integrado en la definición, como derecho a adoptar las medidas de seguridad que se estimaren necesarias.

Expresó que en el ámbito institucional y de gobernanza, un punto central es la creación de la Agencia Nacional de Ciberseguridad, destacando también la creación de un Consejo Multisectorial de Ciberseguridad de carácter consultivo y un Comité Interministerial sobre Ciberseguridad para asesorar a la Presidencia de la República. Asimismo, valoró la flexibilidad para la decisión sobre la creación de nuevos CSIRT de carácter sectorial, en atención a las cambiantes necesidades sectoriales y a los costos involucrados para cada nueva entidad.

Manifestó que, desde el punto de vista de los sujetos regulados, el proyecto pone bajo responsabilidad de la nueva Agencia la determinación de los servicios esenciales, como también iniciar el proceso de identificación dentro de estos servicios a los operadores de importancia vital, de conformidad al procedimiento y los criterios establecidos en el proyecto, que contemplan la intervención de distintos órganos y una decisión mediante decreto previa decisión del Comité Interministerial. Esta forma de determinación es un aspecto positivo del proyecto, facilitando la transparencia. Estas entidades están sujetas a deberes específicos, entre los cuales se encuentra la obligación de implementar sistemas de gestión de seguridad de la información, elaborar y mantener planes de continuidad operacional y designar un delegado de ciberseguridad, entre otros deberes específicos.

Complementó que, el Artículo 5º fija obligaciones generales para los organismos del Estado y para las instituciones privadas, lo que, si bien parece positivo en materia de seguridad, representa una fórmula muy amplia donde el cumplimiento de estos deberes puede variar dependiendo del tamaño de las empresas y donde el rol de la Agencia es clave para guiar su operación.

Además, indicó que el proyecto aborda el fenómeno de la ciberseguridad de manera integral, incluyendo normas relativas a la educación. La Agencia posee atribuciones de diseñar e implementar, en coordinación con el Ministerio de Educación, planes y acciones de educación, formación ciudadana, investigación, innovación, entrenamiento, fomento y difusión, para promover el desarrollo nacional de una cultura de

ciberseguridad. Esto da operatividad mayor a uno de los aspectos que más han preocupado a Derechos Digitales desde la publicación de la Política Nacional de Ciberseguridad 2017-2022.

Concluyó señalando que, si bien consideran que hay aspectos de la redacción que pueden ser mejorados, el proyecto es un avance significativo en materia de gobernanza e institucionalidad en ciberseguridad.

La **abogada especialista, señora Paulina Silva,** con apoyo de una presentación en power point expuso que desde alcances generales el proyecto de ley es necesario y generalmente adecuado.

Señaló que, desde una mirada más específica, por una parte, las facultades que establece el proyecto de ley para la Agencia, son muy amplias, según lo reza particularmente la letra j) del artículo 9: “atribuciones de la Agencia Nacional 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”. El CJEU declaró inválido el Privacy Shield entre Europa y EE.UU. pues los programas de vigilancia del gobierno norteamericano carecían de reglas claras y precisas en el acceso por parte del gobierno a los datos personales en manos de privados.

Asimismo, indicó que no identifican el interés público en requerir los niveles de notificación y de recarga innecesaria al CSIRT Nacional, con el deber de reportar brechas de todas las instituciones del país, sin hacer si quiera la distinción de relevancia si es o no un servicio esencial u operador de importancia vital.

Manifestó que puede generarse un problema de coordinación intersectorial y contiendas de competencia según la redacción del inciso tercero del artículo 21 del proyecto de ley. Es importante no desaprovechar capacidades técnicas de organismos sectoriales, debiendo primar principio de especialidad.

Y por último, añadió que, desde un punto de vista de la estructura de las regulaciones de ciberseguridad, el proyecto de ley busca desincentivar al delincuente promoviendo la protección tanto de la infraestructura crítica, como de los organismos del Estado y los datos personales. Desde la institucionalidad, se establece de manera correcta la supervisión y control, la promoción de la coordinación y la estandarización de las medidas de seguridad y el procedimiento de reporte.

El **Presidente de la mesa legal de la Asociación Chilena de Empresas Tecnologías de Información A. G., ACTI, señor Claudio Magliona,** con ayuda de una presentación en power point señaló que como gremio, apoyan la necesidad de crear un marco regulatorio robusto que aborde la ciberseguridad en nuestro país, pero como toda iniciativa legal creen debe perfeccionarse para dar certeza jurídica a los regulados en el ecosistema digital y en ese sentido consideran positivo revisar algunas preocupaciones.

Detalló que entre las inquietudes más relevantes están las siguientes:

1.- Es muy extenso el ámbito de aplicación de la Ley General: no existen antecedentes similares en derecho comparado, NIS 1 y NIS 2 establecen alcance a entidades u operadores de carácter esencial/importante, aplicando distintas reglas. Consideran que una pyme, almacén, panadería no debería tener obligación de comunicar vulnerabilidades ni en 3 horas ni en el tiempo que finalmente se decida, no comunicar incidentes se sanciona como infracción grave, desde 1.001 UTM. Entienden que la agencia puede eximir de estas obligaciones o dar tratamiento a ciertas entidades, pero esta es una ley que se debe aplicar a servicios esencial y operadores vitales, es importante evitar discrecionalidades y tener certezas jurídicas.

2.- No olvidarse de la importancia del principio de igualdad ante la ley, ya que se excluyen de su aplicación a empresas públicas, estatales o con participación.

3.- Se requiere revisión general del proyecto, ya que contempla definiciones en catálogo que no se aplican nuevamente en todo el cuerpo: como activo informático; no repudio; interagencialidad, entre otras.

4.- Es relevante establecer el proceso de determinación de los Servicios Esenciales, hay que detallarlos, principalmente por un tema de seguridad jurídica.

5.- Respecto al deber de reportar en plazo inferior a 3 horas, no existe antecedente en derecho comparado de plazo tan breve. Además, se debería distinguir en criticidad del incidente para fijar tiempo. Hay incidentes que no pasan de ser un incidente sin afectación, otros son incidentes habilitantes parciales y otros totales.

6.- Regulación del principio del cifrado, a qué se refiere con que nadie puede restringir el cifrado, no se encuentra relación con este proyecto de ley.

7.- Sobre las infracciones y sus sanciones, es necesario propender a un catálogo preciso y definido de conductas infraccionales y sus respectivas sanciones, con catálogo de circunstancias atenuantes y agravantes. Sería positivo revisar catálogo siguiendo así recomendaciones de Corte Suprema: garantizar principios de tipicidad y proporcionalidad. Inclusive ver literal c) de artículo 33 en materia de infracciones gravísimas, donde no se habla de operadores de importancia vital.

8.- La amplitud de las facultades que se establecen en el proyecto de ley para la Agencia, podría diluir mandato de artículo 2 de Ley de Bases Generales de la Administración Del Estado: "… Los órganos de la Administración deberán actuar dentro de su competencia y no tendrán más atribuciones que las que expresamente les haya conferido ordenamiento jurídico.".

9.- Respecto al Hacking ético, no están de acuerdo que se permita acceder a un sistema de tratamiento de la información eludiendo medidas de protección. Esto se discutió durante la tramitación de la nueva ley de delitos informáticos.

10.- Por último, desde el punto de vista del periodo de vacancia, les parece positivo contar con un plazo que permita la decidida adecuación a la normativa, sobre todo considerando que Chile va 20 años tarde en comparación a la normativa internacional sobre la materia. Por lo que, sugieren seguir estándares internacionales en que el plazo de implementación y cumplimiento van entre los 21 a 32 meses.

El **profesor del Departamento de Ciencias de la Computación de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile, señor Alejandro Hevia,** con apoyo de una minuta señaló primeramente que sobre los alcances del artículo 46 que modifica la ley N° 21.459 para permitir la búsqueda y notificación responsable de vulnerabilidades en un contexto restrictivo razonable. Existe suficiente literatura científica que justifica la necesidad técnica de esta actividad para mejorar la seguridad de los sistemas informáticos. En el presente documento se explica por qué la criminalización de la búsqueda y notificación responsable de vulnerabilidades, lejos de ser una medida de protección de los sistemas, los vuelve más inseguros.

Agregó, por otra parte, que quienes se oponen a la autorización de la búsqueda y notificación responsable de vulnerabilidades suelen utilizar como analogía la "violación de morada" para sostener que todo acceso no autorizado debiese ser considerado ilícito. Sin embargo, dicha analogía es no sólo ingenua, sino malintencionada e incompleta en el contexto digital, y como tal no captura la situación sobre la cual se desea legislar. A una analogía de sistemas informáticos como "moradas" debiéramos agregar las figuras de "buen vecino" y de "bodegas digitales". Un buen vecino es aquel miembro de la comunidad que, viendo una puerta o una ventana aparentemente abierta, lo comprueba delicadamente

y luego le avisa al dueño de casa. Claramente esa persona no debiera ser penalizada dado que su ánimo es de ayudar al dueño de casa. En contexto digital, el “hacker ético” es el buen vecino, es un profesional que sin causar daño identifica fallas en un sistema y las notifica responsablemente para evitarle robos al dueño de casa.

Asimismo, complementó que, la autorización propuesta en el proyecto de ley hace prácticamente imposible que el acceso ilícito de los ciberdelincuentes pueda quedar amparado bajo la figura del hacking ético. Para asegurar un reporte responsable, el proyecto de ley contiene previsiones sumamente restrictivas, específicas y explícitas para que quien reporta una vulnerabilidad lo haga a la brevedad posible y no pueda ir más allá de lo estrictamente necesario, ni llevarse o alterar nada. Por otra parte, al ser el reporte un requisito esencial para que opere la exención penal, la norma en ningún caso podría servir como carta de inmunidad para una delincuente in fraganti. Además, el proyecto permite que en el futuro puedan agregarse otras exigencias mediante reglamento. En la práctica, el legislador sigue adecuadamente los estándares internacionales ya capturados en la ley belga, en lo que respecta a métodos, límites y proporcionalidad técnica.

Luego, manifestó que, la búsqueda y reporte de vulnerabilidades democratiza la ciberseguridad de los sistemas. Otorga a pymes y organizaciones sin grandes recursos la opción de mejorar su seguridad vía el apoyo gratuito que pueden proveer los mencionados buenos vecinos digitales. En el proceso, los profesionales que actúan como buenos vecinos digitales construyen su reputación como profesionales de ciberseguridad, descubriendo fallas técnicamente complejas y mostrando públicamente su responsabilidad ética con la comunidad. Tales personas existen en el país, como consta en el alto número de reportes de vulnerabilidades recibidas por el Ministerio del Interior (https://www.csirt.gob.cl/vulnerabilidades/), al menos hasta antes de la promulgación de la ley N° 21.458.

Por último, indicó que una ley sin exenciones para la búsqueda y reporte de vulnerabilidades puede ser utilizada como medio de censura. La experiencia internacional es clara respecto a las consecuencias de instaurar leyes sin excepciones para hacking ético. En países donde han sido instauradas leyes que criminalizan la búsqueda y reporte de vulnerabilidades, inevitablemente terminan instrumentalizadas como medidas disuasivas o punitivas. Ha ocurrido, por ejemplo, al encontrar fallas en sistemas asociados a políticos o personas influyentes quienes no están dispuestos a admitir la existencia de dichas fallas por el posible daño reputacional. Es literalmente el cuento del “traje nuevo del emperador”: la seguridad del sistema informático es el traje nuevo, y su dueño es “el emperador”, y cualquiera que ose poner en duda tal traje arriesga la ira del emperador. Tales sistemas “son seguros” porque nadie se atreve a denunciar. Un reciente de AccessNow (agosto 2021) documenta en detalle estas desafortunadas experiencias en Latinoamérica (Argentina, Ecuador, Colombia, y México).

El Presidente Ejecutivo de Chile Telcos, señor Alfie Ulloa, con ayuda de una presentación en power point precisó que el proyecto de ley en discusión se aleja de lo aprobado en el Senado, y de la Directiva Europea (NIS2), al establecer ampliamente a los sujetos pasivos. Debe enfocarse y definir su ámbito de aplicación sobre servicios esenciales y operadores de importancia vital, siempre que cuya afectación pueda impactar la seguridad, la provisión de servicios esenciales, y el efectivo cumplimiento de las funciones del Estado. Además, agregó que, el proyecto de ley establece una discriminación en favor del Estado, ya que busca regular desde una pyme, almacén, panadería hasta una gran empresa, imponiendo obligaciones, responsabilidades y sanciones, hay una sobre carga al sector privado y una clara exclusión del sector público. ¿El Estado en su totalidad no debiese considerarse de importancia vital?

Añadió también que se debería incluir norma expresa que establezca criterios objetivos o una lista de servicios de telecomunicaciones considerados esenciales, puesto que prestan múltiples servicios y tienen más de 60 millones de contratos vigentes, no todos son servicios esenciales. Para dar certeza, se debe distinguir y definir los servicios esenciales que prestan las telecomunicaciones, como por ejemplo el servicio público de

trasmisión de datos, que considere criterios de “racionalidad, proporcionalidad, relevancia, impacto, daño y contexto”. Comentó, la necesidad además de regular la interrupción o suspensión del servicio, ya que, en telecomunicaciones, un incidente o ataque que afecta la seguridad o la capacidad operativa es aquel que interrumpe el servicio, y no todo incidente o ataque interrumpe los servicios (redundancia), y no todos los servicios interrumpidos son esenciales. Recomendó incluir norma expresa que se establezca respecto a la interrupción de servicios esenciales, y en integridad y confidencialidad aplicar normas sectoriales (Subtel), como a su vez normas generales entregando al regulador técnico sectorial la definición de las partes de la infraestructura que resultan críticas para la provisión de un servicio esencial.

Destacó la importancia de limitar la responsabilidad de las empresas respecto de los incidentes de ciberseguridad que afecten a terceros, no se les puede atribuir responsabilidad por las falencias de seguridad o el daño resultado de ataques a terceros, por lo que recomendó incluir norma expresa sobre límite de responsabilidad de los proveedores de internet.

Manifestó que el órgano competente debe ser el regulador sectorial (subtel), en coordinación con la Agencia, por lo que sugiere reponer norma del Senado de modo que Subtel fiscalice y sancione, esta es: artículo 2. “8. Principio de especialidad en la sanción: en materia sancionatoria, se preferirá la aplicación de la regulación sectorial por sobre la establecida en esta ley.

Señaló que es imposible garantizar que no ocurrirán ciberincidencias por lo que la obligación debe ser de medios y no de resultados: deber de desplegar conductas que disminuyan los riesgos. En los principios, establecidos en el artículo 3, deberes generales, artículo 5, y obligaciones se establecen imprecisiones y se utiliza lenguaje poco técnico. Esto es relevante dado las inversiones que deben realizarse para cumplir dichas obligaciones, por lo que recomendó establecer que las obligaciones son de medios y no de resultados, objetivando el lenguaje empleado, y establecer de manera proporcional en relación con los riesgos y el costo.

Indicó que es probable que una conducta sancionada por esta Ley infrinja otras leyes (Consumidor, Datos Personales, etc.). Ante un incidente de ciberseguridad que exponga datos personales o vulnere derechos de consumidores podrán imponerse sanciones por fundamentos jurídicos de ciberseguridad, por fundamentos jurídicos de datos personales, o por fundamentos jurídicos de protección al consumidor, por lo que recomendó modificar el artículo 33 para eliminar “mismos fundamentos jurídicos”.

Recomendó, además, incorporar período de vacancia legal que se ajuste a los estándares internacionales, como plazo de ajuste a la normativa; los regulados deben acometer inversiones y realizar ajustes, y los internacionalmente se han establecido períodos de entre 22 (Directiva UE 2016/1148) y 25 meses (Directiva UE 2008/114/CE).

Para concluir añadió que los proveedores de servicios digitales sin domicilio, pero con operaciones en Chile deben estar afectos y designar un representante legal, ya que los servicios digitales que sean agentes relevantes del mercado o impacten la operación del Estado pueden suministrarse de manera transfronteriza (OTT, servicios cloud, AI, etc.) por empresas sin domicilio en Chile (e.g., SII usando AI), que limita la capacidad de notificar, fiscalizar, y sancionar. La Directiva UE 2022/25555 (“NIS 2”) menciona tres: proveedores de mercado en línea, motores de búsqueda y plataformas de redes sociales a los que por su importancia cataloga como operadores de servicios esenciales (Anexo II).

El **Coordinador de Asuntos Públicos de la Cámara Chilena Norteamericana de Comercio, AMCHAM, señor Marcelo Guajardo, junto a los Secretarios Ejecutivos de nuestra Mesa de Regulaciones Digitales, Carolina Cabrera y Felipe Álvarez**, con ayuda de una presentación en power point señaló primeramente que la definición de “Operadores de importancia vital” es muy amplia y contiene elementos demasiado generales cuya delimitación, finalmente, quedará a cargo de la Agencia Nacional

de Ciberseguridad. El artículo 4° del proyecto de ley no contiene un mecanismo que permita a las entidades que hayan sido clasificadas como “Operadores de importancia vital” puedan oponerse a dicha decisión, de forma que ello pueda ser dirimido por un organismo imparcial.

Además, indicó que no queda del todo claro el motivo por el que este proyecto de ley aplica a todos los organismos, sin embargo, se excluye a las empresas del Estado, salvo si son clasificadas como “Operadores de Importancia Vital”. Esto, no encuentra asidero en la experiencia internacional y pone en riesgo la legitimidad del marco regulatorio al eventualmente infringir el principio de igualdad ante la ley. Resulta preocupante que se proponga una regulación de aplicación general, tanto entidades públicas como privadas, en atención a los riesgos y niveles de exposición reales de Chile frente a ciber amenazas, debido a que pasa por alto niveles de relevancia y criticidad divergentes entre distintas entidades, especialmente entre aquellas que son de baja criticidad y aquellas de importancia vital por prestar servicios esenciales.

Sostuvo apreciar una diferencia de régimen de responsabilidad, ya que mientras que las multas por infracciones establecidas en el artículo 33 son aplicables exclusivamente a instituciones privadas (máx. 20.000 UTM), el artículo 36 establece que las infracciones a los principios y obligaciones de los artículos 21 y 29 serán sancionadas con una multa del 20% al 50% de la remuneración mensual del jefe superior del organismo público infractor. Esta diferencia podría constituir una infracción al principio de igualdad ante la ley, en tanto no hay una razón legítima para establecer una diferencia así de importante en cuanto a los montos de las multas aplicables. Además, la diferencia de trato que podría aplicar la Agencia Nacional de Ciberseguridad, que también será un organismo público, entre organismos públicos y privados, podría acrecentar la infracción al principio de igualdad ante la ley.

Por otra parte, expresó que en relación con el plazo que se establece para el reporte de incidente, si se consideran todos los elementos desde la detección de un eventual incidente informático hasta su reporte, pareciese que 3 horas es un plazo insuficiente. Incluso, no existe antecedente en derecho comparado de un plazo tan breve. Además, se debiese diferenciar por la criticidad del incidente para fijar tiempo. A nivel internacional, la Directiva NIS2 señala expresamente, que “los operadores de servicios esenciales y a los proveedores de servicios digitales que informen ciertos tipos de incidentes graves a las autoridades relevantes en un plazo de 72 horas. Asimismo, la obligación de notificar a sus CISRT sin demora debida, incidentes de seguridad que tengan un impacto significativo”.

Complementó como observaciones que, dentro de lo establecido en el artículo 9 del proyecto de la ley, las facultades de la Agencia para requerir información, es considerablemente amplia. Y finalmente, la iniciativa no contempla una entrada en vigencia diferida o calendario legal de implementación gradual del proyecto de ley, aun cuando se trata de un proyecto que tendrá grandes impactos económicos y culturales en las empresas.

El **Presidente de la Alianza Chilena de Ciberseguridad, señor Marco Antonio Álvarez, en cuya representación asiste el Director señor Guillermo Carey,** con ayuda de una presentación en power point puntualizó que respecto al objeto y ámbito de aplicación del proyecto de ley, es necesario evitar sobrerregulación de sectores no ligados necesariamente a infraestructura crítica: focalizarnos en operadores de importancia vital que presten servicios esenciales. Hay entidades que no califiquen como operadores de importancia vital que se rijan por autoridades sectoriales y directrices generales (el Proyecto engloba a todas las entidades sin distinción en su objeto y aplicación, haciendo extensibles deberes generales a todos). Es imperante respetar el principio de igualdad ante la ley entre empresas públicas y privadas.

Expresó la necesidad de una homologación regulatoria a estándares internacionales. Los incidentes no reconocen límites, la Agencia debe tener una vocación para uniformar criterios por Agencias y Entidades reconocidas internacionalmente

(adaptabilidad). Para evitar sobrecargas, reconocer certificaciones extranjeras para el cumplimiento de las entidades fiscalizadas por el Proyecto.

Por último, acerca de la Agencia Nacional de Ciberseguridad, el procedimiento de designación del Director o Directora Nacional debiese seguir las normas del Sistema de Alta Dirección Pública (ley N° 19.882), por lo que propuso la ratificación del Senado de los 2/3. Además, existe tensión privacidad-ciberseguridad, por las facultades amplias de la Agencia que podrían afectar la calificación de Chile como un País con niveles adecuados de protección de datos: Artículo 9 letra (j), Atribuciones. 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, sobre protección de la vida privada. Y artículo 9 inciso 2, sobre sus atribuciones, la Agencia contará con todas las facultades que fueren necesarias para el cumplimiento de su función fiscalizadora, (…).

El Presidente de la Comisión de Economía y Productividad Digital de la Cámara Nacional de Comercio, señor Cristóbal Aninat junto al Presidente de la Cámara Nacional de Comercio, señor José Pakomio, con ayuda de una presentación en power point desde la perspectiva de las consideraciones generales respecto al proyecto de ley, valoran la creación de un marco regulatorio general que aborde la ciberseguridad en el país, tema que se hace cada día más necesario, ante el acelerado crecimiento y uso masivo de las tecnologías. Apoyan la creación de una Agencia Nacional de Ciberseguridad y un sistema institucional robusto que vele por la coordinación institucional e intersectorial en materia de ciberseguridad. Con todo, observan ciertas materias que pueden ser precisadas o modificadas, con el objeto de mantener estándares internacionales sobre la materia, y que al mismo tiempo promuevan el desarrollo de nuestro país a través de la economía digital.

Ahora bien, como consideraciones específicas, recomendaron lo siguiente:

1.- No establecer un ámbito de aplicación general para todo tipo de entidades privadas. Sugieren que solo los sujetos obligados de mayor relevancia y criticidad, esto es, operadores de importancia vital por prestar servicios esenciales, tengan obligaciones generales de ciberseguridad definidas por ley o por reglamento.

2.- Que expresamente se establezca en la ley aquellos sectores o servicios que se considerarán esenciales.

3.- Establecer expresamente un mecanismo administrativo/judicial que permita objetar la calificación de una entidad como operador de importancia vital.

4.- Que las facultades de la Agencia sean de carácter estricto y estén expresamente establecidas en la ley.

5.- Revisar la conveniencia de establecer el Hacking Ético sin autorización previa del titular del sistema informático, ya que se trata de una materia que fue zanjada recientemente por el Congreso y que, además, afecta el derecho de propiedad y privacidad.

6.- Limitar el alcance de la obligación de reportar solo a los operadores de importancia vital, y que de manera voluntaria otras entidades puedan realizarlo. Recomiendan aumentar el plazo de 3 a 72 horas para reportar incidentes de ciberseguridad que tienen un impacto significativo, siguiendo los mejores estándares internacionales.

7.- Establecer expresamente la supletoriedad de la ley en el caso de sectores que ya se encuentran regulados tanto en materia de ciberseguridad, protección de datos personales, e infraestructura critica. Lo anterior, debe venir acompañado de coordinación intersectorial e interinstitucional a cargo de la Agencia de Ciberseguridad.

8.- Definir una lista específica de infracciones leves, graves y gravísimas; criterios detallados para guiar la imposición de una sanción; incluir circunstancias atenuantes, y recursos judiciales.

9.- Establecer una entrada en vigencia diferida de la ley y/o un proceso de implementación gradual que permita una debida adecuación de los sujetos regulados a la normativa e internalización de los nuevos costos de cumplimiento.

La **abogada especialista en protección de datos personales y nuevas tecnologías, señora Romina Garrido,** expuso con apoyo de una presentación en power point desde un punto de vista general, sostuvo que si se establecen estándares y responsabilidades claras, las leyes de ciberseguridad ayudarán a proteger los sistemas y redes de infraestructuras críticas, empresas y organizaciones, y así a reducir así el riesgo y el impacto de los ciberataques.

Ahora bien, al referirse sobre particularidades del proyecto de ley, señaló, primeramente, que debe realizarse una revisión de los principios rectores establecidos en el artículo 3, ya que existen principios repetidos en las definiciones, o que no vuelven a ser mencionados en la ley y no queda claro cómo deben aplicarse: Igualdad y no discriminación. Además, agregó, respecto a su artículo 4, la idea del legislador es distinguir servicios esenciales (SE) y dentro de éstos los operadores de importancia vital (OIV), sin embargo, la ley no colabora en la definición de lo uno y lo otro, definiendo lo que ya se ha dicho de manera reiterativa sin aportar información. Si los OIV tendrán mayores obligaciones y responsabilidades debe estar claro quiénes serán y en ocasiones se confunden con los SE.

Agregó que, en consideración a lo establecido en su artículo 5, sobre los sectores regulados, los deberes de la ley aplican a todas las entidades, públicas, privadas sean o no servicios esenciales u OIV (se exceptúan las empresas públicas que no sean OIV y autonomías constitucionales). La ciberseguridad es un asunto importante y debe ser prioritario, pero no todas las organizaciones que tienen altos niveles de digitalización, madurez, recursos o lidian con los mismos niveles de criticidad. También, en su artículo 6, acerca de las obligaciones de los OIV, se imponen fuertes deberes de seguridad en los términos de un sistema de Gestión de Seguridad de la Información. Aquí debe ponerse atención en que dichos estándares deberán ser acreditados por los Centros de Certificación acreditados por la Agencia, artículo 24. No hay más referencia a ellos cumpliendo una labor tan relevante, respecto de su giro, *expertise,* capacidades, si toda entidad deberá certificarse, etc. La adopción de los deberes hace necesario un tiempo razonable para la adecuación.

Sugirió revisar la redacción de las potestades que se establecen a la Agencia Nacional de Ciberseguridad, siendo este el elemento y objetivo principal del proyecto de ley, posee amplias facultades de regular, fiscalizar y sancionar a los órganos públicos y privados (letra n, inciso segundo). A lo largo del texto las funciones van quedando relegadas en una burocracia con distintas instancias consultivas, y la Agencia no es finalmente autónoma en tomar decisiones para las que debería tener potestades claras.

Por último, desde el punto de vista del marco de las sanciones, comentó que se establece uno diferenciado entre leves, graves y gravísimas, aumentado en cada escala si se trata de OIV. Las conductas en las leves son residuales: todo incumplimiento no calificado como grave o gravísimo, por ejemplo, pagar el rescate de ransomware. Las graves consideran tres conductas, entre ellas el incumplimiento de deberes (artículos 5 y 6) cuando se trate de un operador de servicios esenciales (figura distinta de un OIV). Las gravísimas solo pueden ser cometidas por un operador de servicios esenciales (figura distinta de un OIV).

La Comisionada de la Comisión para el Mercado Financiero, señora Bernardita Piedrabuena, expuso con apoyo de una presentación en power point expresó que el proyecto de ley de permitirá fortalecer la institucionalidad y la capacidad de respuesta frente a eventos de ciberseguridad, al promover la coordinación y colaboración entre las distintas agencias del Estado y el sector privado.

Como observación señaló que se puede presentar un potencial traslape de funciones entre la CMF y la Agencia, por lo siguiente:

• La Agencia tendrá las mismas atribuciones que la CMF en relación con los mismos fiscalizados: superposición de funciones y responsabilidades.

• El fiscalizado no debería reportar a más de una autoridad en relación con una misma materia. Por ejemplo, en el caso de incidentes.

• Las funciones de CSIRT sectorial se tienden a traslapar con las funciones de la CMF. Debe quedar claro el alcance de las responsabilidades institucionales. No hay claridad de quién determina la conformación de los CSIRT sectoriales.

• La coordinación entre los privados y las autoridades en caso de ciberataques es esencial. La experiencia nacional e internacional muestra que son las propias instituciones financieras (con sus proveedores tecnológicos), las que manejan sus incidentes de ciberseguridad directamente, sin intervención de la autoridad. La relación debe ser fluida con la autoridad en cuanto a la información proporcionada sobre el incidente y a la coordinación de las comunicaciones externas (público afectado).

Sugirió para avanzar con lo antes expuesto, establecer una estrecha coordinación y colaboración entre la Agencia de Ciberseguridad y la CMF. Coordinar el actuar de las instituciones con competencia en materia de ciberseguridad; dictar protocolos y estándares técnicos con el objeto de regular los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad, y someter la normativa de la Agencia a consulta pública y coordinación regulatoria de la Ley 19.880 de procedimientos administrativos (artículo 37 bis). Pero, manteniendo la deferencia por el regulador financiero al ser el supervisor sectorial, la CMF conoce en profundidad el funcionamiento del sector financiero. Es por ello por lo que en el mundo es el regulador financiero el que regula y supervisa, y el que dicta las instrucciones generales y particulares a las instituciones financieras en materias de ciberseguridad. La CMF viene normando hace años la gestión de riesgos asociados a ciberseguridad en la industria financiera: contamos con experiencia y personas, disponibles 24x7 para supervisar que se cumplan las normativas de ciberseguridad. Contamos con sistema de Reporte de Incidentes Operacionales. El objetivo es evitar acciones que pongan en riesgo la estabilidad del sistema financiero y el sistema de pagos: hablamos de activos cercanos a 2,1 veces el PIB.

Finalizó concluyendo que el proyecto es necesario y representa un avance significativo para nuestro país en materia de ciberseguridad. La preocupación de la CMF es la eventual superposición de funciones con la Agencia, la que debe quedar bien delimitada. Todavía hay espacio para precisar ámbitos de competencia en materia de fiscalización y respuesta. En vista de las atribuciones y funciones que se asignan a la Agencia y al CSIRT, se debe contar con los recursos adecuados para ejercer apropiadamente dichas funciones. En el caso que la CMF se constituya como CSIRT, se deberá diseñar cuidadosamente la convivencia del CSIRT dentro de un organismo fiscalizador que además califica por gestión a sus fiscalizados.

El ingeniero señor Jorge Atton, expuso con apoyo de una presentación en power point sobre algunos comentarios al proyecto de ley, señalando que:

1.- Evitar la duplicidad regulatoria y la multiplicidad de normativas sectoriales El proyecto Incorpora los conceptos de “servicios esenciales” y “operadores de importancia vital”. Establece un régimen de obligaciones de ciberseguridad y sanciones. Son definidos por la Agencia con informe de la ANI. Se busca generar un ecosistema norma0vo en materia de ciberseguridad y sectores regulados, manteniendo las facultades normativas sectoriales, bajo coordinación con la Agencia Nacional de Ciberseguridad. Ello debe quedar claramente definido para evitar duplicidad de normas. Las competencias de especialización la tienen los órganos reguladores. La actual ANI no tiene las competencias para abordar esta temática multisectorial.

Al respecto sugirió la participación de las Entidades Reguladoras de cada Sector, cuyos informes deben ser vinculantes para definición que realice la Agencia. Recoger vía transitorios las normativas vigentes de cada sector.

2.- Desde la organización y mayor certeza jurídica, la Agencia Nacional de Ciberseguridad (ANCI) tendrá facultades regulatorias, fiscalizadoras y sancionatorias, dependiente del Ministerio de Interior, y crea el Consejo Multisectorial sobre Ciberseguridad.

La Agencia tendrá facultades que podrían ser superiores a las Entidades Regulatorias. Se pierde el principio de especialidad, hay una excepción con la CMF, pero no con instituciones claves como son Telecomunicaciones y Energía. La Agencia en la Poli4ca Nacional de Ciberseguridad siempre se pensó como un órgano coordinador de los organizamos especializados (Superintendencias y Entidades regulatorias).

Sobre esto, sugirió crear un Consejo Directivo Autónomo con atribuciones y alcance claramente definido, es decir tratar su organización siguiendo el mismo modelo establecido para la Autoridad de Control en Protección de Datos Personales (Título VI).

3.- En cuanto a la gradualidad de las sanciones es posible un doble efecto con la normativa sectorial, ya que la iniciativa entrega a la Agencia Nacional de Ciberseguridad (ANCI) amplias facultades regulatorias, fiscalizadoras y sancionatorias, dependiente del Ministerio de Interior. Las sanciones no tienen gradualidad, cada sector tiene en sus respectivas leyes orgánicas el tratamiento y apelaciones para las sanciones. Y no se clasifican las sanciones.

En este punto sugirió incorporar la modalidad (artículo 34 del proyecto de Ley Datos Personales) que clasifica las sanciones en función del tamaño y alcance de la afectación.

4.- Respecto al plazo de 3 horas para reporte de incidente, sugirió se establezca un plazo mayor, como ocurre a nivel internacional, y es que las empresas de servicios esenciales informen los incidentes graves en un plazo de 72 horas.

5. Sobre el principio de igualdad ante la ley, expresó que no tiene mucha lógica la exclusión y la discriminación positiva con las empresas del Estado, a excepción de las definidas como servicios esenciales, pero sí la ley se aplica a todas las empresas del sector privado, independiente de su tamaño. Esperó sea una mala redacción y no obedezca a un sesgo ideológico. Las Normas deben ser de aplicación general, señaló.

6. Por último, en lo que respecta a la provisión transfronteriza de servicios esenciales y la dificultad de la aplicación de la ley servicios digitales que son servicios esenciales que pueden suministrarse de manera transfronteriza. La Directiva UE 2022/25555 (“NIS 2”) menciona tres: proveedores de mercado en línea, motores de búsqueda y plataformas de redes sociales a los que por su importancia cataloga como operadores de servicios esenciales.

El **profesor de la Universidad del Desarrollo, señor Juan Pablo González,** expuso con apoyo de una presentación en power point expresó como aspectos generales, el proyecto de ley solo enuncia las Infraestructuras Críticas de la Información en su título, pero cambia la denominación de éstas, a lo largo del mismo por servicios esenciales y los operadores de importancia vital. En conformidad al artículo 4º del Proyecto, que define lo que se entiende por servicio esencial (todo servicio impacte en la defensa nacional, la sociedad o la economía) y operador de importancia vital (institución pública o privada), pero se confunden a lo largo del Proyecto, inclusive en ciertas partes se habla derechamente de “operadores de servicios esenciales”. Los operadores de importancia vital, se tomará en cuenta criterios como: prestar un servicio calificado como esencial; que el servicio depende de redes y sistemas informáticos; y que un incidente de ciberseguridad tenga un impacto perturbador sobre dicho servicio.

Ahora bien, desde una perspectiva más específica, manifestó que en lo que dice relación con el deber de reporte de incidencias, el proyecto señala que debe realizarse dentro de 3 horas desde que tuvo conocimiento (mismo estándar Decreto Supremo Nº273/2022) pero es diferente a lo que ya existen a nivel regulatorio nacional (ej. RAN 20-8 CMF, 30 min desde su ocurrencia) o a nivel internacional (NIS2 (Directiva de Ciberseguridad) y GDPR, 72 horas). En el caso de los operadores de importancia vital deben reportar, además del incidente, su plan de acción ante del incidente, pero no está

dentro de las obligaciones específicas que deben cumplir este tipo de operadores (artículo 6).

Además, agregó analizar que el proyecto crea el Comité Interministerial de Ciberseguridad, aunque ya exista a nivel reglamentario a través del DS Nº 533, 2015, otorgándole no solo facultades de asesoramiento sino resolutivas, particularmente, aprobar aquellos servicios esenciales y operadores de importancia vital.

Asimismo, manifestó, desde la cuestión infraccionaría, que el proyecto reconoce infracciones leves, graves y gravísimas, interesante es que la multa asociada, aumenta inmediatamente en el caso de las infracciones leves o graves que los infractores sean operadores de importancia vital. Se debe analizar con detenimiento las conductas que dan lugar a las infracciones, especialmente, si se tiene en cuenta que se incluye una agravante especial que señala (artículo 38) a saber “si resultare un delito que afecte gravemente la continuidad operativa de un operador de importancia vital o si el delito consiste en la alteración o supresión de datos informáticos de un operador de importancia vital” ¿Esto será calificado por la Agencia? Finalmente, añadió, la regla que propone el Proyecto en que se aplicará la sanción de mayor gravedad en caso de que concurran con arreglo a otras leyes por los mismos hechos y fundamentos jurídicos, no queda del todo clara.

Concluyó expresando que el proyecto es un esfuerzo valorable en para coordinar y sistematizar diversas regulaciones en materia de ciberseguridad, a través de la creación de la Agencia de Ciberseguridad tiene y el reconocimiento de los equipos técnicos de respuesta ante incidentes informáticos (CSIRT). La inclusión de otras temáticas como la regulación del Comité Interministerial de Ciberseguridad, el Consejo Multisectorial Consultivo y la regulación del Ethical Hacking, hace que se torne una estructura burocrática en su funcionamiento. Sin embargo, no queda del todo claro la diferenciación entre los servicios esenciales u operadores de importancia vital, especialmente, si se considera que tendrán obligaciones específicas e infracciones en caso de incumplimiento. Ni tampoco queda expresamente señalado la existencia de un plazo de vacancia o un plan de implementación gradual a la regulación, lo que puede ser complejo para algunos sectores poco maduros en la materia y la temprana adopción de esta regulación.

****

Teniendo a la vista las consideraciones y argumentos reseñados en el mensaje y las opiniones y observaciones expuestas por las autoridades e invitados, las y los señores diputados fueron de parecer de aprobar la idea de legislar sobre la materia.

Puesta en **votación general** la idea de legislar, se **APRUEBA** por unanimidad de votos, en la forma descrita en las constancias reglamentarias previas.

B.- DISCUSIÓN Y VOTACIÓN PARTICULAR.

Primeramente, se deja constancia que se acuerda formar una mesa técnica de trabajo compuesta por los asesores de cada uno de las y los señores diputados miembros de esta Comisión y representantes del Ejecutivo, liderados por doña Michelle Bordachar, con el propósito de procurar acercamientos y consensos respecto de la aprobación del articulado propuesto por el Senado y las indicaciones formuladas tanto por el Ejecutivo como por las y los diputados al proyecto y, por ende la discusión y votación del articulado que ofrece el Senado no necesariamente se hará correlativamente en función del articulado, si no que sobre los avances de los acuerdos que la citada mesa sugirió a la Comisión, a través de propuestas de indicaciones.

****

Se dio lectura al artículo 1° del proyecto de ley aprobado en el Senado:

"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 éstos 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, las Fuerzas 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 éste 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."

Al artículo 1, el diputado señor Jorge Alessandri presentó la siguiente **indicación N°1:**

"En el artículo 1° del proyecto de ley, para reemplazarlo por el siguiente:

"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 éstos 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 efectos de esta ley, la Administración del Estado estará constituida por los Ministerios, las delegaciones presidenciales regionales y provinciales, los Gobiernos Regionales, las Municipalidades, las Fuerzas Armadas, de Orden y Seguridad Pública, las empresas públicas creadas por ley, y los órganos y servicios públicos creados para el cumplimiento de la función administrativa.

Los organismos autónomos constitucionales se ajustarán a las disposiciones de esta ley que expresamente ésta señale, y a las de sus respectivas leyes orgánicas que versen sobre los asuntos a que se refiere el inciso primero de este artículo.

Las disposiciones de esta ley serán aplicables a las empresas del Estado y sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio.

La institucionalidad establecida por esta ley velará por la protección, promoción y respeto del derecho a la seguridad informática de las personas y sus familias,

que comprende la adopción de 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.”.”.

El **presidente diputado señor Jorge Alessandri**, explicó que el objeto de la indicación, respecto a la modificación en su inciso segundo, busca principalmente que se establezca de manera clara y no se defina erróneamente lo que se entiende por Administración del Estado, sino que se identifique qué organismos forman parte de él, siguiendo la formula del artículo 1 de la ley N°18.575 sobre bases generales de la Administración del Estado.

Además, explicó, que la modificación en su inciso tercero tiene como propósito mejorar la redacción del texto original del proyecto de ley, siguiendo la regla del inciso segundo del artículo 2 de la ley N°20.285 sobre acceso a la información pública, por cuanto el inciso de organismos autónomos constitucionales, en las conversaciones de la mesa de trabajo, se dijo que sería sacado para ser incluido en otro capítulo.

Ahora bien, respecto al inciso cuarto, la indicación propone que se disponga expresamente esta norma a las empresas que se indica, lo que concuerda con la indicación del Ejecutivo en referencia a suprimir la parte final del artículo 2, que dice relación con que esta ley se aplique a todas las empresas estatales que se indique y no solo a aquellas que sean calificadas como operadoras de importancia vital. A esto, el comentario que se repitió mucho en la discusión general por diversos expertos fue la de especificar cuáles son las empresas privadas, públicas y estatales estratégicas para esta norma, de lo contrario sería muy difícil su aplicación.

Y, por último, manifestó un par de cambios de redacción, pero que van en la línea de lo propuesto por el Ejecutivo.

El **Subsecretario del Interior, señor Manuel Monsalve**, recordó que, previo a la votación particular, en el Senado este proyecto se aprobó por unanimidad en Sala, teniendo presente que es una materia que le preocupa y ocupa a todas las fuerzas políticas, y por ello se pretende que acá en la Cámara de Diputados se le entregue el tiempo necesario para concretar los consensos necesarios.

Luego, manifestó como Ejecutivo el acuerdo respecto a la indicación presentada por el diputado señor Jorge Alessandri, y por ello sugiere se vote.

El **diputado señor Andrés Longton**, sugirió a la Comisión votar este artículo por incisos, ya que, si bien en algunos hay acuerdo en otro no, como por ejemplo en dejar a la ley de aplicación amplia que afecte a toda empresa sin importar si quiera su tamaño, que probablemente no tienen las capacidades para ser obligadas como lo establece esta ley.

El **Subsecretario del Interior, señor Manuel Monsalve**, indicó que el Ejecutivo no tiene como propósito sancionar a las pequeñas y medianas empresas, pero si entregarles recomendaciones de estándares básicos de seguridad ya que al ser parte de un conjunto puede generar debilidades, por ello la importancia que, en este artículo, sobre el objetivo de la ley sí se incluyan.

El **diputado señor Raúl Leiva**, sugirió aprobar la indicación sustitutiva presentada por el diputado señor Jorge Alessandri, y así poder avanzar.

El **diputado señor Cristián Araya**, compartió la preocupación del diputado Longton, por lo que estimó conveniente se vote por inciso, y en aquel que se refiera a su aplicación en las empresas privadas, se especifique que se trata de aquellas calificadas como operadora de importancia vital, de lo contrario cualquiera, por muy pequeña que sea quedaría obligada a cumplir con la exigencias de esta ley, lo que en la práctica podría ser muy perjudicial para ellas, desde el punto de vista de sus capacidades y recursos.

La **diputada señor Lorena Fries,** señaló que en la exposición del proyecto de ley se determinó que se siguen los lineamentos en la Unión Europea, que amplía su aplicación.

La Comisión acordó votar la indicación sustitutiva al artículo 1 del proyecto de ley, formulada por el diputado señor Jorge Alessandri, con la opción, en caso de que se apruebe, presentar indicaciones respecto de esta.

Puesta en votación **la indicación N°1, que sustituye el artículo 1 del proyecto de ley, se aprueba** por alcanzar la mayoría de los votos. Votan a favor las y los señores diputados señores Jorge Alessandri (presidente), Cristián Araya, José Miguel Castro, Lorena Fries, Henry Leal, Raúl Leiva, Andrés Longton, Maite Orsini, Gloria Naveillán, Alejandra Placencia y Diego Schalper. Votó en contra el diputado señor Jaime Araya. Sin votos en contra. **(11-1-0).**

Luego, se da lectura a una **indicación que propone un nuevo artículo 1°**, acordada entre los asesores del Gobierno y de los parlamentarios, suscrita por la diputada señora Alejandra Placencia y los diputados señores Jorge Alessandri, José Miguel Castro, Henry Leal, Andrés Longton y Andrés Jouannet, que establece lo siguiente:

“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 éstos 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 determinadas en el artículo 4°, y los mecanismos de control, supervisión y de responsabilidad ante infracciones.

Para efectos de esta ley, la Administración del Estado estará constituida por los Ministerios, las delegaciones presidenciales regionales y provinciales, los Gobiernos Regionales, las Municipalidades, las Fuerzas Armadas, de Orden y Seguridad Pública, las empresas públicas creadas por ley, y los órganos y servicios públicos creados para el cumplimiento de la función administrativa.

Las disposiciones de esta ley serán aplicables a las empresas del Estado y sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio”.

El **Subsecretario de Interior, señor Manuel Monsalve**, junto con agradecer el compromiso de parte de las y los diputados de la Comisión en perfeccionar los proyectos de ley sobre seguridad, expresó su acuerdo respecto a la indicación recién leída.

La **asesora legislativa del Ministerio del Interior, señora Michelle Bordachar,** manifestó que en relación con la indicación que se aprobó en su momento, el texto presentado por el diputado Alessandri, se hicieron muy pocas modificaciones. En el inciso primero, en lugar de referirse a instituciones privadas, se refirieren a instituciones determinadas en el artículo cuarto, objeto de mayor debate y opiniones por parte de los expertos, y esta redacción lo permite. Luego la eliminación de la referencia a los órganos autónomos constitucionales, ya que eso será objeto de debate en el artículo 46, eliminaría la referencia en esta nueva propuesta y, por último, en el inciso final, una de las indicaciones proponía hacer una modificación sustancial al inciso final, pero les parece que en honor al tiempo y al compromiso de todas las diputadas y diputados en que este proyecto pueda avanzar rápido, se llegó al acuerdo de que en realidad lo mejor sería eliminar ese artículo porque de todas formas siempre se entiende que la institucionalidad establecida por la ley al final del día, vela por las personas y sus familias, aunque no se diga expresamente.

El presidente diputado señor Andrés Longton, señaló que, en caso de aprobarse esta indicación, se deja sin efecto todas las indicaciones formuladas en relación con el artículo 1° por cuanto lo reemplaza pasando a ser el texto definitivo, inclusive la

indicación N°1 del diputado señor Jorge Alessandri, ya aprobada en sesión N°65, y el texto del artículo 1° del mensaje.

Se da lectura a todas las indicaciones al artículo 1°:

Al artículo 1°, los diputados **señores José Miguel Castro, Andrés Longton y Diego Schalper**, presentaron las siguientes indicaciones:

"Reemplázase, en el inciso primero del artículo 1° la palabra "privadas" por "que prestan servicios esenciales y las calificadas como operadores de importancia vital".".

"Introdúcense las siguientes modificaciones al inciso segundo del artículo 1°:

i. Sustitúyase la frase "a los ministerios, las delegaciones presidenciales regionales y provinciales, los gobiernos regionales, las municipalidades, las Fuerzas Armadas, las Fuerzas de Orden y Seguridad Pública y los órganos y servicios públicos creados para el cumplimiento de la función administrativa" por "aquellos indicados en el inciso segundo del artículo 1º del DFL Nº1-19.653 que fija texto refundido, coordinado y sistematizado de la ley Nº18.575, orgánica constitucional de Bases Generales de la Administración del Estado y las empresas del Estado y sociedades en que éste tiene una participación accionaria superior al 50% o designa a la mayoría de los miembros de su Directorio.";

ii. Sustitúyase la oración: "Los órganos autónomos constitucionales se ajustarán a las disposiciones de esta ley que así lo señalen" por "Los órganos autónomos constitucionales dictarán su propia normativa y quedarán sujetos a su propia tutela, sin perjuicio de la cooperación y asistencia que sus normativas propias dispongan";

iii. Suprímase lo siguiente "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 éste tenga participación accionaria superior al 50% o mayoría en el directorio, salvo que sean calificadas como operadores de importancia vital".

"Sustitúyase el inciso tercero del artículo 1° por el siguiente: "La institucionalidad establecida por esta ley orientará sus acciones para lograr el más alto nivel de ciberseguridad con el objetivo de mejorar el funcionamiento de los mercados y los servicios que las instituciones públicas y privadas entregan a la ciudadanía."

Al artículo 1°, el diputado señor **Jorge Alessandri y la diputada señora Gloria Naveillán**, presentaron las siguientes indicaciones:

"Para agregar, en el artículo 1°, al final del primer inciso la siguiente frase; "Asimismo, se deberá, en coordinación con el Ministerio de Relaciones Exteriores, establecer los convenios de cooperación internacional en materias de ciberseguridad".".

"Para eliminar en el artículo 1°, el párrafo final del 2° inciso y reemplazarlo por la siguiente frase: "Se aplicarán las disposiciones de esta ley a las empresas o instituciones calificadas como operadores de importancia vital, sean estas públicas creadas por ley o empresas del Estado en cuyas sociedades el Estado tenga una participación accionaria superior al 50% o mayoría en el directorio, y a las empresas de sector privado calificadas como operadores de importancia vital.".".

Al artículo 1°, el diputado señor **Jorge Alessandri,** presentó las siguientes indicaciones:

"Para eliminar en el artículo 1°, el párrafo final del 2° inciso y reemplazarlo por el siguiente; "Asimismo, las disposiciones de esta ley serán aplicables a las empresas públicas creadas por ley y a las empresas del Estado y sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio".

“Para suprimir el inciso tercero del artículo 1°”.

Al artículo 1°, el diputado señor **Cristián Araya,** presentó la siguiente indicación:

“Al artículo primero del proyecto de ley: Para agregar en el inciso primero del artículo 1° a continuación de la expresión “, así como los deberes de las instituciones privadas” la expresión “calificadas como operadores de importancia vital”.

Al artículo 1°, el diputado señor **Andrés Jouannet**, presentó las siguientes indicaciones:

“Reemplácese en el inciso primero del artículo 1° propuesto, la expresión “, así como los deberes de las instituciones privadas” por “y los deberes de las instituciones públicas y privadas calificadas como operadores de importancia vital, así como la normativa que regula las relaciones entre estos y sus proveedores”.

“Suprímase en el inciso segundo del artículo 1° propuesto, la expresión "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 éste tenga participación accionaria superior al 50% o mayoría del directorio, salvo que sean calificadas como operadores de importancia vital".

“Suprímase en el inciso tercero del artículo 1° propuesto las expresiones “y sus familias” e “, incluyendo las herramientas de cifrado”.

Puesta en votación la indicación que propone **un nuevo artículo 1°, se aprueba por unanimidad.** Votan la diputada señora Alejandra Placencia, y los diputados señores Jorge Alessandri, Cristián Araya, Andrés Jouannet, Henry Leal y Andrés Longton (presidente). **(6-0-0)**

Por consiguiente, al aprobarse esta indicación sustitutiva al artículo 1°, se rechazan reglamentariamente, todas las otras indicaciones y el texto del mensaje al mismo artículo.

****

Se da lectura al artículo 2° del proyecto de ley:

“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 éste 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.”.

Al numeral 1 del artículo 2°, el diputado señor **Andrés Jouannet**, presentó la siguiente indicación:

“Suprímase el numeral 1 del inciso primero del artículo 2° propuesto.”

Indicación que su autor **retira**.

Puesto en votación el **numeral 1 del artículo 2° del proyecto de ley, se aprueba por unanimidad**. Votan la diputada señora Alejandra Placencia, y los diputados señores Jorge Alessandri, Cristián Araya, Andrés Jouannet, Henry Leal, Raúl Leiva y Andrés Longton (presidente). **(7-0-0)**

Al numeral 4 del artículo 2°, el diputado señor **Andrés Jouannet**, presentó la siguiente indicación:

“Suprímase el numeral 4 del inciso primero del artículo 2° propuesto.”

Indicación que su autor **retira.**

Por no presentarse indicaciones a los numerales 2, 3 y 4 del artículo 2° del proyecto de ley, se someten a votación de manera conjunta.

Puestos en votación **los numeral 2, 3 y 4 del artículo 2° del proyecto de ley, se aprueba por unanimidad.** Votan la diputada señora Alejandra Placencia, y los diputados señores Jorge Alessandri, Cristián Araya, Andrés Jouannet, Henry Leal, Raúl Leiva y Andrés Longton (presidente). **(7-0-0)**

El Subsecretario del Interior, señor Manuel Monsalve, señaló que el artículo 2° establece un conjunto de definiciones que están vinculadas a debates técnicos más de fondo, que están regulados en otros artículos, particularmente el artículo 4°, donde se regulan los servicios esenciales y los operadores de importancia vital, por lo que

propuso dejar pendientes algunos numerales relacionados para el momento de discusión de ese artículo, tales como el numeral 5, autoridad sectorial; 6, ciberataque; 20, operadores de importancia vital; 24, sector regulado y 25 sobre servicios esenciales.

Al número 7 del artículo 2°, los diputados señores **José Miguel Castro, Andrés Longton y Diego Schalper,** presentaron la siguiente indicación:

"Suprímanse los numerales 7 y 8 del artículo 2°.".

Indicación que sus autores **retiran.**

Puesto en votación **el numeral 7 del artículo 2° del proyecto de ley, se aprueba por unanimidad.** Votan la diputada señora Alejandra Placencia, y los diputados señores Jorge Alessandri, Cristián Araya, Andrés Jouannet, Henry Leal, Raúl Leiva y Andrés Longton (presidente). **(7-0-0)**

Al número 8 del artículo 2°, el diputado señor **Andrés Jouannet**, presentó la siguiente indicación:

"Suprímase el numeral 8 del inciso primero del artículo 2° propuesto."

El **diputado señor Andrés Jouannet,** como autor de la indicación, señaló que este es un concepto que restringirá el debate, por lo que sugirió se elimine.

El **diputado señor José Miguel Castro**, complementó que esta definición tiene un vicio base en relación con lo que se ha aprobado hasta el momento, ya que se estaría dejando de lado a las instituciones, lo más importante es que, por ejemplo, un Banco que es una institución que, por ejemplo, un servicio que es una institución tenga programas de ciber higiene, de higiene propia. Apoyó la idea de mejorar la redacción o bien eliminarla.

La **asesora legislativa del Ministerio del Interior, señora Michelle Bordachar,** expresó que hay dos frases típicas en la ciberseguridad, una, que hay dos tipos de institucionas, aquellas que han sido *hackeadas* y las que saben que fueron *hackeada*s, o sea todos pueden ser objeto de ataque, y dos, que la ciberseguridad es tan fuerte como el eslabón más débil que al final del día es la persona.

Agregó estar de acuerdo en que la ciber higiene es parte de las instituciones, pero al final del día quien debe cumplir con esa higiene deben ser las personas que están detrás de los computadores. Si bien este concepto no se utiliza mucho en la ley, sí se utilizará por la Agencia, sobre todo en campañas educaciones, como ocurre en otros países, tanto en las políticas nacionales de ciberseguridad como en la norma en la que se basa este proyecto de ley, que es la directiva de la Unión Europea.

El **presidente diputado señor Andrés Longton**, manifestó su duda en relación con las consecuencias de no cumplimiento con la ciber higiene, en qué se traduce en la práctica, existirá o no una directriz al respecto.

El **abogado señor Juan Pablo Gonzalez, académico de la Universidad del Desarrollo,** comentó que es importante entender que estos conceptos siempre se utilizan en el entorno de la existencia de estrategias de ciberseguridad integrales dentro de la organización. Por lo que propone se vincule expresamente con el resto del texto del proyecto que se está discutiendo. Además, la Agencia Nacional de Ciberseguridad no se maneja o no se expresa de manera clara, por ejemplo, a propósito de las obligaciones del artículo 5° y 6| del proyecto de ley, que son las obligaciones tanto generales como específicas para aquellos de importancia vital y servicios esenciales.

Señaló, que lo relevante de incluir una definición de este tipo es incluirlo de ciertas obligaciones específicas que permitan eventualmente generar alguna acción concreta, ya sea en el incumplimiento de alguna obligación de manera directa o indirecta, lo que en el texto no se visualiza.

El **abogado señor Claudio Magliona, académico de la Universidad de Chile**, agregó a lo anterior, considerando que la palabra tiene hoy día una utilización pensada para procesos de capacitación, recomendó no ocupar el término en el texto legal, sino que lo reserve la Agencia en el futuro para sus campañas de capacitación educativas.

El **Subsecretario del Interior, señor Manuel Monsalve,** solicitó, en virtud a las diversas intervenciones de los diputados y expertos, postergar la votación del resto de los numerales del artículo 2° sobre las definiciones, para reordenarlo y entregar una propuesta más precisa e integral, a propósito de lo acordado por la mesa de trabajo entre asesores del Ejecutivo y de los parlamentarios, colocando las definiciones más esenciales y también estableciendo estas van a primar en el ámbito de la ciberseguridad e independiente de las instituciones, sean públicas o privadas, quedando establecidas en el reglamento de la ley de manera de poder también recoger el principio de flexibilidad que aquí se ha planteado en virtud de definiciones que pueden ir variando en el tiempo.

Recabado el acuerdo solicitado (dejar pendiente el resto de los numerales del artículo 2º), se procede a dar lectura a los siguientes artículo que no poseen indicaciones de las y los diputados.

***

Se da lectura al artículo 10, 11, 12 y 13 del proyecto de ley:

“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 Nº19.882, 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 Nº19.882, que regula la nueva política de personal a los funcionarios públicos que indica, hasta el segundo nivel jerárquico."."

Por no existir indicaciones respecto de los artículos 10, 11, 12 y 13, se acordó someterlos en votación de manera conjunta.

Puestos en votación **los artículos 10, 11, 12 y 13 del proyecto de ley, se aprueban por unanimidad.** Votan la diputada señora Alejandra Placencia, y los diputados señores Jorge Alessandri, Cristián Araya, Andrés Jouannet, Henry Leal, Raúl Leiva y Andrés Longton (presidente). **(7-0-0)**

***

Se da lectura al artículo 14 del proyecto de ley:

"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 Nº1, promulgado el año 2000 y publicado el año 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 el año 2004 y publicado el año 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 el año 2004 y publicado el año 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. Estos 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 el año 2004 y publicado el año 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, promulgado y publicado el año 1977, del Ministerio de Hacienda, y al decreto supremo N°1, promulgado y publicado el año 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 fue fijado por el decreto con fuerza de ley N°1, promulgado el año 2000 y publicado el año 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, promulgado y publicado el año 1975, de Administración Financiera del Estado.".

Al artículo 14, los **diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, presentaron la siguiente indicación:**

"Intercálase, en el artículo 14, entre la palabra "Trabajo" y el punto aparte, una coma y lo siguiente: "con excepción del personal que ejerza funciones directivas, hasta el tercer nivel jerárquico, el cual se regirá por las reglas generales.".".

Los autores de la indicación **la retiran.**

Puesto en votación **el artículo 14 del texto del proyecto, se aprueba por unanimidad**. Votan a favor las y los diputado señores Jorge Alessandri, José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal, Andrés Longton (presidente), Gloria Naveillán, Alejandra Placencia y Diego Schalper. **(9-0-0)**

***

Se da lectura al artículo 15 del proyecto de ley:

“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 éstas 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 a fin de 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 el año 2004 y publicado el año 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N°18.834, sobre Estatuto Administrativo.”

Puesto en votación **el artículo 15 del texto del proyecto, se aprueba por unanimidad.** Votan a favor las y los diputado señores Jorge Alessandri, Jaime Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal, Andrés Longton (presidente), Gloria Naveillán, Alejandra Placencia y Diego Schalper. **(10-0-0)**

***

Se da lectura al artículo 16 del proyecto de ley:

“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.”.

Al artículo 16, el **diputado señor Diego Schalper, presentó la siguiente indicación:**

“Intercalar en el inciso segundo, entre la frase “sociedad civil” y “quienes permanecerán”, la siguiente frase: “cuyo objeto o razón social se refiera a materias de esta ley”

El **diputado señor Diego Schalper**, propone esta indicación porque le preocupa que el concepto de “organizaciones de la sociedad civil” quede así de general y amplio, por ello es preferible acotarlo a que tengan como objeto materias propias de esta ley.

Puesto en votación el **artículo 16 del texto del proyecto junto a la indicación del diputado Diego Schalper, se aprueba por unanimidad**. Votan a favor las y los diputado señores Jorge Alessandri, Jaime Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal, Andrés Longton (presidente), Gloria Naveillán, Alejandra Placencia y Diego Schalper. **(10-0-0)**

***

Se da lectura al artículo 17 del proyecto de ley:

“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.”

Puesto en votación el **artículo 17 del texto del proyecto, se aprueba por unanimidad.** Votan a favor las y los diputado señores Jorge Alessandri, Jaime Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal, Andrés Longton (presidente), Gloria Naveillán, Alejandra Placencia y Diego Schalper. **(10-0-0)**

***

Se da lectura al artículo 18 del proyecto de ley:

“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 sólo por el tiempo que falte para completar el período del consejero reemplazado.”

Puesto en votación el **artículo 18 del texto del proyecto, se aprueba por unanimidad.** Votan a favor las y los diputado señores Jorge Alessandri, Jaime Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal, Andrés Longton (presidente), Gloria Naveillán, Alejandra Placencia y Diego Schalper. **(10-0-0)**

***

Se da lectura al artículo 19 del proyecto de ley:

“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 el funcionamiento de la RCSE y las obligaciones especiales de los organismos de la Administración del Estado.”.

Al artículo 19, los diputados señores **José Miguel Castro, Andrés Longton y Diego Schalper, presentaron la siguiente indicación:**

“Suprímase el artículo 19.”

Los autores de la indicación la **retiran.**

El **diputado señor Diego Schalper,** consultó al Ejecutivo, por qué considerar en este artículo únicamente a los organismos de la Administración del Estado debiendo ser, según su parecer, a los organismos del Estado, como el poder legislativo y el poder judicial, y no solo al Ejecutivo.

La **asesora legislativa del Ministerio del Interior, señora Michelle Bordachar**, respondió señalando que se explicita así para resguardar la independencia de los distintos órganos del Estado, sin perjuicio que si el poder legislativo o el judicial lo quisiesen hacer pueden hacerlo vía convenios como lo establece el mismo artículo.

Puesto en votación el **artículo 19 del texto del proyecto, se aprueba por unanimidad.** Votan a favor las y los diputado señores Jorge Alessandri, Jaime Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal, Andrés Longton (presidente), Gloria Naveillán, Alejandra Placencia y Diego Schalper. **(10-0-0)**

***

Se da lectura al artículo 20 del proyecto de ley:

“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 éstos 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 éstos.

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.”

La **diputada señora Gloria Naveillán**, le consultó al Ejecutivo sobre las implicancias del término “significativo” que, en este artículo y otros, dentro de esta ley, se utiliza ya que así sin definición queda muy amplio.

El **diputado señor Diego Schalper**, en el mismo tenor que la consulta anterior, preguntó al Ejecutivo, sobre el significado de la frase “respuesta rápida”, para evitar que esto quede en manos de la administración de los jueces, generando con ello incerteza jurídica.

El **diputado señor José Miguel Castro**, sugirió, en relación con las consultas previas, dejar este tipo de precisiones en un reglamento.

El **presidente diputado señor Andrés Longton**, agregó que la letra b) del artículo 20 dice relación directamente con lo que se discutirá más adelante sobre CSIRT por lo que su votación debería quedar pendiente.

La **asesora legislativa del Ministerio del Interior, señora Michelle Bordachar**, respondió señalando que la expresión "significativo" es explicado en el artículo 23 de esta ley, y sobre la frase "respuesta rápida", efectivamente puede ser materia de ley. Por último, en cuanto a dejar pendiente la votación de la letra b) del artículo 20, sugiere que debiera quedar pendiente tal como lo expresó el presidente.

Puesto en votación el **artículo 20 del texto del proyecto, excluyendo la letra b), se aprueba por unanimidad.** Votan a favor las y los diputado señores Jorge Alessandri, Jaime Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal, Andrés Longton (presidente), Gloria Naveillán, Alejandra Placencia y Diego Schalper. **(10-0-0). Queda pendiente discutir y votar la letra b).**

***

Se da lectura al artículo 25 del proyecto de ley:

"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."

Puesto en votación el **artículo 25 del texto del proyecto, se aprueba por unanimidad.** Votan a favor las y los diputado señores Jorge Alessandri, Jaime Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal, Andrés Longton (presidente), Gloria Naveillán, Alejandra Placencia y Diego Schalper. **(10-0-0)**

***

Se da lectura al artículo 26 del proyecto de 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.”.

Puesto en votación el **artículo 26 del texto del proyecto, se aprueba por unanimidad.** Votan a favor las y los diputado señores Jaime Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal, Andrés Longton (presidente), Gloria Naveillán, Alejandra Placencia y Diego Schalper**. (9-0-0)**

***

Se da lectura al artículo 28 del texto del proyecto aprobado por el Senado:

“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.”

El **diputado señor Jorge Alessandri**, consultó al Ejecutivo, sobre la redacción del artículo y sus consecuencias, ya que solo establece que se reportará en casos que no se ponga en riesgo la seguridad y la defensa nacional, entonces, ¿qué ocurre en aquellos casos en que sí corre riesgo la seguridad y defensa nacional? ¿no se va a reportar?

La **asesora legislativa del Subsecretario de Interior, la abogada señora Michelle Bordachar**, respondió señalando que en aquellos casos en que sí se pueda poner en riesgo la seguridad nacional, es importante mantener esa información lo más limitado posible en cuanto a las personas que pueden tener acceso a ella y, por lo tanto, es una práctica común que no se traspase información a otros organismos que están fuera de la defensa, por eso se toma esa decisión. La Agencia, expresó, realiza consejos para evaluar la situación, pero sin recepción de información ya que no puede quedar en la Agencia, solo en poder de Defensa, por un tema de seguridad.

El **diputado señor Raúl Leiva**, manifestó que es una constante que cuando no se establece una obligación simplemente no se cumple, y la problemática del *accontability* es que efectivamente lo hagan, de lo contrario queda el accionar supeditado única y exclusivamente a la discrecionalidad de la autoridad de turno, entonces.

Por lo anterior, sugirió que la obligación de informar cualquier incidente, si perjuicio que esa información sea reservada, debe quedar establecido sino en la ley, en su reglamento, pero de alguna manera hay que cautelar aquello, a juicio de quien lo tiene a su cargo.

Al **artículo 28,** los diputados señores Jorge Alessandri, Henry Leal, Raúl Leiva y Andrés Longton, presentaron **la siguiente indicación:**

“Reemplácese el punto final del párrafo final por una coma, agregando luego de ella, la siguiente frase: según lo determine el reglamento.”

Puesto en votación el **artículo 28, con la indicación de los diputados señores Alessandri, Leal, Leiva y Longton, se aprueba por unanimidad.** Votan a favor los diputados Jorge Alessandri, Henry Leal y Andrés Longton (presidente), y la diputada señorita Alejandra Placencia. **(4-0-0).**

***

Se da lectura al artículo 30 del texto del proyecto aprobado por el Senado:

“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.”

Puesto en votación el **artículo 30, se aprueba por unanimidad.** Votan a favor los diputados Jorge Alessandri, Henry Leal y Andrés Longton (presidente), y la diputada señorita Alejandra Placencia. **(4-0-0).**

***

Se da lectura al artículo 32 del texto del proyecto aprobado por el Senado:

“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.”

Puesto en votación el **artículo 32, se aprueba por unanimidad**. Votan a favor los diputados Jorge Alessandri, Henry Leal y Andrés Longton (presidente), y la diputada señorita Alejandra Placencia. **(4-0-0).**

***

Se da lectura al artículo 35 del texto del proyecto aprobado por el Senado:

“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.

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."

Al **artículo 35**, el diputado señor Jorge Alessandri, presentó **las siguientes indicaciones N°s 84, 85 y 86:**

"En el artículo 35 inciso primero del proyecto de ley, para sustituir en su parte final, el párrafo "El reclamo deberá interponerse dentro de los quince días hábiles siguientes a la notificación de la resolución impugnada, según las siguientes reglas:", por el siguiente: "El reclamo deberá interponerse dentro de los quince días hábiles siguientes a la notificación de la resolución impugnada, los que deberán computarse de acuerdo al artículo 25 de la ley N°19.880, según las siguientes reglas:"

"En el artículo 35 literal b) del proyecto de ley, para sustituir la frase "le produzca", por la siguiente "pueda ocasionar".

"En el artículo 35 literal h) del proyecto de ley, para sustituir la frase "no procederá recurso alguno", por la siguiente "se podrá apelar ante la Corte Suprema, dentro del plazo de diez días hábiles, la que resolverá en cuenta".

El **Subsecretario del Interior, señor Manuel Monsalve,** manifestó en representación del Ejecutivo estar de acuerdo con los propuesto por el diputado Alessandri.

Puesto en votación el **artículo 35, con las indicaciones 84, 85 y 86 presentadas por el diputado Alessandri, se aprueba por unanimidad.** Votan a favor los diputados Jorge Alessandri, Henry Leal y Andrés Longton (presidente) Diego Schalper, y la diputada señorita Alejandra Placencia. **(5-0-0).**

***

Se da lectura al artículo 39 del texto del proyecto aprobado por el Senado:

"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 ésta 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."

Al **artículo 39**, el Ejecutivo presentó la **siguiente indicación N°18**:

"Para suprimir los literales d) y e), del artículo 39, readecuándose el orden correlativo de los literales siguientes."

Puesto en votación el **artículo 39, con la indicación N°18 presentada por el Ejecutivo, se aprueba por unanimidad.** Votan a favor los diputados Jorge Alessandri, Henry Leal y Andrés Longton (presidente) Diego Schalper, y la diputada señorita Alejandra Placencia. **(5-0-0).**

***

Se da lectura a los artículos 40, 41, 42 y 43 del texto del proyecto aprobado por el Senado:

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

a) Por el Subsecretario del Interior o quien éste designe.
b) Por el Subsecretario de Defensa o quien éste designe.
c) Por el Subsecretario de Relaciones Exteriores o quien éste designe.
d) Por el Subsecretario General de la Presidencia o quien éste designe.
e) Por el Subsecretario de Telecomunicaciones o quien éste designe.
f) Por el Subsecretario de Hacienda o quien éste designe.
g) Por el Subsecretario de Ciencia, Tecnología, Conocimiento e Innovación o quien éste 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."."

Puestos en una sola votación **los artículos 40, 41, 42 y 43, se aprueban por unanimidad.** Votan a favor los diputados Jorge Alessandri, Henry Leal y Andrés Longton (presidente) Diego Schalper, y la diputada señorita Alejandra Placencia. **(5-0-0).**

****

Continuación de la discusión y votación del artículo 2º, que tenía numerales pendientes por votar:

Al artículo 2, **la y los diputados señores Cristián Araya, Jaime Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal y Andrés Longton, formularon la siguiente indicación:**

"Para reemplazar los numerales 5 a 27 del artículo 2º por los siguientes:

5. Ciberataque: "intento de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático."

6. 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.

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

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

9. 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.

10. 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 de los procesos ejecutados o implementados en las redes y sistemas informáticos.

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

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

13. 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.

14. 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.

15. Vulnerabilidad: debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas."

La **asesora legislativa del Ministerio del Interior, abogada señora Michelle Bordachar**, señaló que esta indicación resultó gracias a un acuerdo con la mesa técnica de trabajo con los asesores parlamentarios y opiniones de expertos, de reducir el número de definiciones, concentrándose en conceptos a utilizarse a lo largo de la ley y que no sean de aquellos que sufran cambios en el tiempo, y sean netamente técnicas.

Puesta en votación **la indicación que modifica el artículo 2, se aprueba por unanimidad**. Votan la y los diputados señores Jaime Araya, Cristián Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal y Andrés Longton (presidente). **(7-0-0)**

En consecuencia, se rechazan los numerales 5 al 37 del artículo 2º del proyecto.

Al artículo 2, el diputado señor Andrés Jouannet, formuló la siguiente indicación:

“Suprímase el numeral 1 del inciso primero del artículo 2° propuesto**.”**

Su autor **la retira.**

Al artículo 2, el diputado señor Andrés Jouannet, formuló la siguiente indicación:

“Suprímase el numeral 4 del inciso primero del artículo 2° propuesto.”

Su autor **la retira.**

Al artículo 2, el diputado señor Jorge Alessandri, formuló la siguiente indicación N°8:

“En el artículo 2° numeral 5 del proyecto de ley, para sustituirlo por el siguiente: “5. Autoridad sectorial: aquellos servicios públicos dotados de facultades regulatorias, fiscalizadoras y sancionatorias respecto de sus regulados.”.

Por haberse aprobado la indicación que reemplaza los numerales 5 a 27 del artículo 2**, reglamentariamente esta se rechaza**.

Al artículo 2, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°9:

“Sustitúyese el numeral 5 del artículo 2°, por el siguiente: “5. Autoridad sectorial: aquellos servicios públicos cuya finalidad es la regulación y/o supervigilancia de un determinado sector de la economía o de actividades realizadas por particulares en ejercicio de la libertad económica.”

Por haberse aprobado la indicación que reemplaza los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza.**

Al artículo 2, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°10:

“Suprímanse los numerales 7 y 8 del artículo 2°.”

Sus autores **la retiran.**

Al artículo 2, el diputado señor Andrés Jouannet, formuló la siguiente indicación:

“Suprímase el numeral 8 del inciso primero del artículo 2° propuesto.”

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza.**

Al artículo 2, el diputado señor Andrés Jouannet, formuló la siguiente indicación:

“Suprímase el numeral 10 del inciso primero del artículo 2° propuesto.”

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza.**

Al artículo 2, el diputado señor Andrés Jouannet, formuló la siguiente indicación:

“Suprímase el numeral 11 del inciso primero del artículo 2° propuesto.”

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza.**

Al artículo 2, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°11:

“En el numeral 13 del artículo 2°, intercálase entre la palabra “competente” y la frase “de conformidad”, entre comas, lo siguiente: “en el ámbito de sus respectivas competencias”.

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza.**

Al artículo 2, el diputado señor Andrés Jouannet, formuló la siguiente indicación:

“Suprímase el numeral 16 y 17 del inciso primero del artículo 2° propuesto.”

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza.**

Al artículo 2, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°12:

“Suprímanse el numerales 17 del artículo 2°.”

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza.**

Al artículo 2, el diputado señor Jorge Alessandri, formuló la siguiente indicación N°13:

“En el artículo 2 numeral 17 del proyecto de ley, para suprimirlo.”

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza.**

Al artículo 2, el diputado señor Cristián Araya, formuló la siguiente indicación:

“Para suprimir en el numeral 17 la expresión: “imposibles de lograr de forma independiente”.”.

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2**, reglamentariamente esta se rechaza.**

Al artículo 2, el diputado señor Andrés Jouannet, formuló la siguiente indicación:

"Suprímase el numeral 18 del inciso primero del artículo 2° propuesto."

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2**, reglamentariamente esta se rechaza.**

Al artículo 2, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°14:

"Sustitúyese el numeral 18 del artículo 2°, por el siguiente:

"18. Interoperabilidad: capacidad de los sistemas informáticos de ser capaces de interactuar y operar entre sí, a través de estándares abiertos que permitan una segura y expedita interconexión entre ellos."

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2**, reglamentariamente esta se rechaza.**

Al artículo 2, el diputado señor Jorge Alessandri, formuló la siguiente indicación N°15:

En el artículo 2° numeral 18 del proyecto de ley, para añadir después del punto aparte, que pasa ser una coma "," la siguiente frase: "con pleno respeto de las normas sobre protección de datos personales".

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza.**

Al artículo 2, el diputado señor Andrés Jouannet, formuló la siguiente indicación:

"Suprímase el numeral 19 del inciso primero del artículo 2° propuesto."

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza.**

Al artículo 2, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°16:

Sustitúyese el numeral 20 del artículo 2°, por el siguiente:

"20. Operadores de importancia vital: son operadores de importancia vital los organismos de la Administración del Estado, el Coordinador Eléctrico Nacional, aquellos agentes privados de los sectores de energía, servicios sanitarios; telecomunicaciones, servicios postales y mensajería; transporte, banca, infraestructura de los mercados financieros, infraestructura digital, gestión de servicios de tecnologías de la información, determinados como tales por el procedimiento del artículo 4º, así como otros que, en virtud del mismo procedimiento, deban tener tal calidad, siempre que dependan de las redes y sistemas informáticos para su funcionamiento y su afectación, interceptación, interrupción o destrucción puede tener un impacto crítico en la seguridad nacional, en la seguridad interior y el orden público, en la provisión continua y regular de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que éste debe proveer o garantizar."

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza.**

Al artículo 2, el diputado señor Andrés Jouannet, formuló la siguiente indicación:

Reemplácese la expresión “tener una repercusión importante en” por “amenazar”.

Incorpórese luego de “actividades sociales o económicas cruciales,”, la expresión “en alguno de los sectores o subsectores regulados de alta criticidad para el país establecidos o identificados en conformidad con la presente ley”,

Suprímase la expresión “, en general, de”.

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza.**

Al artículo 2, el diputado señor Jorge Alessandri, formuló la siguiente indicación N°17:

En el artículo 2° numeral 20 del proyecto de ley, para sustituirlo por el siguiente:

“20. Operadores de importancia vital: son tales los órganos de la Administración del Estado, las empresas del Estado y sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio, y aquellos agentes privados que así sean calificados por la Agencia de conformidad con esta ley, cuyo funcionamiento dependa de las redes y sistemas informáticos, y siempre que su afectación, interceptación, interrupción o destrucción pueda producir graves efectos en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que éste debe proveer o garantizar.”.

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza.**

Al artículo 2, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°18:

Sustitúyase, en el numeral 24 del artículo 2°, la frase “sometido a la supervigilancia de un órgano público con facultades suficientes para regular, fiscalizar y eventualmente sancionar” por “bajo la regulación y/o supervigilancia de una autoridad sectorial”.

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza**.

Al artículo 2, el diputado señor Jorge Alessandri, formuló la siguiente indicación N°19:

Para suprimir, en el numeral 24 del artículo 2°, la palabra “eventualmente”.

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza.**

Al artículo 2, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°20:

Sustitúyase el numeral 25 del artículo 2°, por el siguiente:

"25. Servicios esenciales: son servicios esenciales aquellos provistos por los organismos de la Administración del Estado, por el Coordinador Eléctrico Nacional y por aquellos agentes privados de los sectores de energía, servicios sanitarios; telecomunicaciones, servicios postales y mensajería; transporte, banca, infraestructura de los mercados financieros, infraestructura digital, gestión de servicios de tecnologías de la información y de otros que se determinen en virtud del procedimiento del artículo 4º, cuya afectación, de cualquier manera, cause un grave daño a la salud o al abastecimiento de la población, a actividades económicas esenciales, al medioambiente o a la seguridad del país."

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza**.

Al artículo 2, el diputado señor Jorge Alessandri, formuló la siguiente indicación N°21:

En el artículo 2° numeral 25 del proyecto de ley, para sustituir la frase "tendría", por la siguiente: "pueda producir".

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza.**

Al artículo 2, el diputado señor Andrés Jouannet, formuló la siguiente indicación:

"Artículo 2° N°25°. Servicios Esenciales. Todo servicio identificado como tal de conformidad con el procedimiento establecido en el artículo 4° de la presente ley, que se provea o preste en sectores o subsectores regulados de alta criticidad para el país, incluyendo los sectores de energía y combustibles, sanitario, salud, telecomunicaciones, transporte, bancario y financiero, así como por la administración del Estado, el Poder Legislativo y el Poder Judicial".

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza.**

Al artículo 2, el diputado señor Andrés Jouannet, formuló la siguiente indicación:

"Suprímase en el artículo 2° Numeral N°26 propuesto."

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza.**

Al artículo 2, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°22:

Incorpórese un nuevo numeral 28 al artículo 2°, del siguiente tenor:

"28. Consulta pública y recepción de observaciones: proceso participativo en cuya virtud antes de la emisión de un acto administrativo, éste se da a conocer públicamente, por medios digitales; se disponen los mecanismos necesarios para que los interesados puedan formularle observaciones; y se publican tanto las observaciones como las respuestas de la autoridad a ellas."

Por haberse aprobado la indicación que reemplazar los numerales 5 a 27 del artículo 2, **reglamentariamente esta se rechaza.**

***

Se da lectura al artículo 3 aprobado por el Senado:

"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 éstos, sólo 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."

Al artículo 3, **los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°23:**

Para sustituir el artículo 3º por el siguiente:

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

1. Principio de subsidiariedad regulatoria. Si una autoridad sectorial dicta normativa más exigente que la contemplada en esta ley, se preferirá aquella por sobre ésta;

2. Principio de especialidad sectorial. Frente a la existencia de una autoridad sectorial que cuente con atribuciones establecidas por ley en el ámbito regulatorio, supervisor y sancionatorio, se respetará la prevalencia de las potestades sectoriales en cada caso, en el ámbito de sus competencias. En caso de duda, se privilegiará a la autoridad sectorial respectiva.

3. Principio de coordinación. De conformidad a lo dispuesto por el inciso segundo del artículo 5º del DFL Nº1-19.653 que fija texto refundido, coordinado y sistematizado de la ley Nº18.575, orgánica constitucional de Bases Generales de la Administración del Estado, la Agencia y las autoridades sectoriales deberán cumplir sus cometidos coordinadamente y propender a la unidad de acción, evitando la duplicación o interferencia de funciones.

Asimismo, para la dictación de actos administrativos, se tendrá especialmente en cuenta lo dispuesto por el artículo en el artículo 37 bis de la Ley Nº19.880 que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.”

Al artículo 3, **el diputado señor Jorge Alessandri, formuló la siguiente indicación N°24:**

“Para sustituir, en el numeral 6 del artículo 3°, la frase “niñas, niños, jóvenes, personas de la tercera edad y disidencias sexogenéricas”, por la siguiente: “niños, niñas y adolescentes y personas de la tercera edad”.”.

Al artículo 3, **los diputados señores Jorge Alessandri, José Miguel Castro y Andrés Longton, formularon la siguiente indicación sustitutiva:**

“Para reemplazar el artículo 3 por el siguiente:

“Artículo 3. Principios rectores. Para alcanzar los objetivos de esta ley se deberán observar los siguientes principios:

1. Principio de control de daños: frente a un ciberataque o a un incidente de ciberseguridad siempre se deberá actuar coordinada y diligentemente, adoptando las medidas necesarias para evitar la escalada del ciberataque o del incidente de ciberseguridad y su posible propagación a otros sistemas informáticos.

2. Principio de cooperación con la autoridad: para resolver los incidentes de ciberseguridad se deberá prestar la cooperación debida con la autoridad competente y, si es necesario, cooperar entre diversos sectores, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios.

3. Principio de coordinación: de conformidad a lo dispuesto por el inciso segundo del artículo 5º del DFL Nº1-19.653 que fija texto refundido, coordinado y sistematizado de la ley Nº18.575, orgánica constitucional de Bases Generales de la Administración del Estado, la Agencia y las autoridades sectoriales deberán cumplir sus cometidos coordinadamente y propender a la unidad de acción, evitando la duplicación o interferencia de funciones.

4. Principio de seguridad en el ciberespacio: es deber del Estado resguardar la seguridad en el ciberespacio. El Estado velará porque todas las personas puedan participar de un ciberespacio seguro otorgando especial protección a las redes y sistemas informáticos que contengan información de aquellos grupos de personas que suelen ser en mayor medida objeto de ciberataques.

5. 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.

6. Principio de seguridad informática: toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere necesarias, incluyendo el cifrado.

7. Principio de racionalidad: las medidas para la gestión de incidentes de ciberseguridad, las obligaciones de ciberseguridad y el ejercicio de las facultades de la Agencia deberán ser necesarias y proporcionales al grado de exposición a los riesgos, así como al impacto social y económico que tendría.

8. Principio de seguridad y privacidad por defecto y desde el diseño: Los sistemas informáticos, aplicaciones y tecnologías de la información deben diseñarse, implementarse y gestionarse teniendo en cuenta la seguridad y la privacidad de los datos personales que procesan.”.”

La **asesora legislativa del Ministerio del Interior, abogada señora Michelle Bordachar,** precisó que esta redacción viene a recoger lo sugerido en su oportunidad tanto por la mesa técnica de trabajo como los expertos, dejando en su mayoría principios que venían en el mensaje del presidente Sebastián Piñera, que en gran parte fueron tomados de la ley de Estonia en la materia, procurando dejar solamente los principios que no contenían obligaciones o derechos, entendiendo que se trata solo de eso, de principios. Añadió, que se incorporaron, a la redacción del mensaje, el principio de seguridad y privacidad; el de racionalidad, respecto a la exposición de los regulados y sus capacidades económicas para cumplir con las obligaciones que ley establece, y el de seguridad informática, para que todas las personas puedan gozar de un ciberespacio seguro.

Puesta en votación **la indicación sustitutiva al artículo 3, de los diputados señores Jorge Alessandri, José Miguel Castro y Andrés Longton, se aprueba por unanimidad.** Votan a favor las y los diputados señores Jorge Alessandri, José Miguel Castro, Lorena Fries, Andrés Longton (presidente) y Alejandra Placencia. Sin votos en contra ni abstenciones. **(5-0-0).**

Por aprobarse recientemente la indicación sustitutiva del artículo 3, **reglamentariamente se rechazan, el artículo 3 aprobado por el Senado y las indicaciones N°s 23 y 24.**

***

Se de lectura al artículo 4 del proyecto de ley:

“Artículo 4°. Determinación de los servicios esenciales e identificación de los operadores de importancia vital. En el ejercicio de la facultad establecida en la letra g) del artículo 9° de esta ley, la Agencia determinará aquellos servicios que sean considerados esenciales para los efectos de esta ley, y dentro de éstos 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 éstos, 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 contado 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.

Al artículo 4, el Ejecutivo formuló la siguiente indicación:

“Para reemplazar el artículo 4, por el siguiente:

“Artículo 4.- Ámbito de aplicación. La presente ley se aplicará a las instituciones que presten servicios calificados como esenciales según lo establecido en los

incisos segundo y tercero de este artículo y a aquellas que sean calificadas como operadores de importancia vital, de conformidad con lo dispuesto en los artículos 5 y 6 de esta ley.

Son servicios esenciales aquellos provistos por los organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional; los prestados bajo concesión de servicio público; y los proveídos por instituciones privadas que realicen las siguientes actividades: generación, transmisión o distribución eléctrica; transporte, almacenamiento o distribución de combustibles; suministro de agua potable o saneamiento; telecomunicaciones; infraestructura digital; servicios de tecnología de la información gestionados por terceros; transporte terrestre, aéreo, ferroviario o marítimo, así como la operación de su infraestructura respectiva; banca, servicios financieros y medios de pago; administración de prestaciones de seguridad social; servicios postales y de mensajería; prestación institucional de salud por entidades tales como hospitales, clínicas, consultorios y centros médicos; y la producción y/o investigación de productos farmacéuticos.

La Agencia podrá calificar otros servicios como esenciales mediante resolución fundada del o la Directora Nacional cuando su afectación puede causar un grave daño a la vida o integridad física de la población o a su abastecimiento, a sectores relevantes de las actividades económicas, al medioambiente, al normal funcionamiento de la sociedad, de la Administración del Estado, a la defensa nacional, o a la seguridad y el orden público.

Dicha calificación deberá someterse al proceso de consulta pública y se regirá por las disposiciones de la ley Nº19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.”.”

La **asesora legislativa del Ministerio del Interior, abogada señora Michelle Bordachar,** señaló que esta indicación obedece a la recomendación de los expertos y de la Unión Europea, por cuanto se debe establecer cuáles son los servicios esenciales a los que se le aplicará a la ley.

Los diputados señores Cristián Araya y Andrés Jouannet, expresaron su preocupación de establecer una norma tan abierta respecto de los alcances de aplicación de la ley en consideración a los servicios esenciales y operadores de importancia vital, faltaría explicitar los estándares o calificaciones a considerar para que se les aplique, de lo contrario el solo hecho de fijar un listado de sector del rubro a aplicárseles la ley no es suficiente.

El **abogado señor Claudio Magliona**, indicó que, si bien esta indicación es un avance a lo original en este tema, aun así consideró ser muy amplia, ya que en el listado se establece el rubro como por ejemplo “empresas de tecnología de la información” lo cual es muy extenso, por lo que recomendó, más allá de fijar la materia o rubro de la empresa esencial, es necesario establecer la calificación de estas, muy similar a uno de los incisos propuestos en la indicación original del Ejecutivo.

La **asesora legislativa del Ministerio del Interior, abogada señora Michelle Bordachar,** sugirió agregar como inciso final a esta nueva indicación que reemplaza el artículo 4, para subsanar lo antes expuesto, el inciso segundo de la indicación N°19 formulada por el Ejecutivo, que reza lo siguiente: “La Agencia identificará, mediante resolución exenta dictada conforme el procedimiento dispuesto en el artículo 4, las infraestructuras, procesos o funciones específicas que serán calificadas como esenciales, y que quedarán sujetas a las obligaciones establecidas en el artículo 8.”

Luego, se da lectura a la indicación N° 19 del Ejecutivo, específicamente a lo señalado en el punto 12:

“La Agencia identificará, mediante resolución exenta dictada conforme el procedimiento dispuesto en el artículo 4° de esta ley, las infraestructuras, procesos o funciones específicas que serán calificadas como esenciales, y que quedarán sujetas a las obligaciones establecidas en el artículo 6° (8º) de esta ley.

Puesta en votación **la indicación del Ejecutivo que reemplaza el artículo 4° en conjunto con el punto 12 de la indicación N° 19 del Ejecutivo, se aprueban por unanimidad**. Votan la y los diputados señores Jaime Araya, Cristián Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal y Andrés Longton (presidente). **(7-0-0)**

En consecuencia, se rechaza reglamentariamente el artículo 4º del proyecto.

Al inciso primero del artículo 4, el Ejecutivo formuló la siguiente indicación N°3:

Para reemplazar en el artículo 4°, el inciso primero por el siguiente:

“Artículo 4°. Identificación de los operadores de importancia vital. En el ejercicio de la facultad establecida en el literal g) del artículo 9° de esta ley, la Agencia determinará los operadores de importancia vital dentro de los servicios esenciales identificados en el Título IX, conforme los siguientes criterios y procedimiento:”.

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al inciso primero del artículo 4, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°25:

Sustitúyase, en el inciso primero del artículo 4° la frase “En el ejercicio de la facultad establecida en la letra g) del artículo 9° de esta ley” por la frase “Cada dos años”.

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al inciso segundo del artículo 4, el Ejecutivo formuló la siguiente indicación N°4:

Para suprimir en el artículo 4°, el inciso segundo, readecuando el orden correlativo de los incisos siguientes.

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al inciso segundo del artículo 4, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°26:

Reemplázase el inciso segundo del artículo 4° por el siguiente:

“Para determinar los servicios provistos por agentes privados que deben calificarse como esenciales, se deberá considerar fundadamente:

a) Lo dispuesto en el numeral 25 del artículo 2º de esta ley;

b) La gravedad del daño que la afectación, interceptación, interrupción o destrucción del servicio podría causar a la vida o integridad física de las personas, al abastecimiento de la población, a las actividades económicas, a la defensa nacional, al normal funcionamiento de la sociedad, al medioambiente o a la seguridad del país;

c) La condición de prestarse el servicio bajo concesión de servicio público;

d) La posibilidad de sustitución del servicio, tal que ello no implique perturbación en su acceso;

e) La magnitud de los usuarios en relación al área o sector que se verían afectados en caso de afectarse, interceptarse, interrumpirse o destruirse el servicio;

f) De modo general, el grado de afectación del normal desarrollo y bienestar de la población."

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al inciso segundo del artículo 4, el diputado señor Andrés Jouannet, formuló la siguiente indicación:

Reemplácese el inciso segundo del artículo 4° propuesto por el siguiente:

"A fin de determinar qué servicios resultan esenciales para efectos de esta ley, la Agencia deberá:

a) Identificar los sectores o subsectores regulados de alta criticidad que son cruciales para mantener actividades sociales y económicas vitales, y determinar los servicios que se presten en estos.

b) Evaluar el eventual impacto que la falta, interrupción o afectación de estos servicios podría tener en la defensa nacional, la seguridad pública, el bienestar económico y social, otros sectores o subsectores regulados de alta criticidad y los servicios públicos que el Estado debe proveer o garantizar.

c) Considerar la presencia o uso de infraestructura crítica de la información necesaria para proporcionar los servicios en los sectores o subsectores identificados en virtud de esta ley.

d) Que la magnitud del eventual impacto sea de tal gravedad como para: causar daños catastróficos en la salud o víctimas masivas; obstaculizar u impedir el ejercicio de las facultades de los organismos de la administración del Estado u otros Poderes del Estado; poner en riesgo gravemente el orden y la seguridad pública; impedir el ejercicio legítimo de los derechos fundamentales de las personas garantizados por la Constitución Política de la República; o afectar negativamente la confianza o legitimidad de la institucionalidad pública".

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al inciso segundo del artículo 4, el diputado señor Cristián Araya, formuló la siguiente indicación:

Para sustituirlo por el siguiente: "a fin de determinar qué servicios resultan esenciales, se deberá atender a la entidad del impacto o interrupción podría poner en grave riesgo la seguridad, el orden público, la defensa nacional, la vida de las personas o que estas puedan ejercer sus derechos fundamentales"

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente se rechaza.**

Al inciso tercero del artículo 4, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°27:

Reemplázase el inciso tercero del artículo 4° por los siguientes incisos tercero, cuarto y quinto nuevos:

"Para determinar que agentes privados prestadores esenciales tienen la calidad de operador de importancia vital, se deberán reunir los siguientes requisitos:

a) La prestación de dicho servicio depende para su provisión de las redes y sistemas informáticos; y

b) La afectación, interceptación, interrupción o destrucción del servicio puede tener un impacto crítico en la seguridad nacional, en la seguridad interior y el orden público, en la provisión continua y regular de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que éste debe proveer o garantizar.

Además, podrán tener la calidad de operador de importancia vital aquellos agentes privados que, aun cuando no tengan la calidad de prestadores de servicios esenciales, reúnan los requisitos indicados en el inciso anterior y su inclusión sea indispensable, por motivos fundados, por haber adquirido un rol crítico para el abastecimiento por la población, la distribución de bienes o la producción de aquellos indispensables o estratégicos para el país.

En cualquier caso, siempre se deberá tener en consideración el tamaño del agente privado, teniendo especialmente en consideración las características y necesidades de las micro, pequeñas y medianas empresas, tal como se definen en la ley N°20.416, que fija normas especiales para las empresas de menor tamaño.

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al inciso tercero del artículo 4, el diputado señor Andrés Jouannet, formuló la siguiente indicación:

Intercálese un nuevo literal d) en el inciso tercero del artículo 4° propuesto del siguiente tenor:

"d) El tamaño del operador, teniendo especialmente en consideración las características y necesidades de las micro, pequeñas y medianas empresas, tal como se definen en la ley N°20.416, que fija normas especiales para las empresas de menor tamaño".

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al inciso tercero del artículo 4, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°28:

Introdúcense las siguientes modificaciones al inciso cuarto del artículo 4° que ha pasado a ser sexto:

i. Intercálase un nuevo literal c), pasando el actual c) a ser d), del siguiente tenor:

"c) El grado de exposición de la entidad a los riesgos, la probabilidad de que se produzcan incidentes de ciberseguridad y su gravedad, incluidas sus repercusiones sociales y económicas."

ii. Suprímese el literal h).

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al inciso tercero del artículo 4, el diputado señor Jorge Alessandri, formuló las siguientes indicaciones 29 y 30:

Para sustituir la frase “la identificación de” por la siguiente palabra: “identificar”.

En el literal c) del proyecto de ley, para sustituir la palabra “tendría”, por la siguiente: “podría producir”.

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, r**eglamentariamente esta se rechaza.**

Al inciso cuarto del artículo 4, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°31:

Introdúcense las siguientes modificaciones al inciso cuarto, que ha pasado a ser séptimo:

i. Reemplázase la oración “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 éstos, aquellos operadores que resultan de importancia vital para su provisión” por “Para dar cumplimiento a lo prescrito en este artículo, se observará rigurosamente lo dispuesto en el artículo 37 bis de la Ley Nº19.880 que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado”.

ii. Suprímase la oración “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.”

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al artículo 4, el diputado señor Andrés Jouannet, formuló la siguiente indicación:

Incorpórese un nuevo inciso quinto en el artículo 4° propuesto, pasando el actual a ser sexto y así sucesivamente, del siguiente tenor:

“Los factores anteriormente listados deberán ser ponderados en conjunto con criterios sectoriales atendiendo los sectores o subsectores regulados específicos de alta criticidad establecidos o identificados en conformidad a esta ley. Se deberán utilizar, al menos, los siguientes criterios sectoriales según corresponda:

a) La magnitud de los operadores identificados, por ejemplo, en términos de participación en el mercado. Para estos efectos, se podrán considerar factores tales como el volumen, proporción y número de operaciones de las entidades en periodos de tiempo a nivel nacional, regional o municipal.

b) La importancia sistémica, valorada según los activos totales o la razón entre estos y el producto interno bruto.

c) El tipo y número de usuarios o público específicos a los que van dirigidos los servicios”.

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al inciso quinto del artículo 4, el Ejecutivo formuló la siguiente indicación N°4:

Para modificar en el artículo 4°, el inciso quinto, que ha pasado a ser cuarto, en el siguiente sentido:

a. Reemplázase la frase “los servicios que deban calificarse como esenciales e identifique, para cada uno de éstos, aquellos operadores que resultan de importancia vital para su provisión” por la frase “las entidades que deban calificarse como operadores de importancia vital”.

b. Reemplázase la frase “podrá requerir informes similares a otros organismos públicos o instituciones privadas.” por la frase “deberá requerir informes similares a las autoridades sectoriales competentes y a las entidades que puedan ser calificadas como operadores de importancia vital.”

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al inciso quinto del artículo 4, el diputado señor Jorge Alessandri y la diputada señora Gloria Naveillán, formularon la siguiente indicación N°32:

Para insertar en el inciso quinto del artículo 4° y a continuación de la frase “de Inteligencia,” la siguiente frase “las Autoridades Sectoriales de cada uno de los sectores regulados”. En el mismo inciso y a continuación de la frase vital para su provisión… insertar como punto aparte lo siguiente “Dichos informes serán vinculantes para los efectos de las definiciones de los servicios esenciales que promulgue la Agencia”

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al inciso quinto del artículo 4, el diputado señor Cristián Araya, formuló la siguiente indicación:

Para agregar a continuación de la expresión “informe fundado”, la expresión “y de carácter secreto”.

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al inciso sexto y séptimo del artículo 4, el Ejecutivo formuló la siguiente indicación N°6:

Para reemplazar los incisos sexto y séptimo, del artículo 4°, que han pasado a ser quinto y sexto, por el siguiente inciso quinto y final:

“Transcurrido este plazo, con los antecedentes que hubiere recibido, la Agencia, mediante resolución fundada de su Director o Directora, determinará los operadores de importancia vital dentro de los servicios esenciales. Esta resolución quedará exenta del trámite de toma de razón de la Contraloría General de la República y contra ella procederá el recurso de reclamación judicial contemplado en el artículo 35 de la presente ley.”.

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al inciso quinto, sexto y séptimo del artículo 4, el diputado señor Andrés Jouannet, formuló la siguiente indicación:

“Reemplácese el inciso quinto, sexto y séptimo del artículo 4° propuesto, que han pasado a ser sexto, séptimo y octavo, respectivamente, por los siguientes incisos sexto, séptimo y octavo:

“La Agencia requerirá a la Agencia Nacional de Inteligencia un informe fundado que identifique aquellos operadores que resultan de importancia vital para la provisión de servicios esenciales identificados de conformidad a esta ley, y podrá requerir informes similares a otros organismos públicos o instituciones privadas. De igual manera, la Agencia requerirá informes fundados a las autoridades sectoriales que regulan, supervisan y fiscalizan los sectores o subsectores regulados de alta criticidad establecidos o determinados de conformidad con la presente ley, los que tendrán el carácter de vinculantes para la Agencia. 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 elaborará una primera propuesta de lista actualizada de operadores de importancia vital. Los posibles operadores de importancia vital que se encuentren en la primera propuesta serán notificados por la Agencia, y dispondrán de un plazo de treinta días hábiles a contar desde el día siguiente a la recepción de la notificación para remitir a la Agencia las alegaciones que considere procedentes, transcurrido el cual la Agencia dictará una resolución dentro un plazo de treinta días hábiles en el que podrá acoger o rechazar su inclusión como operador de importancia vital.

Luego de que la Agencia haya dictado las resoluciones acogiendo o rechazando, según corresponda, las alegaciones de los eventuales operadores de importancia vital de la primera propuesta, y hayan sido resueltas las reclamaciones judiciales que los posibles operadores de importancia vital hayan hecho valer contra estas resoluciones en virtud del procedimiento establecido en el artículo 35° de esta Ley, la Agencia propondrá una segunda propuesta de lista actualizada de posibles operadores de importancia vital al Comité Interministerial de Ciberseguridad para que, dentro del plazo de treinta días hábiles, se pronuncie fundadamente, pudiendo aprobar o sugerir las enmiendas que considere necesarias para su aprobación, las que serán comunicadas a la Agencia”.”.

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al inciso sexto del artículo 4, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°33:

Introdúcense las siguientes modificaciones al inciso cuarto, que ha pasado a ser séptimo:

i. Reemplázase la oración “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 éstos, aquellos operadores que resultan de importancia vital para su provisión” por “Para dar cumplimiento a lo prescrito en este artículo, se observará rigurosamente lo dispuesto en el artículo 37 bis de la Ley Nº19.880 que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado”.

ii. Suprímase la oración “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.”

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al inciso séptimo del artículo 4, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°34:

Introdúcense las siguientes modificaciones al inciso séptimo, que ha pasado a ser noveno:

i. Intercálase entre la coma que sigue a la palabra “Ciberseguridad” y la frase “el Ministerio”, lo siguiente: “procederá la interposición del recurso de reposición del artículo 59 de la ley Nº19.880 que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado, sin perjuicio de los demás que dicha ley y otros cuerpos legales autoricen, los cuales se regirán por los plazos establecidos en sus respectivas leyes. Encontrándose firme el acto”, seguido de una coma;

ii. Suprímase la oración “Este decreto quedará exento del trámite de toma de razón de la Contraloría General de la República.”

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al inciso sexto y séptimo del artículo 4, el diputado señor Jorge Alessandri formuló la siguiente indicación N°35:

Para sustituirlos por el siguiente inciso final:

“Transcurrido este plazo, con los antecedentes que hubiere recibido y mediante resolución fundada de su Director o Directora, la Agencia determinará los operadores de importancia vital dentro de los servicios esenciales. Contra esta resolución procederá el reclamo de ilegalidad contemplado en el artículo 35 de la presente ley”.

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al inciso final del artículo 4, el diputado señor Jorge Alessandri y la diputada señora Gloria Naveillán, formularon la siguiente indicación N°36:

Para reemplazar en el inciso final del artículo 4° la frase “quedará exento del” por “será sometido a”.

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Al artículo 4, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°37:

Para incorporar los nuevos incisos décimo, décimo primero y décimo segundo, del siguiente tenor:

“Podrá reclamarse de los fundamentos de hecho y Derecho del decreto señalado en el inciso precedente dentro del plazo de quince días hábiles ante la Corte de Apelaciones del domicilio del reclamante. La Corte dará traslado de la reclamación a la Agencia y ésta dispondrá del plazo de quince días hábiles contados desde que se notifique la reclamación interpuesta, para formular observaciones.

Evacuado el traslado por la Agencia, o vencido el plazo de que dispone para formular observaciones, el tribunal ordenará traer los autos en relación y la causa se agregará extraordinariamente a la tabla de la audiencia más próxima, previo sorteo de la Sala. La Corte podrá, si lo estima pertinente, abrir un término probatorio que no podrá exceder de siete días hábiles, y escuchar los alegatos de las partes.

La Corte dictará sentencia dentro del término de quince días. Contra la resolución de la Corte de Apelaciones se podrá apelar ante la Corte Suprema, dentro del plazo de diez días hábiles, la que conocerá en la forma prevista en los incisos anteriores."

Por haberse aprobado la indicación nueva del Ejecutivo que reemplaza el artículo 4, **reglamentariamente esta se rechaza.**

Posteriormente, se acuerda reabrir debate del artículo 4, respecto al ámbito de aplicación de la ley, para incorporar una indicación formulada por los diputados señores José Miguel Castro y Andrés Jouannet como inciso penúltimo del artículo 4, del siguiente tenor:

"Para incorporar el siguiente nuevo inciso penúltimo al artículo 4: En el caso del servicio esencial de telecomunicaciones previsto en este artículo, para efectos de esta ley, la calificación respecto de qué servicios, redes o elementos de red y sistemas específicos tendrán dicha calidad, se sujetará a la declaración mediante resolución fundada que realice la Subsecretaría de Telecomunicaciones conforme a lo señalado en la ley N°18.168"

La **asesora legislativa del Ministerio del Interior, abogada señora Michelle Bordachar,** indicó que, si solo se tratase de aquellas empresas proveedoras que prestan servicios de telecomunicaciones tales como Claro, Entel, Movistar y otros, dejando fuera a los de infraestructura, estarían de acuerdo, sin perjuicio que en caso de aprobarse sería solo para este sector, y la próxima semana se requerirá para otro sector, generando exclusiones sin justificación, por lo que sugirió se mantenga la norma como está actualmente.

Luego, indicó que, se conversó directamente con el gremio de las empresas de las telecomunicaciones al respecto y se llegó a la conclusión que la especialidad debe realizarse más bien en un artículo transitorio, dejando el artículo 4 original ya aprobado, con excepción a una sugerencia hecha por este gremio, que sería la de incorporar a los servicios digitales dentro de los servicios esenciales.

Acto seguido, los **diputados señores José Miguel Castro, Henry Leal, Andrés Longton y Diego Schalper,** formularon la siguiente indicación al texto del artículo 4, ya aprobado:

"Agregar al inciso segundo del artículo 4, aprobado, entre las frases "infraestructura digital" y "servicios de tecnología", la expresión "servicios digitales".

Puesta en votación **la indicación de los diputados señores José Miguel Castro y Andrés Jouannet, que modifica el artículo 4, se rechaza por unanimidad**. Sin votos a favor. Votan en contra los diputados señores José Miguel Castro, Henry Leal, Andrés Longton, Raúl Leiva y Diego Schalper. Sin abstenciones. **(0-5-0).**

Puesta en votación **la indicación de los diputados señores José Miguel Castro, Henry Leal, Andrés Longton y Diego Schalper, que modifica el artículo 4, se aprueba por unanimidad.** Votan a favor los diputados señores José Miguel Castro, Henry Leal, Andrés Longton, Raúl Leiva y Diego Schalper. Sin votos en contra ni abstenciones. **(5-0-0).**

***

El Ejecutivo formuló una indicación para intercalar los siguientes artículos 5 y 6, nuevos, pasando los actuales a ser 7 y 8, y así sucesivamente:

"**Artículo 5.-** Operadores de Importancia Vital. La Agencia establecerá mediante resolución dictada por el o la Directora Nacional, según se establece en el artículo

siguiente, a los prestadores de servicios esenciales que sean calificados como operadores de importancia vital.

La Agencia podrá calificar como operadores de importancia vital a quienes reúnan los siguientes requisitos:

1.- que la provisión de dicho servicio dependa de las redes y sistemas informáticos; y,

2.- que la afectación, interceptación, interrupción o destrucción de sus servicios tenga un impacto significativo en la seguridad y el orden público; en la provisión continua y regular de servicios esenciales; en el efectivo cumplimiento de las funciones del Estado; o, en general, de los servicios que éste debe proveer o garantizar.

Además, la Agencia podrá calificar como operadores de importancia vital a instituciones privadas que, aunque no tengan la calidad de prestadores de servicios esenciales, reúnan los requisitos indicados en el inciso anterior y cuya calificación sea indispensable por haber adquirido un rol crítico en el abastecimiento de la población, la distribución de bienes o la producción de aquellos indispensables o estratégicos para el país; o por el grado de exposición de la entidad a los riesgos y la probabilidad de incidentes de ciberseguridad, incluyendo su gravedad y las consecuencias sociales y económicas asociadas.

En cualquier caso, siempre se deberá tener en consideración el tamaño de la institución privada, especialmente las características y necesidades de las micro, pequeñas y medianas empresas, tal como se definen en la ley N°20.416.

Artículo 6.- Procedimiento de calificación de los operadores de importancia vital. Al menos cada tres años, la Agencia deberá revisar y actualizar la calificación de operadores de importancia vital mediante una resolución dictada por la Directora o el Director Nacional.

Para los efectos del inciso anterior, la Agencia requerirá informe fundado a los organismos públicos con competencia sectorial para que se pronuncien sobre aquellas instituciones públicas y privadas que deban calificarse como operadores de importancia vital. Dichos informes deberán evacuarse en la forma prescrita en el artículo 37 bis de la ley Nº19.880.

Recibidos los informes indicados precedentemente la Agencia dispondrá de un plazo de treinta días corridos para evacuar un informe que contendrá la nómina preliminar de las instituciones calificadas como operadores de importancia vital. Esta nómina preliminar deberá ser sometida a consulta pública por un plazo de treinta días corridos sólo respecto de las instituciones privadas, en la forma que determine el reglamento de la presente ley. Respecto de las instituciones públicas, se deberá requerir informe del Ministerio de Hacienda, en los términos del inciso precedente.

Terminado el proceso de consulta pública y recibido el informe del Ministerio de Hacienda, la Agencia dispondrá de treinta días corridos para elaborar el informe que contendrá la nómina final de instituciones que deban ser calificadas como operadores de importancia vital, individualizándolas en la forma que señale el reglamento.

Cumplidas las etapas anteriores, la Agencia, mediante resolución fundada de su Director o Directora, determinará los operadores de importancia vital.

En contra de la resolución que se dicte sólo podrá deducirse recurso de reposición dentro del plazo de diez días corridos contado desde la respectiva notificación a que se refiere el artículo 46 de la ley Nº19.880. El recurso deberá resolverse dentro del plazo de veinte días corridos.

Un reglamento expedido por el ministerio a cargo de la seguridad pública contemplará los demás aspectos del procedimiento que sean necesarios para su correcta ejecución.”.”

La **asesora legislativa del Ministerio del Interior, abogada señora Michelle Bordachar,** señaló que el artículo 5 se decidió separar en dos artículos distintos, lo que son los servicios esenciales y los operadores de importancia vital, atendida a la confusión que generaba el que estuvieran juntos, puesto que se pensaba que los deberes específicos, que se establecen más adelante, aplicaban a cualquier institución que presta un servicio esencial, lo cual no es así ya que sería solo y exclusivamente a los operadores de importancia vital, a detallar en un listado que fija las instituciones públicas y privadas a considerar.

Agregó, que en el artículo 5 nuevo propuesto, se establecen cuáles son los criterios y la forma de su determinación, y en el 6 nuevo propuesto, el procedimiento donde se establecen los plazos y recursos procesales.

El presidente diputado señor Andrés Longton, consultó a la asesora, el motivo por el cual se fijó solo como recurso, al de reposición y no todos a aquellos que considera la ley N°19.880.

Los **diputados señores Cristián y Jaime Araya,** manifestaron en la misma línea, su preocupación en relación a la falta de recursos procesales posibles de deducir en contra de la resolución, por lo que sugiere ampliar el sistema recursivo en esta materia.

La **asesora legislativa del Ministerio del Interior, abogada señora Michelle Bordachar,** respondió que solo fue considerado el recurso de reposición porque el jerárquico no procede en la Agencia, sin olvidar que de todas maneras se contempla también el recurso de reclamación de legalidad, por lo que no sería necesario el jerárquico.

El **presidente diputado señor Andrés Longton,** insistió señalando que si bien comprende que muchas veces en los órganos de administración del estado no procede el jerárquico porque no hay un jerárquico, procediendo solo el de reposición, sin embargo, es posible considerar otros contemplados en la ley N°19.880, como es el de invalidación que además tiene un plazo mayor, y su regulación en general.

Por lo anterior, sugirió que esto se amplié a todos los recursos contemplados en la ley N°19.880.

A la propuesta del Ejecutivo, respecto a los artículos 5 y 6, reemplazar el inciso sexto de la propuesta del artículo 6, **los diputados señores Cristián Araya, Jaime Araya y Andrés Longton, la siguiente indicación:**

“En contra de la resolución que se dicten podrán deducirse aquellos recursos a que se refiere la ley N°19.880, sin perjuicio de la facultad de ejercer el recurso establecido en el artículo 35 de la presente ley”.

Puesta en votación **la indicación del Ejecutivo que incorpora los artículos 5 y 6 nuevos, junto a la indicación de modificación, se aprueba por unanimidad.** Votan la y los diputados señores Jaime Araya, Cristián Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal y Andrés Longton (presidente). **(7-0-0)**

****

Se da lectura al artículo 5 del proyecto de ley que ha pasado a ser 7:

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.”

Al artículo 5 que ha pasado a ser 7, el Ejecutivo formuló la siguiente indicación:

Para reemplazar los incisos primero, segundo, tercero, cuarto, y quinto, del actual artículo 5, que ha pasado a ser artículo 7, por los siguientes:

“Las instituciones obligadas por la presente ley deberán aplicar de manera permanente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad. Estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso.

El cumplimiento de estas obligaciones exige 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. El objeto de estos protocolos y estándares será la prevención y gestión de los riesgos asociados a la ciberseguridad, así como la contención y mitigación del impacto que los incidentes pueden tener sobre la continuidad operacional del servicio prestado o la confidencialidad y la integridad de la información o de las redes o sistemas informáticos de conformidad con lo prescrito en la presente ley.

Para efectos de emitir las medidas de seguridad a que se refiere el inciso primero, la Agencia deberá observar lo prescrito en el artículo 23, según corresponda. Dichos protocolos y estándares deberán someterse a consulta pública, en la misma forma y plazo señalados en el inciso tercero del artículo 6. La medida deberá publicarse junto con el informe en que se justifique el rechazo o modificación de las observaciones que correspondan.

La Agencia deberá establecer medidas de seguridad diferenciadas según el tipo de organización de que se trate, teniendo especialmente en consideración las características y posibilidades de las pequeñas y medianas empresas definidas por la ley N°20.416, que fija normas especiales para las empresas de menor tamaño.”.

La asesora legislativa del Ministerio del Interior, abogada señora Michelle Bordachar, explicó que esta indicación viene a recoger gran parte de las indicaciones formuladas al artículo 5 del proyecto, que actualmente pasó a ser 7, que establece en qué consiste este deber de ciberseguridad, el cómo se cumple y los criterios para definir los estándares, tomando en consideración su aplicabilidad, ya que la idea es ayudar a las empresas y no crearles una carga. Agregó que, si bien se modifican todos los incisos, el último no, porque no se llegó a consenso a la eliminación o no de la prohibición del pago de ramsonware.

Puesta en votación **la indicación del Ejecutivo que reemplaza los incisos primero, segundo, tercero, cuarto, y quinto, del actual artículo 5, que ha pasado a ser artículo 7, se aprueba por unanimidad.** Votan la y los diputados señores Jaime Araya, Cristián Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal y Andrés Longton (presidente). **(7-0-0)**

Al inciso final del artículo 5 que ha pasado a ser 7, los diputados señores Cristián Araya, José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°40:

“Suprímase el inciso final del artículo 5.”

El **diputado señor José Miguel Castro**, explicó que esta indicación se debe a que el inciso final del artículo 5 prohíbe a los organismos e instituciones señalados en el inciso primero, a 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. Agregó que no están de acuerdo a establecer por ley una prohibición de ese tipo, considerando que las empresas deben tener la libertad de poder optar de salir o no del riego, considerando situaciones extremas que pueden suscitarse.

Además, no existe normativa en el mundo que lo prohíba, solo existen recomendaciones.

Puesta en votación **la indicación N°40, se aprueba por unanimidad.** Votan la y los diputados señores Jaime Araya, Cristián Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal y Andrés Longton (presidente). **(7-0-0)**

Al artículo 5 que ha pasado a ser actual artículo 7, el Ejecutivo formuló la siguiente indicación N°7:

Para intercalar, en el artículo 5°, inciso primero, entre la expresión “ciberseguridad” y el punto que le sigue, la frase “incluyendo aquellas contenidas en instrucciones generales y particulares dictadas por la Agencia”.

Por haberse aprobado la indicación del Ejecutivo que modifica el artículo 5 que ha pasado a ser 7, junto a la indicación N°40, **reglamentariamente esta se rechaza.**

Al inciso primero del artículo 5 que ha pasado a ser actual artículo 7, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°38:

“Sustitúyese el inciso primero del artículo 5° por el siguiente:

“Artículo 5. Deberes generales. La Administración del Estado así como los agentes privados calificados como prestadores de servicios esenciales y operadores de importancia vital, deben aplicar de manera permanente las medidas necesarias para prevenir, reportar y resolver incidentes de ciberseguridad que pudieran afectarlos. Estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso.”.”

Por haberse aprobado la indicación del Ejecutivo que modifica el artículo 5 que ha pasado a ser 7, junto a la indicación N°40, **reglamentariamente esta se rechaza.**

Al inciso primero del artículo 5 que ha pasado a ser actual artículo 7, el diputado señor Andrés Jouannet, formuló la siguiente indicación:

Incorpórese al inciso primero del artículo 5° propuesto, luego de “instituciones privadas” la siguiente expresión “y públicas calificadas como operadores de importancia vital”.

Por haberse aprobado la indicación del Ejecutivo que modifica el artículo 5 que ha pasado a ser 7, junto a la indicación N°40, **reglamentariamente esta se rechaza.**

Al inciso tercero del artículo 5 que ha pasado a ser actual artículo 7, el diputado señor Andrés Jouannet, formuló la siguiente indicación:

“Suprímase en el inciso tercero del artículo 5° propuesto la expresión “En el caso de los organismos de la Administración del Estado e instituciones privadas que presten servicios esenciales,”.

Por haberse aprobado la indicación del Ejecutivo que modifica el artículo 5 que ha pasado a ser 7, junto a la indicación N°40, **reglamentariamente esta se rechaza.**

Al inciso cuarto del artículo 5 que ha pasado a ser actual artículo 7, el diputado señor Andrés Jouannet, formuló la siguiente indicación:

“Incorpórese en el inciso cuarto del artículo 5° propuesto, luego del punto final, que pasa a ser punto y seguido, lo siguiente: “Para estos efectos, las necesidades de las micro, pequeñas y medianas empresas deberán ser abordadas a través de, especialmente, la Política Nacional de Ciberseguridad, y la prestación de servicios por parte de la Agencia u otros organismos del Estado competentes, para que les proporcionen orientación y asistencia acerca de cuestiones relacionadas con la ciberseguridad”.

Por haberse aprobado la indicación del Ejecutivo que modifica el artículo 5 que ha pasado a ser 7, junto a la indicación N°40, **reglamentariamente esta se rechaza.**

Al inciso quinto del artículo 5 que ha pasado a ser actual artículo 7, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°39:

“Incorpórese, en el inciso quinto del artículo 5° después del punto aparte, que pasa a ser seguido, lo siguiente: “Dichos protocolos y estándares deberán someterse a consulta pública y recepción de observaciones.”.”

Por haberse aprobado la indicación del Ejecutivo que modifica el artículo 5 que ha pasado a ser 7, junto a la indicación N°40, **reglamentariamente esta se rechaza.**

Al artículo 5 que ha pasado a ser 7, el Ejecutivo formuló la siguiente indicación N°8:

Para incorporar en el artículo 5°, el siguiente inciso final, nuevo:

“En todo caso, las obligaciones de ciberseguridad contenidas en las instrucciones generales o particulares dictadas por la Agencia, 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.”.

Por haberse aprobado la indicación del Ejecutivo que modifica el artículo 5 que ha pasado a ser 7, junto a la indicación N°40, **reglamentariamente se rechazan las otras indicaciones.**

***

Se da lectura al artículo 6º que ha pasado a ser 8º.

“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.

Al artículo 6 que ha pasado a ser 8, el Ejecutivo formuló la siguiente indicación:

Para reemplazar el actual artículo 6, que ha pasado a ser artículo 8, por el siguiente:

“Artículo 8°. Deberes específicos de los operadores de importancia vital.

Todos los operadores de importancia vital deberán:

a) Implementar un sistema de gestión de seguridad de la información continuo con el fin de determinar aquellos riesgos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y la continuidad operacional del servicio.

Este sistema deberá permitir evaluar tanto la probabilidad como el potencial impacto de un incidente de ciberseguridad.

b) Mantener un registro de las acciones ejecutadas que compongan el sistema de gestión de seguridad de la información, de conformidad a lo que señale el reglamento.

c) Elaborar e implementar planes de continuidad operacional y ciberseguridad, los cuales deberán certificarse en conformidad al artículo 26 de la presente ley, y deberán someterse a revisiones periódicas por parte de los sujetos obligados, con una frecuencia mínima de dos años.

Con todo, la Agencia podrá instruir a uno o más operadores de importancia vital, fundadamente y por motivos sobrevinientes graves, la certificación de sus planes de continuidad operacional o ciberseguridad en un plazo menor al indicado en el párrafo precedente; sin embargo, la Agencia sólo podrá ejercer esta facultad, respecto de cada operador de importancia vital, siempre que la certificación tenga al menos un año de vigencia.

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 Nacional, 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 que señale el artículo 26 de la presente ley.

g) Informar a los potenciales afectados sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos, especialmente cuando involucren datos personales y no exista otra disposición legal que requiera su notificación; o cuando sea necesario para prevenir la ocurrencia de nuevos incidentes o para gestionar uno que ya hubiera ocurrido.

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 actuará como contraparte de la Agencia e informará a la autoridad o jefatura o jefe superior del órgano o servicio de la Administración del Estado o a los directores, gerentes, administradores o ejecutivos principales, según lo definan las instituciones privadas.”.

El **presidente diputado señor Andrés Longton,** luego de escuchar las opiniones de algunos expertos, diputados y diputadas de la Comisión, determinó dejar pendiente este artículo, pero con el acuerdo que se tiene consenso en todo el texto propuesto, con excepción de la letra g), para que el Ejecutivo, en conjunto con la mesa técnica de trabajo de asesores, sugiera una redacción más adecuada a ese literal. Queda pendiente su estudio y votación.

Luego, **se de lectura al artículo 8 que ha pasado a ser 10:**

“Artículo 8°. Agencia Nacional de Ciberseguridad. Créase la Agencia Nacional de Ciberseguridad como un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propio, 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.”.

Al inciso segundo del artículo 8 que ha pasado a ser 10, el diputado señor Jorge Alessandri y la diputada señora Gloria Naveillan, formularon la siguiente **indicación N°57**:

Para insertar en el inciso segundo del artículo 8°, después de la palabra ciberseguridad, la siguiente frase; “en coordinación con las autoridades sectoriales de las industrias reguladas”.

Al inciso segundo del artículo 8 que ha pasado a ser 10, de los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente **indicación N°58**:

“Introdúcense las siguientes modificaciones al inciso segundo del artículo 8º:

a) Suprímese la frase “de los organismos de la Administración del Estado”;

b) Intercálese, entre las palabras “privadas” y “en materia de seguridad”, la frase “calificadas como operadores de importancia vital”; y

c) Sustitúyese la frase “incluida la facultad de impartir instrucciones generales y particulares” por “dentro del ámbito de su competencia y de conformidad a lo dispuesto en el artículo 3”.

Al inciso segundo del artículo 8 que ha pasado a ser 10, el diputado señor Andrés Jouannet, formuló la siguiente **indicación N°31**:

“Incorpórese en el inciso segundo del artículo 8° propuesto, luego de “instituciones privadas”, la expresión “y públicas calificadas como operadores de importancia vital”.”.

La asesora legislativa del Ministerio del Interior, Michelle Bordachar, comentó que, respecto a este artículo, las indicaciones formuladas por los diputados tienen como objetivo mejorar el inciso segundo, por lo que se acordó eliminarlo para llegar a consenso.

Puesto en votación **el artículo 8 que ha pasado a ser 10, excluyendo su inciso segundo, se aprueba por unanimidad**. Votan a favor la y los diputados señores Jorge Alessandri, Chiara Barchiesi en reemplazo del diputado señor Cristián Araya, José Miguel Castro y Andrés Longton (presidente) y Maite Orsini. Sin votos en contra. Sin abstenciones**. (5-0-0).**

Puesto en votación **el inciso segundo del artículo 8 que ha pasado a ser 10, se rechaza por unanimidad.** No hay votos a favor. Votan en contra la y los diputados señores Jorge Alessandri, Chiara Barchiesi en reemplazo del diputado señor Cristián Araya, José Miguel Castro y Andrés Longton (presidente) y Maite Orsini. Sin abstenciones. **(0-5-0).**

En sesión del 6 de septiembre de 2023 se discutió y aprobó el artículo 20 que ha pasado a ser 22, dejando pendiente su letra b) y d), a la espera de una mejor redacción de parte del Ejecutivo en relación a CSIRT Sectoriales.

Según lo anterior, **el Ejecutivo formula la siguiente indicación N°5, para modificar el literal b) y d) del artículo 20 que ha pasado a ser 22:**

a) Modifícase el literal b) en el siguiente sentido:

“i) Reemplázase la expresión “Sectoriales”, la primera vez que aparece, por la frase “que pertenezcan a organismos de la Administración del Estado”.

ii) Suprímese, la expresión “por parte de los CSIRT Sectoriales,”.

iii) Agrégase, el siguiente párrafo final, nuevo:

“Cuando los ciberataques o incidentes puedan afectar el normal funcionamiento del sistema financiero, la respuesta del CSIRT Nacional deberá realizarse en coordinación con el Consejo de Estabilidad Financiera creado por la ley N°20.789. Sin perjuicio de la obligación del CSIRT Nacional de comunicar al mencionado Consejo sobre el incidente, podrá tomar medidas sin esperar respuesta en casos de urgencia calificada.”.”.

b) Reemplázase, en el literal d), la expresión “Sectoriales” por la frase “que pertenezcan a organismos de la Administración del Estado.”.

La Comisión **acordó,** por sugerencia del Ejecutivo y del diputado señor Andrés Longton, por no definirse qué se entiendo por “urgencia calificada”, eliminar del texto la expresión “calificada”.

Puesta en votación la **indicación del Ejecutivo N°5, con el acuerdo de suprimir la expresión de “calificada”, se aprueba por unanimidad**. Votan a favor la y los diputados señores Jorge Alessandri, Chiara Barchiesi en reemplazo del diputado señor Cristián Araya, José Miguel Castro y Andrés Longton (presidente) y Maite Orsini. Sin votos en contra. Sin abstenciones. **(5-0-0).**

***

Al Título IV sobre Otras Instituciones Intervinientes, el Ejecutivo presenta la siguiente indicación N°6:

"Para reemplazar el encabezado del Título IV por "Coordinación regulatoria y otras disposiciones".".

Puesta en votación la indicación del Ejecutivo N°6, se **aprueba por unanimidad**. Votan a favor la y los diputados señores Jorge Alessandri, Chiara Barchiesi en reemplazo del diputado señor Cristián Araya, José Miguel Castro y Andrés Longton (presidente) y Maite Orsini. Sin votos en contra. Sin abstenciones**. (5-0-0).**

***

Se da lectura al artículo 21 que ha pasado a ser 23:

"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 ésta lo solicite.

En el ejercicio de sus funciones, los CSIRT Sectoriales deberán dar cumplimiento a todos 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.”.

Al artículo 21 que ha pasado a ser 23, **el Ejecutivo formuló la siguiente indicación N°7:**

“Para reemplazar el actual artículo 21, que ha pasado a ser artículo 23, por el siguiente:

“Artículo 23. Coordinación regulatoria. Cuando la Agencia deba dictar protocolos, estándares técnicos o instrucciones de carácter general en el ejercicio de sus funciones, y estos tengan efectos en las áreas de competencia de otra entidad sectorial, deberá previamente remitir la información relevante a dicha entidad y solicitar un informe con el propósito de prevenir posibles conflictos normativos y garantizar la coordinación, cooperación y colaboración efectivas entre ambas autoridades.

La autoridad sectorial requerida deberá evacuar su informe dentro de un plazo de treinta días corridos a partir de la fecha en que recibió la solicitud indicada en el inciso anterior. La Agencia considerará el contenido de este informe en la motivación del acto administrativo de carácter general que emita. Transcurrido el plazo sin que se hubiere recibido el informe correspondiente, la Agencia procederá a emitir los protocolos, estándares técnicos o instrucciones generales requeridos.

Cuando una autoridad sectorial, en el ejercicio de sus atribuciones establecidas en sus leyes orgánicas, deba emitir actos administrativos de carácter general que tengan efectos en los ámbitos de competencia de la Agencia en conformidad a la presente ley, deberá remitir a la Agencia la información pertinente y solicitar un informe con el objeto de prevenir posibles conflictos normativos y garantizar la coordinación, cooperación y colaboración entre ambas entidades. Además, en el ejercicio de estas atribuciones, las autoridades sectoriales deben tener en cuenta, al menos, los protocolos, estándares técnicos e instrucciones generales previamente emitidos por la Agencia.

Lo establecido en los incisos anteriores no se aplicará en los casos en que el acto administrativo respectivo requiera una aplicación inmediata o en el plazo más breve posible atendida a su naturaleza y urgencia, siempre que se justifique dicha circunstancia y se deje constancia. No obstante, en estos casos, la Agencia deberá, en un plazo de tres días corridos, proporcionar a las autoridades sectoriales competentes, o viceversa según corresponda, todos los documentos tenidos a la vista y solicitar un informe con el fin de cumplir con los objetivos mencionados en los incisos primero y tercero.”.”.

La asesora legislativa del Ministerio del Interior, Michelle Bordachar, explicó que el objetivo de esta indicación, acordada con la Comisión para el Mercado Financiero, es una norma espejo de lo que actualmente existe en el artículo 37 bis de la ley sobre Procedimientos de la Administración del Estado, con las modificaciones pertinentes para adaptarlas a esta ley.

Puesta en votación la **indicación del Ejecutivo N°7**, se aprueba por unanimidad. Votan a favor la y los diputados señores Jorge Alessandri, Chiara Barchiesi en reemplazo del diputado señor Cristián Araya, José Miguel Castro y Andrés Longton (presidente) y Maite Orsini. Sin votos en contra. Sin abstenciones. **(5-0-0).**

Por aprobarse la indicación antes discutidas y votadas**, se rechaza reglamentariamente el artículo 21 que ha pasado a ser 23 del texto aprobado por el Senado.**

***

Se da lectura al artículo 22 que ha pasado a ser 24:

“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 éstos 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.”

Al artículo 22 que ha pasado a ser 24**, el Ejecutivo presentó la siguiente indicación N°8:**

“Para reemplazar el actual artículo 22, que ha pasado a ser artículo 24, por el siguiente:

“Artículo 24. Normativa Sectorial. Las autoridades sectoriales podrán emitir normativas generales, técnicas e instrucciones necesarias para fortalecer la ciberseguridad en las instituciones de su sector, en conformidad con la regulación respectiva y siguiendo lo dispuesto en el artículo anterior, cuando corresponda.

Las instituciones supervisadas deberán cumplir obligatoriamente con estas normas e instrucciones en la gestión de sus riesgos, de acuerdo con la autoridad sectorial que las haya emitido. La fiscalización y sanción relacionadas con estas disposiciones se regirán por las leyes respectivas de dicha autoridad sectorial.

Cuando las normas o instrucciones emitidas por una autoridad sectorial establezcan obligaciones para un sector a fin de prevenir incidentes de ciberseguridad, que tengan, al menos, efectos equivalentes a las obligaciones previstas en los protocolos, normas o instrucciones de la Agencia, prevalecerán las disposiciones de la autoridad sectorial. Esto no afectará los deberes de coordinación establecidos en el artículo 23 ni la aplicación de las normas de la presente ley. No obstante, si las normas o instrucciones de una autoridad sectorial no cubren a todas las entidades de un sector o solo se aplican a una parte de sus supervisados, los protocolos, normas o instrucciones de la Agencia seguirán siendo plenamente aplicables a las entidades no exceptuadas en los términos indicado en este inciso.

Para efectos de lo indicado en el inciso anterior, la Agencia y la autoridad sectorial correspondiente deberán previamente dictar una norma conjunta de carácter general. Dicha norma tendrá por objeto establecer criterios para la evaluación de la equivalencia de los efectos entre una normativa o instrucción.

Lo anterior no será aplicable a la Comisión para el Mercado Financiero (CMF), la cual deberá integrar en el correspondiente acto administrativo los antecedentes y fundamentos que permitan determinar la equivalencia de los efectos de una norma o instrucción. Esto se llevará a cabo tomando en consideración los elementos contenidos en el informe elaborado por la Agencia, de conformidad con el artículo 23.”.

La **asesora legislativa del Ministerio del Interior, Michelle Bordachar,** señaló que esta indicación lo que busca es darle especialidad a lo establecido en el artículo anterior, fijando el deber de coordinación en el caso de la normativa sectorial, y prioridad de aplicación de normas y su equivalencia.

Además, solicitó, por sugerencia del CMF, que en el inciso final se modifique la expresión “lo anterior”, por el “inciso anterior”, para que no se interprete que lo que se establece hace referencia a todo el artículo, cuando es solo al artículo anterior al inciso final.

Agregó que la **mesa de trabajo, compuesta por el Ejecutivo y los asesores de los parlamentarios integrantes de la Comisión**, sugieren darle votación a la indicación del Ejecutivo con exclusión del inciso final, por considerar que hay una regulación especial para una institución como es la CMF y no otras, debiendo existir una general a aplicar a las instituciones sectoriales.

Puesta en votación **la indicación del Ejecutivo N°8, sin el inciso final, se aprueba por unanimidad.** Votan a favor la y los diputados señores Jorge Alessandri, Chiara Barchiesi en reemplazo del diputado señor Cristián Araya, José Miguel Castro y Andrés Longton (presidente) y Maite Orsini. Sin votos en contra. Sin abstenciones. **(5-0-0).**

Por tanto, se rechaza reglamentariamente el artículo 22 del texto aprobado por el Senado.

***

Se da lectura al artículo 6º que ha pasado a ser 8º (reanudación del estudio y posterior votación de este artículo):

“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.”.”.

Al artículo 6 que ha pasado a ser 8, **el diputado señor Andrés Jouannet, formuló la siguiente indicación N°26:**

“Reemplácese en el inciso primero del artículo 6° propuesto la expresión “instituciones privadas” por “instituciones públicas y privadas”.”.

Al artículo 6 que ha pasado a ser 8, **los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°41:**

“Introdúcense las siguientes modificaciones al artículo 6º:

Sustitúyase oración “Todos los organismos del Estado con competencias específicas sobre servicios esenciales y las instituciones privadas calificadas como operadores de importancia vital deberán” por lo siguiente: “La Administración del Estado y las instituciones calificadas como operadores de importancia vital adoptarán las medidas de naturaleza tecnológica, organizacional, física o informativa, según sea el caso, mencionadas en el artículo anterior, y estas garantizarán un nivel de seguridad de los sistemas de redes y de información adecuado en relación con los riesgos planteados. Al evaluar la proporcionalidad de dichas medidas, se tendrá debidamente en cuenta el grado de exposición de la entidad a los riesgos, el tamaño de la entidad y la probabilidad de que se produzcan incidentes y su gravedad, incluidas sus repercusiones sociales y económicas. Tales medidas se fundamentarán en un enfoque basado en riesgos que tenga por objeto proteger los sistemas de redes y de información y el entorno físico de dichos sistemas frente a incidentes y consistirán en”.”.

Al artículo 6 que ha pasado a ser 8, **el diputado señor Jaime Araya y la diputada señorita Maite Orsini, formularon la siguiente indicación N°42:**

“Para agregar en la letra a) del artículo 6°, la palabra "riesgos" a continuación de la palabra "aquellos".”.

Al artículo 6 que ha pasado a ser 8, **los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°43:**

En el literal b) del inciso primero del artículo 6° suprímese la frase: “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.”

Reemplázase el literal c) por el siguiente:

c) Elaborar e implementar planes de continuidad operacional y ciberseguridad, debiendo ser acreditados ante la Agencia cuando corresponda.”

Al artículo 6 que ha pasado a ser 8, **el diputado señor Jorge Alessandri y la diputada señora Gloria Naveillán, formularon la siguiente indicación N°44:**

“Para reemplazar el literal c) del artículo 6°, por el siguiente: “c) Elaborar e implementar planes de continuidad operacional y ciberseguridad, certificados por un centro o entidades de certificación nacional o internacional. Para estos efectos la Agencia, en conjunto con las Autoridades Sectoriales de los sectores regulados, deberán establecer el procedimiento y los requisitos para la implementación de un registro público de centros o entidades certificadoras. Dichos planes deberán ser actualizados y certificados anualmente.”.”

Al artículo 6 que ha pasado a ser 8, **los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°45:**

“Suprímese el literal f) del artículo 6°.”

Al artículo 6 que ha pasado a ser 8, **el diputado señor Jorge Alessandri y la diputada señora Gloria Naveillán, formularon la siguiente indicación N°46:**

“Para reemplazar el literal f) del artículo 6° por el siguiente: “f) Contar con las certificaciones nacionales o internacionales de los sistemas de gestión y procesos”.”.

Al artículo 6 que ha pasado a ser 8, **los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°47:**

“Sustitúyase el literal g) del artículo 6° por el siguiente: “g) Informar sin demora a los destinatarios de sus servicios de las medidas o soluciones que pueden aplicar para reducir el riesgo resultante de un incidente de efecto negativo, en los términos artículo 23º de esta ley. En su caso, y en particular cuando sea probable que se materialice un incidente de efecto significativo, también debe informarse a los destinatarios de sus servicios del propio incidente de efecto significativo. La exigencia de informar de tales amenazas a los destinatarios debe cumplirse en la medida de lo posible, pero no exime a las entidades de la obligación de tomar a sus expensas medidas inmediatas y adecuadas para prevenir o subsanar cualquier incidente de efecto significativo y restablecer el nivel normal de seguridad del servicio. La mencionada información sobre los incidentes de efectos significativos a los destinatarios del servicio debe facilitarse de forma gratuita y la información debe estar redactada en un lenguaje fácil de comprender.”.”

Al artículo 6 que ha pasado a ser 8, **el diputado señor Jorge Alessandri y la diputada señora Gloria Naveillán, formularon la siguiente indicación N°48:**

“Para reemplazar el literal i) del artículo 6°, por el siguiente texto: “Designar un representante de ciberseguridad, quien será la contraparte de la Agencia y de las Autoridades Sectoriales”.”.

“Para agregar en el último inciso de la letra a) del artículo 6 y a continuación de la palabra reglamento la frase “que deberá ser sometido a trámite de toma de razón de la Contraloría General de la República.”.”

“Para eliminar completamente el texto final del artículo 6.”

Al artículo 6 que ha pasado a ser 8, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente **indicación N°49:**

“Suprímese el inciso final del artículo 6°”.

Al artículo 6 que ha pasado a ser 8, **el diputado señor Jaime Araya y la diputada señorita Maite Orsini, formularon la siguiente indicación N°50:**

“Para agregar una nueva letra j) al artículo 6°, del siguiente tenor:

j) En el caso de las instituciones privadas que sean calificadas como operadores de importancia vital, y que estén organizadas como sociedades anónimas, al menos un miembro de su directorio, deberá contar con experiencia o conocimientos en materia de ciberseguridad.”

Finalmente, al artículo 6 que ha pasado a ser 8, el Ejecutivo formuló la siguiente indicación sustitutiva:

“**AL ACTUAL ARTÍCULO 6, QUE HA PASADO A SER ARTÍCULO 8**

Para reemplazar el actual artículo 6, que ha pasado a ser artículo 8, por el siguiente:

“Artículo 8°. Deberes específicos de los operadores de importancia vital.

Todos los operadores de importancia vital deberán:

a) Implementar un sistema de gestión de seguridad de la información continuo con el fin de determinar aquellos riesgos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y la continuidad operacional del servicio.

Este sistema deberá permitir evaluar tanto la probabilidad como el potencial impacto de un incidente de ciberseguridad.

b) Mantener un registro de las acciones ejecutadas que compongan el sistema de gestión de seguridad de la información, de conformidad a lo que señale el reglamento.

c) Elaborar e implementar planes de continuidad operacional y ciberseguridad, los cuales deberán certificarse en conformidad al artículo 26 de la presente ley, y deberán someterse a revisiones periódicas por parte de los sujetos obligados, con una frecuencia mínima de dos años.

Con todo, la Agencia podrá instruir a uno o más operadores de importancia vital, fundadamente y por motivos sobrevinientes graves, la certificación de sus planes de continuidad operacional o ciberseguridad en un plazo menor al indicado en el párrafo precedente; sin embargo, la Agencia sólo podrá ejercer esta facultad, respecto de cada operador de importancia vital, siempre que la certificación tenga al menos un año de vigencia.

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 Nacional, 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 que señale el artículo 26 de la presente ley.

g) Informar a los potenciales afectados sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos, especialmente cuando involucren datos personales y no exista otra disposición legal que requiera su notificación; o cuando sea necesario para prevenir la ocurrencia de nuevos incidentes o para gestionar uno que ya hubiera ocurrido.

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 actuará como contraparte de la Agencia e informará a la autoridad o jefatura o jefe superior del órgano o servicio de la Administración del Estado o a los directores, gerentes, administradores o ejecutivos principales, según lo definan las instituciones privadas.”.

El **presidente diputado señor Andrés Longton**, recordó que luego de escuchar las opiniones de algunos expertos, diputados y diputadas de la Comisión, se determinó dejar pendiente este artículo, pero con el acuerdo que se tiene consenso en todo el texto propuesto por el Ejecutivo, con excepción de la letra g), para que los parlamentarios, en la siguiente sesión sugieran una redacción más adecuada a ese literal.

Por lo anterior, y habiendo acuerdo en aprobar el articulado 6º que ha pasado a ser 8º con sus letras formulado en indicación por el Ejecutivo, salvo la excepción referida a la letra g), la y los diputados señores Jorge Alessandri, José Miguel Castro, Andrés Longton y Maite Orsini, formularon la siguiente indicación: complementaria al texto del Ejecutivo:

“g) Informar a los potenciales afectados, en la medida que puedan identificarse y cuando así requiera la Agencia, sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos, cuando involucren datos personales y no exista otra disposición legal que requiera su notificación; o cuando sea necesario para prevenir la ocurrencia de nuevos incidentes o para gestiona uno que ya hubiera ocurrido.”

Puesta en votación la indicación del Ejecutivo, que sustituye el artículo 6º que ha pasado a ser 8º, conjuntamente con **la indicación antes descrita, se aprueba por unanimidad.** Votan a favor la y los diputados señores Jorge Alessandri, Chiara Barchiesi en reemplazo del diputado señor Cristián Araya, José Miguel Castro y Andrés Longton (presidente) y Maite Orsini. Sin votos en contra. Sin abstenciones. **(5-0-0).**

En consecuencia, se rechazan reglamentariamente el artículo 6º del proyecto y las indicaciones formuladas al mismo.

***

Se da lectura al artículo 7 que ha pasado a ser 9:

“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 éste 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.”.

Al artículo 7 que ha pasado a ser 9, **el diputado señor Andrés Jouannet, formuló las siguientes indicaciones:**

“Reemplácese en el inciso primero del artículo 7 propuesto la expresión “Todas las instituciones, sean públicas o privadas, e independiente de si son o no operadores de servicios esenciales” por “Todas las instituciones públicas y privadas calificadas como operadores de importancia vital”.”.

“Reemplácese en el inciso tercero la expresión “, todos los operadores de servicios esenciales, sean de importancia vital o no,” por “, todos los operadores de importancia vital”.”.

“Reemplácese el inciso cuarto del artículo 7° propuesto por uno del siguiente tenor: “Los organismos de la Administración del Estado, las instituciones públicas y privadas calificadas como operadores de importancia vital, y, cuando proceda, sus proveedores, podrán intercambiar entre sí de forma voluntaria información relevante sobre ciberseguridad, incluyendo la ocurrencia de incidentes de ciberseguridad y vulnerabilidades, siempre que dicho intercambio de información se haga con el objetivo de prevenir, detectar o responder a incidentes, recuperarse de ellos o reducir su repercusión; o refuerce el nivel de ciberseguridad de los organismos de la administración del Estado y operadores de importancia vital. Dicho intercambio se pondrá en práctica a través de mecanismos de intercambio de información sobre ciberseguridad que respeten la posible naturaleza delicada de la información compartida”.”.

“Incorpórese el siguiente inciso final al artículo 7° propuesto: “No obstante el deber de reportar los ciberataques e incidentes de ciberseguridad al CSIRT Nacional establecido en este artículo, adicionalmente los operadores de importancia vital deberán cooperar eficazmente con el Ministerio Público poniendo a su disposición datos o informaciones precisas, verídicas y comprobables y denunciar, cuando corresponda, en el caso de que el incidente de ciberseguridad que pueda tener efectos significativos corresponda a la comisión de alguno de los delitos establecidos en 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”.”.

Al artículo 7 que ha pasado a ser 9, **el diputado señor Jorge Alessandri y la diputada señora Gloria Naveillán, formularon las siguientes indicaciones:**

“Para reemplazar el inciso primero del artículo 7° por el siguiente: “Deber de reportar. Todas las instituciones, sean públicas o privadas, definidos como operadores de servicios esenciales, 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.”.”

“Para reemplazar el inciso segundo del artículo 7° por el siguiente: “La obligación de reportar, como primera alerta, deberá cumplirse en un plazo inferior a tres horas contadas desde que se tuvo conocimiento del evento respectivo. La entidad informante deberá entregar en un plazo no superior a 48 horas información complementaria respecto al incidente referido. 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.”.”.

“Para eliminar en el inciso tercero del artículo 7° las palabras “sean” y “o no”.”.

“Para insertar en el inciso cuarto del artículo 7, después de los jefes de servicio, la frase “En el caso de las Instituciones del Estado”.”.

“Para reemplazar el inciso final del artículo 7° por el siguiente texto: “La Agencia en conjunto con las Autoridades Sectoriales dictarán las instrucciones que sean necesarias para la debida realización y recepción de los reportes a que se refiere el presente artículo, procurando simplificar y no duplicar el reporte de información en los casos de empresas reguladas”.”.

Al artículo 7 que ha pasado a ser 9, **los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación:**

“i.Sustitúyese el inciso primero por el siguiente:

“Artículo 7. Deber de reportar. Será obligación de la Administración del Estado y de los agentes privados calificados como servicios esenciales y operadores de importancia vital 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, y de la posibilidad de que agentes privados no sujetos a las disposiciones de esta ley puedan, de manera voluntaria, reportar al CSIRT nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos, en cuyo caso se estarán a la forma dispuesta en este artículo.”

ii.Sustitúyese el inciso segundo por el siguiente:

“El deber de reportar comprende:

a) La emisión de una alerta temprana dentro de las primeras veinticuatro horas desde que se haya tenido constancia del incidente significativo en la que se indicará, cuando proceda, si cabe sospechar que el incidente significativo responde a una acción ilícita o malintencionada;

b) Dentro de las 72 horas desde que se haya tenido constancia del incidente significativo, la actualización de la alerta temprana, exponiéndose una evaluación inicial del incidente significativo, incluyendo su gravedad e impacto, así como indicadores de compromiso, cuando estén disponibles;

c) Un informe final, a más tardar un mes después de presentar la notificación del incidente contemplada en la letra b), en el que se recojan los siguientes elementos:

i) Una descripción detallada del incidente, incluyendo su gravedad e impacto;

ii) El tipo de amenaza o causa principal que probablemente haya desencadenado el incidente; y

iii) Las medidas paliativas aplicadas y en curso.

d) Si el incidente siguiera en curso al momento de la presentación del informe final contemplado en la letra c) precedente, éste se reemplazará por un informe de situación en ese momento y un informe final, que se presentará en el plazo de un mes a partir de que se haya gestionado el incidente.

Tanto el CSIRT respectivo como la autoridad sectorial competente podrán requerir informes intermedios con las actualizaciones pertinentes sobre la situación.”.”

Al artículo 7 que ha pasado a ser 9, **el Ejecutivo formuló las siguientes indicaciones:**

“Para reemplazar en el artículo 7°, los incisos primero y segundo por los siguientes: “Todos los organismos de la Administración del Estado, así como los operadores de servicios esenciales y los operadores de importancia vital, así como las demás instituciones privadas que determine la Agencia, tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos en los términos del artículo 23, tan pronto hayan tenido constancia del incidente, sin demora indebida y conforme el siguiente esquema:

a) Dentro del plazo máximo de 12 horas, deberá enviarse una alerta temprana sobre la ocurrencia del evento, junto a una breve caracterización técnica de él;

b) Dentro del plazo máximo de 72 horas, una actualización de la información contemplada en la letra a), que incluya una evaluación inicial del incidente, su gravedad e impacto, así como indicadores de compromiso, si estuvieran disponibles;

c) A requerimiento del CSIRT Nacional o, en su caso, del CSIRT sectorial existente, un informe intermedio con las actualizaciones pertinentes sobre la situación;

d) A más tardar dentro del plazo máximo de quince días corridos, un informe que contenga, al menos:

i) una descripción detallada del incidente, incluyendo su gravedad e impacto;

ii) el tipo de amenaza o causa principal que probablemente haya causado el incidente;

iii) las medidas de mitigación aplicadas y en curso;

iv) si procede, las repercusiones transfronterizas del incidente;

e) En el caso de que el incidente siga en curso con posterioridad a la presentación del informe contemplado en el literal d), la institución afectada deberá presentar un informe final dentro del plazo de un mes contados desde el primer día que comenzó la gestión del incidente.

Sin perjuicio de lo anterior, los operadores de importancia vital que vean afectada la prestación de sus servicios esenciales a causa de un incidente, deberán notificarlo al CSIRT Nacional tan pronto les sea posible y, en cualquier caso, deberán entregar la información señalada en las letras a y b anteriores, en un plazo máximo de tres horas desde que haya tenido constancia del incidente.”.”

“Para agregar en el artículo 7°, un inciso final, nuevo, del siguiente tenor: “El esquema anterior no será aplicable a las instituciones financieras y demás entidades fiscalizadas por la Comisión para el Mercado Financiero, siempre y cuando la normativa sectorial fuere más exigente que la presente ley, o en aquellas materias no reguladas por la misma.”.”

Al artículo 7 que ha pasado a ser 9, **las y los diputados señores Jorge Alessandri, Cristián Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal, Maite Orsini, Alejandra Placencia y Diego Schalper, formularon la siguiente indicación sustitutiva:**

“Artículo 9°. Deber de reportar.

Todas las instituciones públicas y privadas señaladas en el artículo 4° de la presente ley, tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos en los términos del artículo 25, tan pronto les sea posible y conforme el siguiente esquema:

a) Dentro del plazo máximo de 3 horas contadas desde que se tiene conocimiento de la ocurrencia del ciberataque o incidente de ciberseguridad que tiene impactos significativos, se deberá enviar una alerta temprana sobre la ocurrencia del evento,

b) Dentro del plazo máximo de 72 horas, una actualización de la información contemplada en la letra a), que incluya una evaluación inicial del incidente, su gravedad e impacto, así como indicadores de compromiso, si estuvieran disponibles.

Sin embargo, en caso que la institución afectada fuera un operador de importancia vital y este viera afectada la prestación de sus servicios esenciales a causa del incidente, la actualización de la información deberá entregarse al CSIRT Nacional en un plazo máximo de 24 horas contadas desde que haya tenido conocimiento del incidente;

c) Dentro del plazo máximo de quince días corridos contados desde el envío de la alerta temprana contemplada en la letra a), un informe final en el que se recojan al menos los siguientes elementos:

i) una descripción detallada del incidente, incluyendo su gravedad e impacto;

ii) el tipo de amenaza o causa principal que probablemente haya causado el incidente;

iii) las medidas de mitigación aplicadas y en curso;

iv) si procede, las repercusiones transfronterizas del incidente;

e) En el caso de que el incidente siga en curso con posterioridad a la presentación del informe contemplado en el literal c), éste se reemplazará por un informe de situación en ese momento, debiendo el informe final ser presentado en el plazo de 15 días corridos contados desde que se haya gestionado el incidente.

Sin perjuicio de lo anterior, tanto el CSIRT Nacional como la autoridad sectorial competente podrán requerir las actualizaciones pertinentes sobre la situación.

Los operadores de importancia vital deberán, además, 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 contados desde que se tuvo conocimiento de la ocurrencia del incidente.

En el caso de los organismos del Estado, 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, y siempre que tenga por objeto prevenir, detectar o responder a incidentes, recuperarse de ellos o reducir su repercusión; o reforzar el nivel de ciberseguridad, garantizando a su vez que se respete la posible naturaleza delicada de la información compartida. Con el objeto de cumplir con lo anterior, los contratos de prestación de servicios no podrán contener ninguna cláusula que pudiera restringir o dificultar de cualquier modo la comunicación de información sobre amenazas por parte del prestador de servicios, siempre y cuando con ello no se comprometa la seguridad y protección de datos, incluida la confidencialidad y protección de la propiedad intelectual.

La Agencia dictará las instrucciones que sean necesarias para la debida realización y recepción de los reportes a que se refiere el presente artículo. En caso de existir la obligación de notificar a más de una autoridad, la Agencia en conjunto con las autoridades involucradas y conforme lo dispuesto en el artículo 23 de la presente ley, procurará poner a disposición de los obligados un sistema de ventanilla única que permita la notificación simultánea a todas ellas.”

Puesta en votación **la indicación sustitutiva antes descrita, se aprueba por unanimidad.** Votan a favor la y los diputados señores Jorge Alessandri, Chiara Barchiesi en reemplazo del diputado señor Cristián Araya, José Miguel Castro, Andrés Longton (presidente) y Maite Orsini. Sin votos en contra. Sin abstenciones. **(5-0-0).**

Por aprobarse las indicaciones antes discutida y votada, se rechaza reglamentariamente el artículo 7 que ha pasado a ser 9 del texto aprobado por el Senado, y el resto de las indicaciones al respecto.

Luego, por acuerdo de la Comisión se reabre el debate del artículo 7 que ha pasado a ser 9, para agregar una indicación a la sustitutiva ya aprobada, formulada por los diputados señores Jorge Alessandri, José Miguel Castro y Andrés Longton, que incorpora un inciso final en el siguiente tenor:

"Un reglamento expedido por el Ministerio encargado de la Seguridad Pública regulará el contenido de las diversas clases de reporte señalados en este artículo".

Puesta en votación **la indicación adicionada a la indicación sustitutiva del artículo 7 que ha pasado a ser 9, de agregar inciso final, se aprueba por unanimidad.** Votan a favor la y los diputados señores Jorge Alessandri, José Miguel Castro, Andrés Longton (presidente) y Maite Orsini. Sin votos en contra. Sin abstenciones. **(4-0-0).**

***

Se da lectura al artículo 23 que ha pasado a ser 27[3]:

"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.".

La **asesora legislativa del Ministerio del Interior, Michelle Bordachar**, explicó que este artículo especifica y define qué se entiende por incidente de efecto significativo y por tanto debe ser reportado. Indicó ser una norma espejo a la normativa dispuesta en la Unión Europea.

Puesto en votación **el artículo 23 que ha pasado a ser 27, se aprueba por unanimidad.** Votan a favor la y los diputados señores Jorge Alessandri, Chiara Barchiesi en reemplazo del diputado señor Cristián Araya, José Miguel Castro y Andrés Longton (presidente). Sin votos en contra. Sin abstenciones. **(4-0-0).**

***

[3]Ver página 127.

Se da lectura al artículo 29 que ha pasado a ser 33[4]:

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 éstos. 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 éstas.

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 éste 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.”.”

Puesto en votación el artículo 29 que ha pasado a ser 33, se aprueba por unanimidad. Votan a favor la y los diputados señores Jorge Alessandri, José Miguel Castro, Henry Leal, Andrés Longton (presidente) y Maite Orsini. Sin votos en contra. Sin abstenciones. **(5-0-0).**

***

Se da lectura al artículo 9 que ha pasado a ser 11:

“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.

[4]Ver página 127.

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, sobre protección de la vida privada.”

Al artículo 9 que ha pasado a ser 11, **el Ejecutivo formuló las siguientes indicaciones N°11 y 12:**

“Para reemplazar el literal g) del artículo 9°, por el siguiente: “g) Determinar y calificar los servicios esenciales, en la forma prevista en el título IX de esta ley; y determinar a los operadores de importancia vital, en la forma prevista en el artículo 4° de la presente ley.”.”.

“Para modificar el literal j) del artículo 9°, en el siguiente sentido:

a. Elimínase, en el literal j), la frase “, así como los consagrados por la ley N°19.628, sobre protección de la vida privada”.

b. Agrégase, a continuación del punto final, la frase: “Cuando la información a la que tenga acceso la Agencia incluya datos personales estos deberán ser anonimizados siempre que ello sea posible y no entorpezca el ejercicio de las funciones de la Agencia. En cualquier caso, los datos personales sólo podrán ser tratados dando estricto cumplimiento a lo dispuesto en la ley 19.628.”.”.

Al artículo 9 que ha pasado a ser 11, el diputado señor Andrés Jouannet, formuló las siguientes indicaciones N°32, 33, 34, 35, 36, 37, 38:

Incorpórese en el literal b) del inciso primero del artículo 9° propuesto, luego de “instituciones públicas y privadas”, la expresión “calificadas como operadores de importancia vital, así como la normativa que regula las relaciones entre estos y sus proveedores”.

Incorpórese en el literal d) del inciso primero del artículo 9° propuesto,

luego de “instituciones privadas”, la expresión “y públicas calificadas como operadores de importancia vital”.

Incorpórese en el literal j) del inciso primero del artículo 9° propuesto, luego de “instituciones privadas”, la siguiente expresión “y públicas calificadas como operadores de importancia vital”.

Incorpórese en el literal j) del inciso primero del artículo 9°, luego del punto final, que pasa a ser punto y aparte, lo siguiente:

“Los requerimientos realizados por la Agencia deberán expresar el objeto de la solicitud, estar debidamente fundamentados, detallar los documentos, antecedentes o información solicitados y establecer un plazo razonable para su entrega, según corresponda, para efectos de determinar el cumplimiento de la normativa aplicable por parte del operador de importancia vital, y siempre y cuando no se altere el normal desenvolvimiento de sus actividades.

El requerimiento de acceso a redes o sistemas informáticos, así como la restricción de su acceso o uso, podrá efectuarse previa resolución fundada dictada por la Agencia, cuando resulte indispensable para fiscalizar el cumplimiento de la normativa aplicable al operador de importancia vital o contrarrestar ciberataques o incidentes de ciberseguridad, según corresponda. Se entenderá que el requerimiento es indispensable cuando se cumpla con los siguientes requisitos:

1. Un incidente de ciberseguridad comprometa o dañe otra red o sistema informático.

2. El operador de importancia vital esté imposibilitado de contrarrestar las amenazas originadas por el incidente de ciberseguridad.

3. No es posible utilizar una medida menos gravosa que permita contrarrestar el incidente de ciberseguridad.

4. El acceso a la red o sistemas informáticos, así como la restricción de su acceso o uso, según corresponda, no cause un daño desproporcional a terceros o al titular de la red o sistema informático”.

Reemplácese el párrafo segundo del literal n) del inciso primero del artículo 9° propuesto por el siguiente:

“La Agencia contará con las facultades necesarias para el cumplimiento de su función fiscalizadora, comprendiendo:

1. Llevar a cabo inspecciones, incluyendo las realizadas por vía remota, por medio de sus empleados o centros de certificación acreditados.

En las inspecciones que la Agencia realice en el marco de la fiscalización, podrá integrar su propio personal con el de la entidad fiscalizada.

2. Realizar o establecer auditorías de seguridad periódicas o específicas, por medio de sus empleados o centros de certificación acreditados.

Los resultados de cualquier auditoría de seguridad específica se pondrán a disposición de la Agencia. Los costos de dicha auditoría de seguridad específica realizada por un centro de certificación acreditado serán costeados por la entidad auditada, salvo en aquellos casos debidamente fundamentados en los que la Agencia establezca lo contrario.

Tras la evaluación de la información o del resultado de cualquier auditoría de seguridad la Agencia podrá dictar instrucciones particulares a la entidad auditada para subsanar las deficiencias detectadas.

3. Realizar auditorías específicas, por medio de sus empleados, que estén justificadas por la ocurrencia de un incidente de ciberseguridad que pueda tener efectos significativos, de conformidad con el artículo 23, o una infracción a las disposiciones de la presente ley.

4. Realizar análisis de seguridad basados en criterios de evaluación de riesgos objetivos, no discriminatorios, justos y transparentes, con la cooperación de la entidad en cuestión cuando fuere necesario.

5. Solicitar pruebas de la implementación de los planes de continuidad operacional y ciberseguridad, referidos en la letra c) del artículo 6°.

6. 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, incluyendo especialmente el conocimiento de la información necesaria para prevenir, identificar, eliminar o contrarrestar un incidente de ciberseguridad.

No estarán obligadas a concurrir a declarar las personas indicadas en el artículo 361 del Código de Procedimiento Civil, a las cuales la Agencia, para los fines expresados en el párrafo precedente, deberá pedir declaración por escrito.

7. Designar empresas de auditoría externa o centros de certificación acreditados en las entidades fiscalizadas, para que realicen las tareas que específicamente les encomiende, con las facultades que estime necesarias, comprendiendo la supervisión, durante un período determinado, del cumplimiento por parte de las entidades fiscalizadas de las obligaciones previstas en los artículos 5° y 6° de la presente ley.

Para estos efectos, las empresas de auditoría externa o centros de certificación acreditados designados por la Agencia deberán observar de manera estricta el deber de reserva que esta ley impone, así como los consagrados por la ley N°19.628, sobre protección de la vida privada, y serán remunerados por la entidad fiscalizada. La remuneración gozará del privilegio establecido en el Nº4 del artículo 2472 del Código Civil.

8. Contratar o hacer contratar por las entidades fiscalizadas los servicios de peritos o técnicos para los trabajos que les encomiende, los que serán de cargo de dichas personas o entidades fiscalizadas.

9. Adoptar o solicitar la adopción de las medidas tendientes a corregir las deficiencias que observare, en general, en el ejercicio de sus atribuciones de fiscalización.

10. Solicitar a los centros de certificación acreditados que suspendan temporalmente una certificación referente a una parte o la totalidad de los servicios o actividades de que se trate prestados por la entidad fiscalizada, cuando esta no adopte las medidas referidas en el párrafo tercero del número 2 o el número 10 anterior.

11. Requerir a las entidades fiscalizadas que proporcionen al público, por las vías que señale, información veraz, suficiente y oportuna sobre determinados aspectos del incumplimiento de la presente ley de una manera específica. La Agencia podrá efectuar directamente las publicaciones que fueren necesarias para los fines precisados en este numeral, con cargo a las entidades fiscalizadas".

Incorpórese en el literal ñ) del inciso primero del artículo 9° propuesto, luego de "instituciones públicas y privadas", la siguiente expresión "calificadas como operadores de importancia vital".

Incorpórese los siguientes literales antepenúltimo y penúltimo al inciso primero del artículo 9° propuesto, del siguiente tenor:

"x) Formular las denuncias que correspondieren al Ministerio Público por los hechos de que tomare conocimiento en el ejercicio de sus atribuciones y que pudieren revestir caracteres de delito, sin perjuicio de los deberes generales que sobre la materia determine la ley.

y) Evacuar los informes que le requieran los fiscales del Ministerio Público que estén dirigiendo investigaciones criminales, siempre que correspondan a materias de su competencia y se refieran a información que esté disponible en sus archivos".

Al artículo 9 que ha pasado a ser 11, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon las siguientes indicaciones N°59, 60, 61, 62, 64, 67, 68, 69 y 70:

Introdúcense las siguientes modificaciones al literal b) del artículo 9°:

i. Intercálase entre la expresión "instituciones públicas y privadas" y la coma que le sigue, la expresión "calificadas como operadores de importancia vital";

ii. Intercálase entre la palabra "ciberseguridad" y el punto aparte, un coma seguido de lo siguiente: "dentro del ámbito de su competencia".

Intercálase en el literal d) del artículo 9°, entre las frases “instituciones privadas” y “y al CSIRT Nacional”, lo siguiente “calificadas como operadores de importancia vital.

En el literal h) del artículo 9°, suprímase la frase “y que se encuentre en posesión de estas instituciones”;

Introdúcense las siguientes modificaciones al literal j) del artículo 9°:

i. Intercálase entre las frases “instituciones privadas” y “cualquier documento” la expresión “calificadas como operadores de importancia vital”;

ii. Suprímase la frase “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, sobre protección de la vida privada”;

iii. Incorpórese el siguiente párrafo segundo, nuevo:

“Los requerimientos realizados por la Agencia deberán ser fundados y expresar el objeto de la solicitud y detallar claramente los documentos, antecedentes o información solicitada, según corresponda. Queda prohibido a la Agencia formular solicitudes genéricas.”

Introdúcense las siguientes modificaciones al literal m) del artículo 9°:

i. Suprímase la expresión “coordinar”;

ii. Suprímase la expresión “interagencialmente”.

Introdúcense las siguientes modificaciones al párrafo segundo del literal n) del artículo 9°:

i. Sustitúyese la expresión “todas las facultades que fueren necesarias” por “las facultades que le señale la ley”;

ii. Sustitúyese el siguiente la coma que sigue a la palabra “fiscalizadora” por un punto seguido y el texto “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” por el que se indica a continuación:

“Para el cumplimiento de su función podrá:

1. Llevar a cabo inspecciones, incluyendo las realizadas por vía remota.

2. Realizar o establecer auditorías de seguridad periódicas o específicas, por medio de sus empleados. Tras la evaluación de la información o del resultado de cualquier auditoría de seguridad la Agencia podrá dictar instrucciones particulares a la entidad auditada para subsanar las deficiencias detectadas.

3. Realizar análisis de seguridad basados en criterios de evaluación de riesgos objetivos, no discriminatorios, justos y transparentes, con la cooperación de la entidad en cuestión cuando fuere necesario.

4. Solicitar pruebas de la implementación de los planes de continuidad operacional y ciberseguridad, referidos en la letra c) del artículo 6°.

5. 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, incluyendo especialmente el conocimiento de la información necesaria para prevenir, identificar, eliminar o contrarrestar un incidente de ciberseguridad.

No estarán obligadas a concurrir a declarar las personas indicadas en el artículo 361 del Código de Procedimiento Civil, a las cuales la Agencia, para los fines expresados en el párrafo precedente, deberá pedir declaración por escrito.

6. Adoptar o solicitar la adopción de las medidas tendientes a corregir las deficiencias que observare, en general, en el ejercicio de sus atribuciones de fiscalización.

7. Requerir a las entidades fiscalizadas que proporcionen al público, por las vías que señale, información veraz, suficiente y oportuna sobre determinados aspectos del incumplimiento de la presente ley de una manera específica."

Intercálase en el literal ñ) del artículo 9°, entre las palabras "privadas" y "respecto", la frase "calificadas como operadores de importancia vital".

Intercálase en el literal p) del artículo 9°, entre la palabra "funciones" y el punto aparte, lo siguiente: "dentro del ámbito de sus competencias."

Suprímase el literal t) del artículo 9°.

Al artículo 9 que ha pasado a ser 11, el diputado señor Jorge Alessandri y la diputada señora Gloria Naveillán, formularon las siguientes indicaciones N°63, 65 y 66:

Para agregar al final de la letra j) del artículo 9, lo siguiente, a continuación de N°19.628; "y a lo que define la presente ley y sus reglamentos".

Para sustituir el artículo 9° literal n) inciso segundo del proyecto de ley, por el siguiente: "Para el cumplimiento de su función fiscalizadora, la Agencia podrá realizar inspecciones; auditorías; análisis de seguridad o evaluar un sistema de gestión de seguridad de la información; requerir el acceso a sistemas; citar a declarar a cualquier persona que, a cualquier título, preste o haya prestado servicios para las entidades fiscalizadas y a toda otra persona que hubiere ejecutado y celebrado con ellas actos y convenciones de cualquier naturaleza; establecer la forma, plazos y procedimientos para que las entidades fiscalizadas cumplan la obligación de presentar los antecedentes y explicaciones referidos precedentemente, además de las facultades que esta ley le encomiende con el objeto evitar o resolver incidentes de ciberseguridad".

Para insertar en la letra o) (inciso 2 de la letra N?) del artículo 9°, a continuación de las palabras "función fiscalizadora" lo siguiente: "de acuerdo a lo que define la presente ley y sus reglamentos"

Luego, a**l artículo 9 que ha pasado a ser 11, el Ejecutivo formuló la siguiente indicación sustitutiva:**

"Artículo 11. 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 los protocolos y estándares que señala el artículo 7; las instrucciones generales y particulares, de carácter obligatorio, para las instituciones, tanto públicas como privadas obligadas por la presente ley; y las demás disposiciones necesarias para la aplicación y el cumplimiento de esta ley y sus reglamentos.

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 al CSIRT Nacional y a los demás pertenecientes a la Administración del Estado; y requerir de estos la información que sea necesaria para el cumplimiento de sus fines.

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) Calificar, mediante resolución fundada y en la forma prevista en los artículos 4, 5 y 6 de esta ley, a los servicios esenciales y a los operadores de importancia vital.

h) Requerir a 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, conforme lo dispuesto en el literal g) del artículo 8 de la presente ley.

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 de la Administración del Estado y a las instituciones privadas señaladas en el artículo 4 de la presente ley acceso a la información necesaria para prevenir la ocurrencia de incidentes de ciberseguridad o para gestionar uno que ya hubiera ocurrido. Especialmente, podrá requerir el acceso al registro de actividades de las redes y sistemas informáticos que permitan comprender detalles de los incidentes de seguridad que puedan haber ocurrido.

Para el ejercicio de esta atribución, la instrucción siempre tendrá carácter particular, debiendo especificarse la información solicitada y fundarse debidamente. Cuando la información referida en el inciso anterior incluya datos personales estos deberán ser anonimizados, siempre que ello no entorpezca el ejercicio de las funciones de la Agencia. En cualquier caso, los datos personales sólo podrán ser tratados dando estricto cumplimiento a lo dispuesto en la ley 19.628, y en particular, al principio de finalidad, sin perjuicio de lo que define la presente ley y sus reglamentos.

k) Requerir, mediante instrucción de su Director o Directora, en casos de incidentes de impacto significativo cuya gestión lo haga imprescindible, el acceso a redes o sistemas informáticos. Este requerimiento deberá notificarse sin demora al requerido, debiendo éste dar las facilidades que sean necesarias.

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.

l) Cooperar con organismos públicos e instituciones privadas, 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 autoridades nacionales de ciberseguridad extranjeras o sus homólogos y con los organismos internacionales con competencia en materia de ciberseguridad.

Cuando se trate de la cooperación con Estados y organizaciones internacionales, dicha actividad deberá realizarse en coordinación con el Ministerio de Relaciones Exteriores, en conformidad con lo previsto en el inciso primero del artículo 2 de la ley N°21.080.

m) Prestar**,** cuando sus recursos humanos, técnicos y financieros así lo permitan, 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 mencionada ley N°19.628.

n) 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.

ñ) 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.

Para el cumplimiento de su función fiscalizadora, la Agencia podrá realizar inspecciones; instruir de manera particular auditorías por sí o mediante terceros autorizados y análisis de seguridad basados en criterios de evaluación de riesgos objetivos, los cuales deberán ser no discriminatorios, equitativos y transparentes. La entidad fiscalizada deberá cooperar en todo momento con los funcionarios de la Agencia o con los terceros autorizados por ella, según corresponda.

Asimismo, la Agencia podrá requerir el acceso a sistemas informáticos, datos, documentos y demás información que fuere necesaria para el desempeño de sus funciones de supervisión y fiscalización; instruir de manera particular a los sujetos obligados que realicen pruebas que demuestren la implementación de los planes de continuidad operacional y ciberseguridad, referidos en la letra c) del artículo 8 °. Adicionalmente, podrá citar a declarar, respecto de hechos cuyo conocimiento estime necesario para el cumplimiento de sus funciones, a los socios, directores, administradores, representantes, empleados, y cualquier persona que, a cualquier título, preste o haya prestado servicios para las personas o entidades fiscalizadas, así como a toda persona que hubiere ejecutado o celebrado con ellas actos o convenciones de cualquier naturaleza. No obstante, no estarán obligadas a concurrir a declarar las personas indicadas en el artículo 361 del Código de Procedimiento Civil, a las cuales la Agencia, para los fines expresados en el párrafo precedente, deberá pedir declaración por escrito.

Para el ejercicio de esta atribución podrá establecer la forma, plazos y procedimientos para que las entidades fiscalizadas cumplan la obligación de presentar los antecedentes e informaciones referidos en los párrafos precedentes.

o) Instruir el inicio de procedimientos sancionatorios y sancionar las infracciones e incumplimientos en que incurran las instituciones obligadas por la presente ley respecto de sus disposiciones, reglamentos e instrucciones generales y particulares que emita la Agencia. Para tales efectos, y de manera fundada, podrá citar a declarar, en los términos señalados en el literal n) de este artículo, 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. La declaración podrá tomarse presencialmente o por otros medios que aseguren su integridad y fidelidad.

p) 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.

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

r) Informar al CSIRT de la Defensa Nacional y a los CSIRT de los organismos de la Administración del Estado 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.

s) 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.

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

u) 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.

v) 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.

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

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

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

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

Acto seguido, el debate es en torno a la indicación sustitutiva del Ejecutivo respecto del artículo 9º que pasa a ser 11.

E**l diputado señor Diego Schalper**, señaló que este artículo es el corazón del proyecto y por lo mismo hay que analizar en profundidad letra por letra, escuchar a los expertos, ya que el funcionamiento y atribuciones de la Agencia como se propone sería un organismo muy robusto, y eso puede no ser conveniente.

Comentó, respecto a la letra g), se establece que se va a calificar a aquellos que son servicios esenciales y los operadores de vital importancia, en el fondo está fijando en gran medida el ámbito de aplicación de esta ley, y por ello es importante saber si se está considerando algún elemento de impugnación o de apelación a esa calificación.

Además, respecto a la letra j), expresó su preocupación en cuanto a la protección de los datos personales, por cuanto establecen que se dará cumplimiento a lo dispuesto en la ley N°19.628, siempre que ello no entorpezca el ejercicio de las funciones de la Agencia, por lo que prevalece el cumplimiento de los objetivos de la Agencia no así del respeto a los datos personales, lo que daría a malas interpretaciones.

Asimismo, en cuanto a la letra n), desde el punto de vista de la coordinación interagencial en materia de seguridad nacional, se refiere a atribuciones de mayor magnitud, y por ello es importante saber si en otros países es la misma entidad la que fiscaliza los delitos de ciberseguridad o las situaciones de ciberseguridad de una empresa privada la que simultáneamente además está a cargo de la coordinación interagencial en materia de defensa nacional.

Por otra parte, en la letra ñ), se les otorga atribuciones tales como citar a declarar personas, y la posibilidad de requerir procedimientos sancionatorios, es decir cuestiones complejas que pueden atentar con el debido proceso y de la posibilidad de poder impugnar ese tipo de decisiones, por lo que preocupa que termine siendo un organismo con funciones de juez y parte, o sea quien investiga también sanciona. Hay una seria de cuestiones en materia procesal penal, que en esta propuesta son inconstitucionales.

El **diputado señor Raúl Leiva,** señaló que este artículo le atribuye a la Agencia un poder omnímodo nunca antes visto, saltándose incluso el control jurisdiccional, no hay un símil en la administración pública o en el Estado de Chile que posea tal poder o atribución, considerando además que la dirige una sola persona. Comentó incluso que pareciera que el Director o Directora de la Agencia tuviera más atribuciones que el mismo ministro de seguridad pública que se pretende regular.

Se sumó a la preocupación de falta de sistema de control respecto a las letras de este artículo comentado por el diputado Schalper.

El **diputado señor José Miguel Castro,** solicitó reabrir el debate del artículo 4 de este proyecto de ley, para poder incorporar una indicación relativa a los servicios esenciales que va a colaborar con la discusión.

El **presidente diputado señor Jorge Alessandri,** recabó el acuerdo, y luego de discutir y votar el artículo 9 que ha pasado a ser 11, se reabre la discusión del artículo 4.

El **diputado señor Henry Leal**, solicitó se pueda requerir a la Biblioteca del Congreso Nacional, para que realice un informe en derecho comparado sobre la

existencia de una institución u organismo con las características y atribuciones que la indicación del Ejecutivo formula en relación con la Agencia de Ciberseguridad.

El **diputado señor Andrés Jouannet,** indicó preocuparle la letra n), si bien concuerda con que debe existir coordinación interagencial en relación con la seguridad nacional, sin embargo, al respecto, existe información muy delicada y sensible que solo algunas autoridades especificas pueden manejar de maneras reservada.

Agregó, que, si bien debe existir un control de parte del Estado por sobre la Agencia, entiende el sentido de rapidez con la que se debe operar en casos de ataques cibernautas.

El **diputado señor Cristián Araya,** manifestó que le preocupa el exceso de poder que se le entrega a una sola persona, la letra k) establece que el Director o Directora no tiene restricciones para el acceso o uso de redes o sistemas informáticos, existe sin duda una concentración de poder, por lo que sugiere analizarlo muy bien y cotar letra por letra.

Igualmente le preocupa la redacción a la letra n), que crea una especie de supraestructura donde la Agencia podría inmiscuirse en una serie de espacios que requieren por su naturaleza cierta autonomía y coordinación en otros planos.

El **asesor legislativo participante de la mesa de trabajo, abogado señor Juan Ignacio Gómez,** comentó que, en relación con las facultades de la Agencia, en sus artículos 4, 5 y 6, que ya la Comisión aprobó, y que tiene un correlato con la letra g) del artículo 9 que ha pasado a ser 11. Respecto a la impugnación, en el artículo 35 del proyecto actual 37, existe el reclamo judicial general sin perjuicio que el procedimiento de los artículos 4, 5 y 6 también tiene instancias iterativas entre los regulados y la Agencia, específicamente se contemplan procesos de consulta pública y otras materias que han permitido que el proceso desde un inicio general ya sea más particular.

Asimismo, señaló que respecto a la letra k), comparte que este tipo de medidas deberían tener un correlato en autorizaciones judiciales.

Y, por último, respecto a la idea de la interagencial, se espera que exista una explicación de fondo que converse con el resto de las normas de la administración.

El **diputado señor Andrés Jouannet,** sugirió que pueda existir la figura de un subdirector como a su vez un Consejo de expertos al que se le pueda consultar para situaciones complejas y con responsabilidades.

Los **diputados señores Raúl Leiva y Diego Schalper,** expresaron estar de acuerdo con el texto de la letra g), siempre y cuando quede constancia en la historia fidedigna de la ley que es una norma espejo a los artículos 4, 5 y 6 de la misma ley, desde el punto de vista de la reclamación e impugnación.

El **presidente diputado señor Jorge Alessandri**, solicitó al Ejecutivo que puedan redactar una propuesta que considere la existencia de una administración colegiada de expertos a los que se le pueda responsabilizar y consultar, y no dejar toda la carga a una sola persona.

Por la dificultad y complejidad del artículo, se determinó que se procederá a discutir y votar letra por letra de la indicación sustitutiva formulada por el Ejecutivo.

Puesta en votación **la letra a) de la indicación sustitutiva del Ejecutivo al artículo 9 que ha pasado a ser 11, se aprueba por unanimidad**. Votan a favor las y los diputados señores Jorge Alessandri (presidente), José Miguel Castro, Lorena Fries, Andrés

Jouannet, Henry Leal, Raúl Leiva, Alejandra Placencia y Diego Schalper. Sin votos en contra. Sin abstenciones. **(8-0-0).**

Puesta en votación **la letra b) de la indicación sustitutiva del Ejecutivo al artículo 9 que ha pasado a ser 11,** se aprueba por unanimidad. Votan a favor las y los diputados señores Jorge Alessandri (presidente), José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal, Raúl Leiva, Alejandra Placencia y Diego Schalper. Sin votos en contra. Sin abstenciones. **(8-0-0).**

Puesta en votación **la letra c) de la indicación sustitutiva del Ejecutivo al artículo 9 que ha pasado a ser 11, se aprueba por unanimidad.** Votan a favor las y los diputados señores Jorge Alessandri (presidente), José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal, Raúl Leiva, Alejandra Placencia y Diego Schalper. Sin votos en contra. Sin abstenciones. **(8-0-0).**

Puesta en votación **la letra d) de la indicación sustitutiva del Ejecutivo al artículo 9 que ha pasado a ser 11**, **se aprueba por unanimidad**. Votan a favor las y los diputados señores Jorge Alessandri (presidente), José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal, Raúl Leiva, Alejandra Placencia y Diego Schalper. Sin votos en contra. Sin abstenciones. **(8-0-0).**

Puesta en votación **la letra e) de la indicación sustitutiva del Ejecutivo al artículo 9 que ha pasado a ser 11, se aprueba por unanimidad.** Votan a favor las y los diputados señores Jorge Alessandri (presidente), José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal, Raúl Leiva, Alejandra Placencia y Diego Schalper. Sin votos en contra. Sin abstenciones. **(8-0-0).**

Puesta en votación **la letra f) de la indicación sustitutiva del Ejecutivo al artículo 9 que ha pasado a ser 11, se aprueba por unanimidad**. Votan a favor las y los diputados señores Jorge Alessandri (presidente), José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal, Raúl Leiva, Alejandra Placencia y Diego Schalper. Sin votos en contra. Sin abstenciones. **(8-0-0).**

Puesta en votación **la letra g) de la indicación sustitutiva del Ejecutivo al artículo 9 que ha pasado a ser 11, se aprueba por unanimidad**. Votan a favor las y los diputados señores Jorge Alessandri (presidente), José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal, Raúl Leiva, Alejandra Placencia y Diego Schalper. Sin votos en contra. Sin abstenciones. **(8-0-0).**

En otra sesión, se continuó con la discusión y votación del actual artículo 9 que ha pasado a ser artículo 11.

La **asesora legislativa del Ministerio del Interior, abogada señora Michelle Bordachar,** expresó que a propósito de las observaciones de las y los diputados en relación con las atribuciones de la Agencia, principalmente enfocada en la preocupación de que toda la responsabilidad recae en una sola persona que es la figura del Director, y que por otra parte, para algunos casos se pueda acceder a datos sin requerir una orden judicial, el Ejecutivo formuló indicaciones, que modifican el actual artículo 9 que ha pasado a ser 11, para conciliar aquello. Es decir, sí se requerirá orden judicial para el acceso a datos y se incorporará la existencia de un Subdirector.

Se da lectura a las letras que aún no se han discutido ni votado de la indicación del Ejecutivo que reemplaza el actual artículo 9, que ha pasado a ser artículo 11, por el siguiente:

“h) Requerir a 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, conforme lo dispuesto en el literal g) del artículo 8 de la presente ley.”

Puesta en **votación la letra h) de la indicación del Ejecutivo que reemplaza el actual artículo 9 que ha pasado a ser 11, se aprueba por unanimidad.** Votan a favor los diputados señores José Miguel Castro, Henry Leal, Andrés Longton, Raúl Leiva y Diego Schalper. Sin abstenciones. **(5-0-0).**

Se da lectura a la letra i) de la indicación del Ejecutivo que reemplaza el actual artículo 9, que ha pasado a ser artículo 11, por el siguiente:

“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.”

El **diputado señor Diego Schalper**, manifestó que esta redacción implicaría una modificación a la Ley orgánica constitucional del Ministerio de Educación, ya que un organismo extrínseco venga a diseñar la malla curricular de las universidades, es algo nunca antes visto a nivel comparado. Ahora bien, el que existan campañas educativas en relación con la ciberseguridad, es necesario y adecuado, pero de ahí a entrometerse a diseñar o implementar planes educativos en coordinación con el Ministerio de Educación se escapa de lo objetivo y lógico de esta ley.

El **diputado señor Raúl Leiva y la diputada señora Gloria Naveillán,** señalaron que, en vista de lo discutido, lo más adecuado, para que se desarrolle una cultura de ciberseguridad en la ciudadanía, es que la Agencia proponga y coopere con el diseño e implementación de planes y acciones de educación al respecto.

Quedó pendiente la discusión y la votación de la letra i), a la espera de una nueva redacción de parte del Ejecutivo que recoja las sugerencias vertidas.

Se da lectura a la letra j) de la indicación del Ejecutivo que reemplaza el actual artículo 9, que ha pasado a ser artículo 11, por el siguiente:

“j) Requerir a los organismos de la Administración del Estado y a las instituciones privadas señaladas en el artículo 4 de la presente ley acceso a la información necesaria para prevenir la ocurrencia de incidentes de ciberseguridad o para gestionar uno que ya hubiera ocurrido. Especialmente, podrá requerir el acceso al registro de actividades de las redes y sistemas informáticos que permitan comprender detalles de los incidentes de seguridad que puedan haber ocurrido.

Para el ejercicio de esta atribución, la instrucción siempre tendrá carácter particular, debiendo especificarse la información solicitada y fundarse debidamente. Cuando la información referida en el inciso anterior incluya datos personales estos deberán ser anonimizados, siempre que ello no entorpezca el ejercicio de las funciones de la Agencia. En cualquier caso, los datos personales sólo podrán ser tratados dando estricto cumplimiento a lo dispuesto en la ley 19.628, y en particular, al principio de finalidad, sin perjuicio de lo que define la presente ley y sus reglamentos.”

El **diputado señor Diego Schalper y la diputada señora Gloria Naveillán**, en virtud de lo argumentado en su oportunidad por expertos, señalaron que si al Ministerio Público se le exige, para acceder a cualquier tipo de información, una orden de un Tribunal, con mayor razón a un órgano de la administración se le debiera requerir lo mismo, a menos que la redacción se especifique y establezca que solo se refiere, es decir exclusivamente y no especialmente, el registro de actividades de las redes y sistemas informáticos.

Quedó pendiente la discusión y la votación de la letra j), a la espera de una nueva redacción de parte del Ejecutivo que recoja las sugerencias vertidas.

Se da lectura a la letra k) de la indicación del Ejecutivo que reemplaza el actual artículo 9, que ha pasado a ser artículo 11, por el siguiente:

"k) Requerir, mediante instrucción de su Director o Directora, en casos de incidentes de impacto significativo cuya gestión lo haga imprescindible, el acceso a redes y sistemas informáticos. Este requerimiento deberá notificarse sin demora al requerido en la dirección de correo electrónico que le que hubiere sido facilitada a la Agencia conforme con el reglamento. Una vez notificado, el requerido deberá dar las facilidades de acceso que sean necesarias. Con todo, si el requerido fuese una institución privada, de las señaladas en el artículo 4, podrá oponerse mediante la interposición del reclamo establecido en el artículo 37.

En caso de no existir oposición dentro de los plazos legales establecidos, la Agencia podrá acceder a las redes y sistemas objeto del requerimiento.

Si la naturaleza del incidente requiriese una gestión urgente y el requerido se opusiere, la atribución señalada en el párrafo precedente podrá ejercerse sin que proceda el reclamo previsto en el artículo 37, siempre que ella sea autorizada judicialmente en la forma señalada en el párrafo siguiente. Corresponderá a un ministro de la Corte de Apelaciones de Santiago conocer del requerimiento. Anualmente, el Presidente de la Corte de Apelaciones de Santiago deberá designar, por sorteo, a dos de sus miembros para cumplir esta labor. Si ninguno de los ministros estuviere en funciones, corresponderá otorgar la autorización al Presidente de la Corte o a quien lo subrogue.

La autorización deberá solicitarse por escrito, para tales efectos todos los días y horas se entenderán hábiles.

La solicitud deberá fundarse en hechos específicos que justifiquen la urgencia. Para su conocimiento, se deberá citar a una audiencia en el más breve plazo en la que se escuchará a las partes, debiendo resolverse en ella. En contra de la resolución que dicte la Corte procederá el recurso de apelación que, en el caso de interponerse en contra de la resolución que otorga el acceso solicitado, procederá en el solo efecto devolutivo.

En caso de que se requiriera la restricción del acceso o uso de redes o sistemas informáticos se estará a lo dispuesto en este literal. No obstante, la Agencia deberá actuar conjuntamente con la autoridad sectorial correspondiente."

La **asesora legislativa del Ministerio del Interior, abogada señora Michelle Bordachar,** comentó que esta letra refleja una situación más compleja que la anterior, donde hay más sistemas comprometidos en los que requiere acercarse a la corroboración de información, con independencia que la entidad la entregue, ya que se deben observar las máquinas para así comprender las características y alcances del incidente. Esta idea proviene de la Unión Europea que les ordena a sus países que al menos la Agencia tenga la posibilidad de acceder remotamente a los datos, en ciertos casos, sin perjuicio que se requiera de una orden judicial y acceder a estos datos siempre que sea estrictamente necesario.

Por existir reparos respecto de la redacción de la letra k), quedó pendiente su discusión y la votación, a la espera de una nueva y más comprensiva redacción de parte del Ejecutivo.

Finalmente, s**e continuó con la votación del resto de las letras del artículo 9 que ha pasado a ser 11, que, en sesión del 18 de octubre, se dio lectura a cada una de ellas, y se votó hasta la letra h).**

Se **acordó** leer, discutir y votar las letras i), j) y k) del artículo 9 que ha pasado a ser 11, y sus indicaciones de manera conjunta.

A las letras j) y k) del artículo 9 que ha pasado a ser 11, **el Ejecutivo formuló las siguientes primeras indicaciones N°s 12 y 13:**

"12. Para modificar el literal j) del artículo 9°, en el siguiente sentido:

a. Elimínase, en el literal j), la frase ", así como los consagrados por la ley N°19.628, sobre protección de la vida privada".

b. Agrégase, a continuación del punto final, la frase: "Cuando la información a la que tenga acceso la Agencia incluya datos personales estos deberán ser anonimizados siempre que ello sea posible y no entorpezca el ejercicio de las funciones de la Agencia. En cualquier caso, los datos personales sólo podrán ser tratados dando estricto cumplimiento a lo dispuesto en la ley 19.628.".

13. Para reemplazar el literal k) del artículo 9°, por el siguiente:

"k) Cooperar con organismos públicos e instituciones privadas, 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 autoridades nacionales de ciberseguridad extranjeras o sus equivalentes y con los organismos internacionales con competencia en materia de ciberseguridad.

Cuando se trate de la cooperación con Estados y organizaciones internacionales, dicha actividad deberá realizarse en coordinación con el Ministerio de Relaciones Exteriores, en conformidad a lo previsto en el inciso primero del artículo 2 de la ley N°21.080."."

A la letra j) del artículo 9 que ha pasado a ser 11, **los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°62:**

"Introdúcense las siguientes modificaciones al literal j) del artículo 9°:

i. Intercálase entre las frases "instituciones privadas" y "cualquier documento" la expresión "calificadas como operadores de importancia vital";

ii. Suprímase la frase "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, sobre protección de la vida privada";

iii. Incorpórese el siguiente párrafo segundo, nuevo: Los requerimientos realizados por la Agencia deberán ser fundados y expresar el objeto de la solicitud y detallar claramente los documentos, antecedentes o información solicitada, según corresponda. Queda prohibido a la Agencia formular solicitudes genéricas.".

A la letra j) del artículo 9 que ha pasado a ser 11**, el diputado señor Jorge Alessandri y la diputada señora Gloria Naveillán, formularon la siguiente indicación N°63:**

"Para agregar al final de la letra j) del artículo 9, lo siguiente, a continuación de N°19.628; "y a lo que define la presente ley y sus reglamentos".

A la letra j) del artículo 9 que ha pasado a ser 11, **el diputado señor Jorge Alessandri y la diputada señora Gloria Naveillán, formuló las siguientes indicaciones N°s 34 y 35:**

34. Incorpórese en el literal j) del inciso primero del artículo 9° propuesto, luego de "instituciones privadas", la siguiente expresión "y públicas calificadas como operadores de importancia vital".

35. Incorpórese en el literal j) del inciso primero del artículo 9°, luego del punto final, que pasa a ser punto y aparte, lo siguiente:

"Los requerimientos realizados por la Agencia deberán expresar el objeto de la solicitud, estar debidamente fundamentados, detallar los documentos, antecedentes o información solicitados y establecer un plazo razonable para su entrega, según corresponda, para efectos de determinar el cumplimiento de la normativa aplicable por parte del operador de importancia vital, y siempre y cuando no se altere el normal desenvolvimiento de sus actividades.

El requerimiento de acceso a redes o sistemas informáticos, así como la restricción de su acceso o uso, podrá efectuarse previa resolución fundada dictada por la Agencia, cuando resulte indispensable para fiscalizar el cumplimiento de la normativa aplicable al operador de importancia vital o contrarrestar ciberataques o incidentes de ciberseguridad, según corresponda. Se entenderá que el requerimiento es indispensable cuando se cumpla con los siguientes requisitos:

1. Un incidente de ciberseguridad comprometa o dañe otra red o sistema informático.

2. El operador de importancia vital esté imposibilitado de contrarrestar las amenazas originadas por el incidente de ciberseguridad.

3. No es posible utilizar una medida menos gravosa que permita contrarrestar el incidente de ciberseguridad.

4. El acceso a la red o sistemas informáticos, así como la restricción de su acceso o uso, según corresponda, no cause un daño desproporcional a terceros o al titular de la red o sistema informático".

A la letra i), j) y k) del artículo 9 que ha pasado a ser 11, **el Ejecutivo formuló con fecha 25 de octubre, nueva propuesta, específicamente a lo referido a aquellas letras, por no existir consenso al respecto:**

"Para reemplazar el literal i), j) y k) del actual artículo 9, que ha pasado a ser artículo 11, por el siguiente:

"i) Diseñar e implementar planes y acciones de formación ciudadana, capacitación, fortalecimiento, difusión y promoción de la cultura en ciberseguridad.

j) Requerir a los organismos de la Administración del Estado y a las instituciones privadas señaladas en el artículo 4 de la presente ley acceso a la información estrictamente necesaria para prevenir la ocurrencia de incidentes de ciberseguridad o para gestionar uno que ya hubiera ocurrido. Para lo anterior, podrá requerir la entrega del registro de actividades de las redes y sistemas informáticos que permitan comprender detalles de los incidentes de ciberseguridad que puedan haber ocurrido.

Para el ejercicio de esta atribución, la instrucción siempre tendrá carácter particular, debiendo especificarse la información solicitada y fundarse debidamente. Cuando la información referida en el inciso anterior pudiera incluir datos personales estos deberán ser anonimizados, siempre que ello sea posible sin entorpecer la gestión de incidentes. En cualquier caso, los datos personales sólo podrán ser tratados dando estricto cumplimiento a lo dispuesto en la ley 19.628, y en particular, al principio de finalidad, sin perjuicio de lo que define la presente ley y sus reglamentos.

Con todo, para efectos de lo dispuesto en esta ley, no se considerará que la dirección IP sea un dato personal.".

k) Requerir, mediante instrucción de su Director o Directora, en casos de incidentes de impacto significativo cuya gestión lo haga imprescindible, el acceso a redes y sistemas informáticos. Este requerimiento deberá notificarse sin demora al requerido a través de la dirección de correo electrónico que haya sido proporcionada a la Agencia, de conformidad con lo establecido en el reglamento. Una vez notificado, el requerido deberá proporcionar todas las facilidades de acceso que sean necesarias. En caso de que el requerido sea una institución privada de las señaladas en el artículo 4, podrá oponerse. Formulada la oposición la Agencia solo podrá acceder previa autorización judicial conforme lo dispuesto en los párrafos siguientes y no procederá el reclamo establecido en el artículo 37.

Corresponderá a un ministro de la Corte de Apelaciones de Santiago conocer del requerimiento. Anualmente, el Presidente de la Corte de Apelaciones de Santiago deberá designar, por sorteo, a dos de sus miembros para cumplir esta labor. Si ninguno de los ministros estuviere en funciones, corresponderá otorgar la autorización al Presidente de la Corte o a quien lo subrogue. La autorización deberá solicitarse por escrito y fundarse en hechos específicos que justifiquen la necesidad del requerimiento. Para tales efectos todos los días y horas se entenderán hábiles.

La resolución que autorice o deniegue el acceso a las redes y sistemas, deberá dictarse previa audiencia en el más breve plazo en la que se escuchará a las partes.

En contra de la resolución que dicte el Ministro de Corte procederá el recurso de apelación ante la Corte de Apelaciones de Santiago, que, en el caso de interponerse en contra de la resolución que otorga el acceso solicitado, procederá en el solo efecto devolutivo. La Corte de Apelaciones de Santiago podrá resolver la apelación en cuenta sin más trámite. Los autos se agregarán de manera extraordinaria y con preferencia a la tabla del día siguiente; pero si este fuere inhábil, deberá el tribunal funcionar extraordinariamente para el solo conocimiento del recurso. Si producto de la interposición de recusaciones o implicancias no hubiere tribunal, los autos serán conocidos el día siguiente, según las reglas precedentes.

En caso de que se requiriera la restricción del acceso o uso de redes o sistemas informáticos se estará a lo dispuesto en este literal. No obstante, la Agencia deberá actuar conjuntamente con la autoridad sectorial correspondiente.

El procedimiento dispuesto en los incisos precedentes también será aplicable los requerimientos de acceso a redes y sistemas informáticos a que se refiere en el inciso tercero del literal ñ) del presente artículo.”.”

El **presidente diputado señor Andrés Longton,** señaló que, si bien acordaron votar estar tres letras en una misma votación, respecto a la letra k), solicitó votación separada respecto a un extracto que dice relación con la frase “procederá en el solo efecto devolutivo”, ya que considera que debería ser “procederá en ambos efectos”, de tal manera al ser esta la regla general, en caso de rechazarse esa frase se entenderá que el recurso de apelación procederá en ambos efectos.

Puesta en votación la frase “procederá en el solo efecto devolutivo” de la letra k) de la indicación del Ejecutivo formulada en fecha 25 de octubre, se rechaza por la mayoría de los votos. Votan a favor las diputadas señoras Lorena Fries y Alejandra Placencia. Con votos en contra de los diputados señores Jorge Alessandri, José Miguel Castro y Andrés Longton (presidente). Sin abstenciones. **(2-3-0).**

Puesta en votación las letras i), j) y k) de la indicación del Ejecutivo formulada en fecha 25 de octubre, se aprueban por unanimidad. Votan a favor las y los diputados señores Jorge Alessandri, José Miguel Castro, Lorena Fries, Andrés Longton (presidente) y Alejandra Placencia. Sin votos en contra ni abstenciones. **(5-0-0).**

Por aprobarse las letras i), j) y k) de la indicación del Ejecutivo formulada en fecha 25 de octubre, con la eliminación de la frase “procederá en el solo efecto devolutivo”, reglamentariamente se rechazan, las letras i), j) y k) del artículo 9 aprobado por el Senado y las indicaciones N°s 12 y 13 del Ejecutivo y N°s 34, 35, 62 y 63 de parlamentarios.

Luego, se continuó **con la votación de las letras de la indicación formulada por el Ejecutivo al artículo 9 que ha pasado a ser 11, de fecha 11 de octubre, específicamente a lo referido a las letras l) y m):**

“l) Cooperar con organismos públicos e instituciones privadas, 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 autoridades nacionales de ciberseguridad extranjeras o sus homólogos y con los organismos internacionales con competencia en materia de ciberseguridad.

Cuando se trate de la cooperación con Estados y organizaciones internacionales, dicha actividad deberá realizarse en coordinación con el Ministerio de Relaciones Exteriores, en conformidad con lo previsto en el inciso primero del artículo 2 de la ley N°21.080.

m) Prestar, cuando sus recursos humanos, técnicos y financieros así lo permitan, 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 mencionada ley N°19.628.”.

Por aprobarse, las letras l) y m) de la indicación del Ejecutivo formulada en fecha 11 de octubre, reglamentariamente se rechazan, las letras l) y m) del artículo 9 aprobado por el Senado.

Se continuó con la votación de la letra n) del artículo 9 que ha pasado a ser 11.

A la letra n) del artículo 9 que ha pasado a ser 11, **el Ejecutivo primeramente formuló la siguiente indicación N°14:**

“Para reemplazar el segundo párrafo del literal n) del artículo 9°, por el siguiente:

“Para el cumplimiento de su función fiscalizadora, la Agencia podrá examinar sin restricción alguna y por los medios que estime pertinentes todas las actividades, archivos y documentos de las entidades o actividades fiscalizadas o de sus matrices, filiales o coligadas, y requerir de ellas o de sus administradores, asesores o personal, los antecedentes y explicaciones que juzgue necesarios para obtener información acerca de cualquier punto que convenga esclarecer para efectos de determinar el cumplimiento de la normativa aplicable por parte de la entidad fiscalizada. Asimismo, la Agencia podrá realizar inspecciones; auditorías; análisis de seguridad o evaluar un sistema de gestión de seguridad de la información; requerir el acceso a sistemas; citar a declarar a cualquier persona que, a cualquier título, preste o haya prestado servicios para las entidades fiscalizadas y a toda otra persona que hubiere ejecutado y celebrado con ellas actos y convenciones de cualquier naturaleza; establecer la forma, plazos y procedimientos para que las entidades fiscalizadas cumplan la obligación de presentar los antecedentes y explicaciones referidos precedentemente; y, en general, requerir la adopción de todas las medidas preventivas o correctivas que se estimen necesarias y sean pertinentes, proporcionales y adecuadas para evitar o resolver incidentes de ciberseguridad. La Agencia también podrá solicitar información de otros organismos públicos, la que en caso de ser secreta o reservada.”.”.

A la letra n) del artículo 9 que ha pasado a ser 11, **el diputado señor Andrés Jouannet, formuló la siguiente indicación N°36:**

“Reemplácese el párrafo segundo del literal n) del inciso primero del artículo 9° propuesto por el siguiente:

“La Agencia contará con las facultades necesarias para el cumplimiento de su función fiscalizadora, comprendiendo:

1. Llevar a cabo inspecciones, incluyendo las realizadas por vía remota, por medio de sus empleados o centros de certificación acreditados.

En las inspecciones que la Agencia realice en el marco de la fiscalización, podrá integrar su propio personal con el de la entidad fiscalizada.

2. Realizar o establecer auditorías de seguridad periódicas o específicas, por medio de sus empleados o centros de certificación acreditados.

Los resultados de cualquier auditoría de seguridad específica se pondrán a disposición de la Agencia. Los costos de dicha auditoría de seguridad específica realizada por un centro de certificación acreditado serán costeados por la entidad auditada, salvo en aquellos casos debidamente fundamentados en los que la Agencia establezca lo contrario.

Tras la evaluación de la información o del resultado de cualquier auditoría de seguridad la Agencia podrá dictar instrucciones particulares a la entidad auditada para subsanar las deficiencias detectadas.

3. Realizar auditorías específicas, por medio de sus empleados, que estén justificadas por la ocurrencia de un incidente de ciberseguridad que pueda tener efectos significativos, de conformidad con el artículo 23, o una infracción a las disposiciones de la presente ley.

4. Realizar análisis de seguridad basados en criterios de evaluación de riesgos objetivos, no discriminatorios, justos y transparentes, con la cooperación de la entidad en cuestión cuando fuere necesario.

5. Solicitar pruebas de la implementación de los planes de continuidad operacional y ciberseguridad, referidos en la letra c) del artículo 6°.

6. 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, incluyendo especialmente el conocimiento de la información necesaria para prevenir, identificar, eliminar o contrarrestar un incidente de ciberseguridad.

No estarán obligadas a concurrir a declarar las personas indicadas en el artículo 361 del Código de Procedimiento Civil, a las cuales la Agencia, para los fines expresados en el párrafo precedente, deberá pedir declaración por escrito.

7. Designar empresas de auditoría externa o centros de certificación acreditados en las entidades fiscalizadas, para que realicen las tareas que específicamente les encomiende, con las facultades que estime necesarias, comprendiendo la supervisión, durante un período determinado, del cumplimiento por parte de las entidades fiscalizadas de las obligaciones previstas en los artículos 5° y 6° de la presente ley.

Para estos efectos, las empresas de auditoría externa o centros de certificación acreditados designados por la Agencia deberán observar de manera estricta el deber de reserva que esta ley impone, así como los consagrados por la ley N°19.628, sobre protección de la vida privada, y serán remunerados por la entidad fiscalizada. La remuneración gozará del privilegio establecido en el Nº4 del artículo 2472 del Código Civil.

8. Contratar o hacer contratar por las entidades fiscalizadas los servicios de peritos o técnicos para los trabajos que les encomiende, los que serán de cargo de dichas personas o entidades fiscalizadas.

9. Adoptar o solicitar la adopción de las medidas tendientes a corregir las deficiencias que observare, en general, en el ejercicio de sus atribuciones de fiscalización.

10. Solicitar a los centros de certificación acreditados que suspendan temporalmente una certificación referente a una parte o la totalidad de los servicios o

actividades de que se trate prestados por la entidad fiscalizada, cuando esta no adopte las medidas referidas en el párrafo tercero del número 2 o el número 10 anterior.

11. Requerir a las entidades fiscalizadas que proporcionen al público, por las vías que señale, información veraz, suficiente y oportuna sobre determinados aspectos del incumplimiento de la presente ley de una manera específica. La Agencia podrá efectuar directamente las publicaciones que fueren necesarias para los fines precisados en este numeral, con cargo a las entidades fiscalizadas".

A la letra n) del artículo 9 que ha pasado a ser 11, **los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°64:**

"Introdúcense las siguientes modificaciones al literal n) del artículo 9°:
i. Suprímase la expresión "coordinar";
ii. Suprímase la expresión "interagencialmente

A la letra n) del artículo 9 que ha pasado a ser 11, **el diputado señor Jorge Alessandri, formuló la siguiente indicación N°65:**

"Para sustituir el artículo 9° literal n) inciso segundo del proyecto de ley, por el siguiente:

"Para el cumplimiento de su función fiscalizadora, la Agencia podrá realizar inspecciones; auditorías; análisis de seguridad o evaluar un sistema de gestión de seguridad de la información; requerir el acceso a sistemas; citar a declarar a cualquier persona que, a cualquier título, preste o haya prestado servicios para las entidades fiscalizadas y a toda otra persona que hubiere ejecutado y celebrado con ellas actos y convenciones de cualquier naturaleza; establecer la forma, plazos y procedimientos para que las entidades fiscalizadas cumplan la obligación de presentar los antecedentes y explicaciones referidos precedentemente, además de las facultades que esta ley le encomiende con el objeto evitar o resolver incidentes de ciberseguridad".

A la letra n) del artículo 9 que ha pasado a ser 11**, el diputado señor Jorge Alessandri y la diputada señora Gloria Naveillán, formularon la siguiente indicación N°66:**

"Para insertar en la letra n) del artículo 9°, a continuación de las palabras "función fiscalizadora" lo siguiente: "de acuerdo a lo que define la presente ley y sus reglamentos".

A la letra n) del artículo 9 que ha pasado a ser 11, **de los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°67:**

"Introdúcense las siguientes modificaciones al párrafo segundo del literal n) del artículo 9°:
i. Sustitúyese la expresión "todas las facultades que fueren necesarias" por "las facultades que le señale la ley";
ii. Sustitúyese el siguiente la coma que sigue a la palabra "fiscalizadora" por un punto seguido y el texto "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" por el que se indica a continuación:

“Para el cumplimiento de su función podrá:

1. Llevar a cabo inspecciones, incluyendo las realizadas por vía remota.

2. Realizar o establecer auditorías de seguridad periódicas o específicas, por medio de sus empleados. Tras la evaluación de la información o del resultado de cualquier auditoría de seguridad la Agencia podrá dictar instrucciones particulares a la entidad auditada para subsanar las deficiencias detectadas.

3. Realizar análisis de seguridad basados en criterios de evaluación de riesgos objetivos, no discriminatorios, justos y transparentes, con la cooperación de la entidad en cuestión cuando fuere necesario.

4. Solicitar pruebas de la implementación de los planes de continuidad operacional y ciberseguridad, referidos en la letra c) del artículo 6°.

5. 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, incluyendo especialmente el conocimiento de la información necesaria para prevenir, identificar, eliminar o contrarrestar un incidente de ciberseguridad.

No estarán obligadas a concurrir a declarar las personas indicadas en el artículo 361 del Código de Procedimiento Civil, a las cuales la Agencia, para los fines expresados en el párrafo precedente, deberá pedir declaración por escrito.

6. Adoptar o solicitar la adopción de las medidas tendientes a corregir las deficiencias que observare, en general, en el ejercicio de sus atribuciones de fiscalización.

7. Requerir a las entidades fiscalizadas que proporcionen al público, por las vías que señale, información veraz, suficiente y oportuna sobre determinados aspectos del incumplimiento de la presente ley de una manera específica.”.”

Al existir acuerdo por la mesa técnica de aprobar la letra n) complementada a la indicación N°64, se puso en votación únicamente lo referido a esa letra.

Puesta en votación la letra n) de la indicación del Ejecutivo formulada en fecha 11 de octubre, complementada con la indicación N°64, se aprueban por unanimidad. Votan a favor las y los diputados señores Jorge Alessandri, José Miguel Castro, Lorena Fries, Andrés Longton (presidente) y Alejandra Placencia. Sin votos en contra ni abstenciones. **(5-0-0).**

Por aprobarse la letra n) de la indicación del Ejecutivo formulada en fecha 11 de octubre, complementada a la indicación N°64, reglamentariamente se rechaza la letra n) del artículo 9 aprobado por el Senado y las indicaciones N°s 14, 39, 65, 66 y 67.

Por último, se continuó con la votación de las letras ñ) a la z) del artículo 9 que ha pasado a ser 11.

A las letras ñ) a la z) del artículo 9 que ha pasado a ser 11, el Ejecutivo, formuló la siguiente indicación N°15:

“Para intercalar, en el literal r), entre la expresión “para estos efectos” y la coma que le sigue, la frase “las instituciones que no siendo operadores de servicios esenciales estarán obligadas a reportar incidentes de conformidad con lo dispuesto en el artículo 7, así como”.”

A las letras ñ) a la z) del artículo 9 que ha pasado a ser 11**, el diputado señor Andrés Jouannet, formuló las siguientes indicaciones N°s 37 y 38:**

37. “Incorpórese en el literal ñ) del inciso primero del artículo 9° propuesto, luego de “instituciones públicas y privadas”, la siguiente expresión “calificadas como operadores de importancia vital”.”.

38. “Incorpórese los siguientes literales antepenúltimo y penúltimo al inciso primero del artículo 9° propuesto, del siguiente tenor:

“x) Formular las denuncias que correspondieren al Ministerio Público por los hechos de que tomare conocimiento en el ejercicio de sus atribuciones y que pudieren revestir caracteres de delito, sin perjuicio de los deberes generales que sobre la materia determine la ley.

y) Evacuar los informes que le requieran los fiscales del Ministerio Público que estén dirigiendo investigaciones criminales, siempre que correspondan a materias de su competencia y se refieran a información que esté disponible en sus archivos”.”.

A las letras ñ) a la z) del artículo 9 que ha pasado a ser 11**, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon las siguientes indicaciones N°s 68, 69 y 70:**

68. “Intercálase en el literal ñ) del artículo 9°, entre las palabras “privadas” y “respecto”, la frase “calificadas como operadores de importancia vital”.

69. “Intercálase en el literal p) del artículo 9°, entre la palabra “funciones” y el punto aparte, lo siguiente: “dentro del ámbito de sus competencias.

70. “Suprímase el literal t) del artículo 9°.”

A la letra ñ) a la z) del artículo 9 que ha pasado a ser 11, **el Ejecutivo formuló con fecha 11 de octubre, la siguiente propuesta sustituta:**

“ñ) 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.

Para el cumplimiento de su función fiscalizadora, la Agencia podrá realizar inspecciones; instruir de manera particular auditorías por sí o mediante terceros autorizados y análisis de seguridad basados en criterios de evaluación de riesgos objetivos, los cuales deberán ser no discriminatorios, equitativos y transparentes. La entidad fiscalizada deberá cooperar en todo momento con los funcionarios de la Agencia o con los terceros autorizados por ella, según corresponda.

Asimismo, la Agencia podrá requerir el acceso a sistemas informáticos, datos, documentos y demás información que fuere necesaria para el desempeño de sus funciones de supervisión y fiscalización; instruir de manera particular a los sujetos obligados que realicen pruebas que demuestren la implementación de los planes de continuidad operacional y ciberseguridad, referidos en la letra c) del artículo 8 °. Adicionalmente, podrá citar a declarar, respecto de hechos cuyo conocimiento estime necesario para el cumplimiento de sus funciones, a los socios, directores, administradores, representantes, empleados, y cualquier persona que, a cualquier título, preste o haya prestado servicios para las personas o entidades fiscalizadas, así como a toda persona que hubiere ejecutado o celebrado con ellas actos o convenciones de cualquier naturaleza. No obstante, no estarán obligadas a concurrir a declarar las personas indicadas en el artículo 361 del Código de Procedimiento Civil, a las cuales la Agencia, para los fines expresados en el párrafo precedente, deberá pedir declaración por escrito.

Para el ejercicio de esta atribución podrá establecer la forma, plazos y procedimientos para que las entidades fiscalizadas cumplan la obligación de presentar los antecedentes e informaciones referidos en los párrafos precedentes.

o) Instruir el inicio de procedimientos sancionatorios y sancionar las infracciones e incumplimientos en que incurran las instituciones obligadas por la presente ley respecto de sus disposiciones, reglamentos e instrucciones generales y particulares que emita la Agencia. Para tales efectos, y de manera fundada, podrá citar a declarar, en los términos señalados en el literal n) de este artículo, 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. La declaración podrá tomarse presencialmente o por otros medios que aseguren su integridad y fidelidad.

p) 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.

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

r) Informar al CSIRT de la Defensa Nacional y a los CSIRT de los organismos de la Administración del Estado 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.

s) 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.

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

u) 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.

v) 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.

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

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

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

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

Puesta en votación desde la letra ñ) a la z) de la indicación del Ejecutivo formulada en fecha 11 de octubre, se aprueban por unanimidad. Votan a favor las y los diputados señores Jorge Alessandri, José Miguel Castro, Lorena Fries, Andrés Longton (presidente) y Alejandra Placencia. Sin votos en contra ni abstenciones. **(5-0-0).**

Por aprobarse desde la letra ñ) a la z) de la indicación del Ejecutivo formulada en fecha 25 de octubre, reglamentariamente se rechaza desde la letra ñ) a la z) del artículo 9 aprobado por el Senado y las indicaciones N°s 15, 37, 38, 68, 69 y 70.

***

Se da lectura a **una indicación del Ejecutivo que agrega el siguiente artículo 13, nuevo, readecuándose el orden correlativo de los artículos siguientes**:

“Artículo 13. Existirá un Subdirector o Subdirectora Nacional de la Agencia, quien dependerá del Director o Directora Nacional y lo subrogará, en caso de ausencia o impedimento, y además ejercerá las funciones de los literales ñ) y o) del artículo 11. Para ello, contará con la atribución de instruir la apertura de procedimientos administrativos sancionadores, designar a los funcionarios a cargo, determinar las sanciones e imponerlas.

El Subdirector o Subdirectora Nacional de la Agencia, estará afecto al Sistema de Alta Dirección Pública, establecido en la ley N°19.882, como cargo de segundo nivel jerárquico.”.

El **presidente (A) diputado señor Jorge Alessandri**, expresó su conformidad con lo propuesto por cuanto es necesario a lo menos dos autoridades a cargo, por ejemplo, en caso de conflicto de interés decide uno y el otro no, tener la posibilidad de delegar a un segundo responsable.

Puesta en votación la **indicación del Ejecutivo que agrega un nuevo artículo 13, se aprueba por unanimidad.** Votan a favor las y los diputados señores Jorge Alessandri (presidente), José Miguel Castro, Lorena Fries, Andrés Jouannet, Alejandra Placencia y Hugo Rey en reemplazo de Diego Schalper. Sin votos en contra ni abstenciones. **(6-0-0).**

La **asesora legislativa del Ministerio del Interior, abogada señora Michelle Bordachar,** solicitó a la Comisión, con la aprobación de este nuevo artículo 13, reabrir la discusión y votación del artículo 11 que ha pasado a ser 13, para eliminar el literal g) porque esa facultad ahora estaría entregada al Subdirector.

Puesta en votación **la reapertura del debate de la letra g) del artículo 11 que ha pasado a ser 13, para eliminarlo, por un tema de armonización por aprobarse la incorporación de un nuevo artículo 13, se aprueba por unanimidad**. Votan a favor las y los diputados señores Jorge Alessandri (presidente), José Miguel Castro, Lorena Fries, Andrés Jouannet, Alejandra Placencia y Hugo Rey en reemplazo de Diego Schalper. Sin votos en contra ni abstenciones. **(6-0-0).**

***

Se da lectura **al artículo 31 que ha pasado a ser 33:**

“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.”

Al artículo 31 que ha pasado a ser 33**, los diputados señores Cristián Araya, José Miguel Castro y Andrés Jouannet, formularon la siguiente indicación sustitutiva:**

“Artículo 31. Deber de reserva de la Agencia. La Agencia deberá mantener y cautelar la reserva de la información que llegare a conocer en el desempeño de su labor cuando ella

tenga tal calidad en virtud de una norma legal o porque, habiendo sido requerido por ella, le sea entregada bajo tal calidad por el requerido. Asimismo, deberá procurar 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."

Al artículo 31 que ha pasado a ser 33, **los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación sustitutiva:**

"Artículo 33. Deber de reserva de la Agencia. La Agencia deberá mantener y cautelar la reserva de la información que llegue a conocer en el desempeño de sus funciones cuando ella tenga tal calidad en virtud de una norma legal o porque, habiendo sido requerida por ella, le sea entregada bajo tal calidad. Asimismo, deberá procurar 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.

Sin perjuicio de lo anterior, no se incumple el deber de reserva en aquellos casos en que la Agencia o el CSIRT Nacional, en cumplimiento de sus funciones, deba difundir antecedentes que se encontraren sujetos a reserva, siempre que ello permita gestionar, prevenir o contener un incidente de ciberseguridad."

La **asesora legislativa del Ministerio del Interior, abogada señora Michelle Bordachar,** señaló que esta redacción viene a recoger lo solicitado en su oportunidad en relación con modificar la expresión "la reserva de los secretos o información comercial sensible".

Puesta en votación **la indicación sustitutiva de los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper formulada al artículo 31 que ha pasado a ser 33, se aprueba por unanimidad**. Votan a favor las y los diputados señores Jorge Alessandri (presidente), José Miguel Castro, Lorena Fries, Andrés Jouannet, Alejandra Placencia y Hugo Rey en reemplazo de Diego Schalper. Sin votos en contra ni abstenciones. **(6-0-0).**

Por aprobarse la indicación sustitutiva de los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper formulada al artículo 31 que ha pasado a ser 33**, reglamentariamente se rechazan, el artículo 31 aprobado por el Senado y la indicación sustitutiva formulada por los diputados señores Cristián Araya, José Miguel Castro y Andrés Jouannet.**

***

Se da lectura **al artículo 33 que ha pasado a ser 35:**

"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 contado 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.”

Al artículo 33, **el diputado señor Andrés Jouannet, formuló las siguientes indicaciones N°s 41, 42, 43, 44, 45, 46, 47, 48 y 49:**

41. “Reemplácese el inciso primero del artículo 33° propuesto por el siguiente:

“Artículo 33. De las infracciones. Las sanciones a las infracciones de la presente ley cometidas por instituciones públicas y privadas calificadas como operadores de importancia vital serán las siguientes:”

42. “Reemplácese el literal a) del inciso primero del artículo 33° por el siguiente:

“a) Las infracciones leves serán sancionadas con amonestación escrita o multa de hasta 5.000 unidades tributarias mensuales”

43. “Reemplácese el literal b) del inciso primero del artículo 33° por el siguiente:

“b) Las infracciones graves serán sancionadas con multa de hasta 10.000 unidades tributarias mensuales”.

44. “Reemplácese el literal c) del inciso primero del artículo 33° por el siguiente:

“c) Las infracciones gravísimas serán sancionadas con multa de hasta 20.000 unidades tributarias mensuales”.

45. “Reemplácese el inciso segundo del artículo 33° por el siguiente:

“Se consideran infracciones leves las siguientes:

a) Incumplir las instrucciones generales o particulares impartidas por la Agencia en los casos que no esté sancionado como infracción grave o gravísima.

b) Incumplir total o parcialmente con los protocolos y estándares diferenciados establecidos por la Agencia en virtud del artículo 5°.

c) No haber designado un delegado de ciberseguridad en conformidad con el literal i) del artículo 6°.

d) No contar con programas de capacitación, formación y educación de sus trabajadores, en conformidad con el literal h) del artículo 6°.

e) No contar con las certificaciones requeridas por la ley o el Reglamento, de conformidad con los literales c) y f) del artículo 6°.

f) Cometer cualquier otra infracción a las obligaciones y principios establecidos en esta ley, que no sea calificada como una infracción grave o gravísima”.

46. “Reemplácese el inciso tercero del artículo 33° por el siguiente:

“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°, en los casos que no esté sancionado como infracción gravísima.

c) Incumplir con el deber general de no realizar pagos de cualquier tipo por rescate ante ataques de secuestro digital o ransomware, establecido en el artículo 5°.

d) Incumplir injustificadamente con el deber de informar a la comunidad sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente sus redes y sistemas informáticos, de conformidad con el literal g) del artículo 6°.

e) No haber adoptado de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad, en conformidad con lo establecido en el literal e) del artículo 6°.

f) No mantener un registro de las acciones ejecutadas que compongan el sistema de seguridad de la información, de conformidad al literal b) del artículo 6°.

g) Incumplir con el deber de elaborar e implementar planes de continuidad operacional y ciberseguridad, según lo señalado por el literal c) del artículo 6°.

h) La reiteración de una misma infracción calificada como leve de acuerdo con este artículo”.

47. “Reemplácese el inciso tercero del artículo 33° por el siguiente:

“Las siguientes infracciones se consideran gravísimas:

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 injustificada o maliciosamente con el deber de reportar establecido en el artículo 7°.

d) Incumplir injustificadamente con los deberes establecidos en los literales a) y d) del artículo 6°.

e) La reiteración de infracciones calificadas como graves de acuerdo con este artículo”.

48. “Intercálese en el inciso cuarto (quinto?) del artículo 33°, luego de “la gravedad de los efectos de los ataques” la expresión “incluidas sus repercusiones sociales o económicas, la gravedad de la infracción, el grado de exposición del infractor a los riesgos, el tamaño del infractor, el beneficio económico obtenido con motivo de la infracción en caso

que lo hubiese, la intencionalidad en la comisión de la infracción y el grado de participación en el hecho, acción u omisión constitutiva de la misma, las sanciones aplicadas con anterioridad por la Agencia en las mismas circunstancias, el porcentaje de usuarios afectados por la infracción".

49. "Incorpórese un nuevo inciso final al artículo 33° del siguiente tenor:

"Se consideran circunstancias atenuantes:
a) Haber adoptado códigos de conducta certificados por un centro de certificación acreditado.
b) Haber adoptado directrices autorregulatorias certificadas por un centro de certificación acreditado.
c) Haber designado a un delegado de ciberseguridad;
d) Que la entidad infractora haya tomado medidas para mitigar o prevenir el daño o las pérdidas causadas;
e) Que la entidad infractora haya colaborado con la Agencia Nacional de Ciberseguridad".

Al artículo 33, **los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon las siguientes indicaciones N°s 74, 75, 77, 78, 79 y 80:**

74. "Intercálase en el inciso primero del artículo 33, entre las palabras "privadas" y "serán" lo siguiente "señaladas en los artículos 5 y 6".

75. "Sustitúyanse los literales a), b) y c) del inciso primero del artículo 33, por los siguientes:
a) Las infracciones leves serán sancionadas con amonestación escrita o multa de hasta 5.000 unidades tributarias mensuales.
b) Las infracciones graves serán sancionadas con multa de hasta 10.000 unidades tributarias mensuales.
c) Las infracciones gravísimas serán sancionadas con multa de hasta 20.000 unidades tributarias mensuales."

77. "Sustitúyese el inciso segundo del artículo 33, por el siguiente:

"Se considerarán infracciones leves las siguientes:
a) Incumplir total o parcialmente los deberes generales de ciberseguridad establecido en el artículo 5 en los casos que no esté sancionado como infracción grave o gravísima;
b) Incumplir las instrucciones generales o particulares impartidas por la agencia en los casos que no esté sancionado como infracción grave o gravísima;
c) No haber actualizado los planes de continuidad operacional y ciberseguridad, previa instrucción particular en general de la agencia;
d) No haber designado un delegado de ciberseguridad;
e) No contar con programas de capacitación, formación y educación de sus trabajadores;
f) Cometer cualquier otra infracción a las obligaciones y principios establecidos en esta ley que no sea calificada como una infracción grave o gravísima."

78. "Sustitúyese el inciso tercero del artículo 33, por el siguiente:

"Se considerarán infracciones graves la siguientes:
a) Entregar fuera de plazo a 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, en los casos que no esté sancionado como infracción gravísima;
c) Incumplir con el deber de garantizar un nivel de seguridad a los sistemas de redes y de información adecuado en relación con los riesgos planteados, establecido en el artículo 6;

d) Incumplir injustificadamente con el deber de informar sin demora a los destinatarios de sus servicios de las medidas o soluciones que pueden aplicar para reducir el riesgo resultante de un incidente de efecto significativo, establecido en el literal g) del artículo 6;

e) No haber adoptado de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad coma según lo establecido en el artículo 6;

f) Negar injustificadamente la ejecución o implementación de alguna de las facultades de la agencia establecidas en el literal n) del artículo noveno.

g) La reincidencia en una infracción leve dentro del periodo de un año.”

79. “Sustitúyese el inciso cuarto del artículo 33, por el siguiente:

“Se considerarán infracciones gravísimas las siguientes:

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 injustificada o maliciosamente el deber de reportar establecido en el artículo 7;

d) Incumplir con las obligaciones prescritas en los literales a), c) y d) del artículo 6;

e) La reincidencia en una infracción grave dentro del periodo de dos años.”

80. “Para sustituir el inciso quinto del artículo 33, por el siguiente:

“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, el grado de exposición del infractor a los riesgos, la gravedad de los efectos de los ataques incluidas sus repercusiones sociales o económicas, la reiteración en la infracción dentro del plazo de 3 años contado desde el momento en que se produjo el incidente, el tamaño y la capacidad económica del infractor.”

Al artículo 33, **el diputado señor Jorge Alessandri, formuló las siguientes indicaciones N°s 79, 81 y 82:**

76. Para sustituir el inciso primero del literal c) del artículo 33, por el siguiente:

“c) Las infracciones gravísimas serán sancionadas con multa de 5.001 a 10.000 unidades tributarias mensuales. En caso de que el infractor sea un operador de importancia vital, la multa podrá ser de hasta 20.000 unidades tributarias mensuales.”.

81. Para suprimir, en el inciso séptimo del artículo 33, la frase: “y fundamentos jurídicos”.

82. En el artículo 33 inciso octavo del proyecto de ley, para sustituir la frase “a los tres años de cometidas” por la siguiente: “en el plazo de tres años desde que hubieren sido cometidas”.

Al artículo 33, que ha pasado a ser 35, **el diputado señor José Miguel Castro, formuló la siguiente indicación:**

“Artículo 35. Competencia de la autoridad sectorial. La autoridad sectorial será competente para fiscalizar, conocer y juzgar las infracciones, así como ejecutar las sanciones a la normativa sobre ciberseguridad que hubiere dictado y cuyos efectos sean al menos equivalentes al de la normativa dictada por la Agencia, conforme lo dispuesto en el artículo 24. Para este efecto, las sanciones y procedimientos sancionatorios serán los que

correspondan a la autoridad sectorial de conformidad a su normativa. Fuera de dichos casos, corresponderá a la Agencia fiscalizar, conocer y juzgar las infracciones, así como ejecutar las sanciones a la presente ley, sin perjuicio de la facultad de los organismos de la Administración del Estado de poner en conocimiento del organismo competente las infracciones a la norma de que tomaren conocimiento."

El **diputado señor José Miguel Castro**, como autor de la indicación recién leída, la modificó por sugerencia de los expertos, reemplazando la expresión "juzgar" por "sancionar", de tal manera evitar confusiones de funciones pertenecientes a otro órgano del Estado.

Puesta en **votación la indicación sustitutiva del diputado señor José Miguel Castro, con la modificación de la expresión "juzgar" por "sancionar", formulada al artículo 33 que ha pasado a ser 35, se aprueba por unanimidad.** Votan a favor las y los diputados señores Jorge Alessandri (presidente), José Miguel Castro, Lorena Fries, Andrés Jouannet, Alejandra Placencia y Hugo Rey en reemplazo de Diego Schalper. Sin votos en contra ni abstenciones. **(6-0-0).**

Por aprobarse la indicación sustitutiva del diputado señor José Miguel Castro, formulada al artículo 33 que ha pasado a ser 35, **reglamentariamente se rechazan, el artículo 33 aprobado por el Senado y todas las indicaciones formuladas al referido texto.**

***

Se da lectura **al artículo 34 que ha pasado a ser 36:**

"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.”

Al artículo 34, que ha pasado a ser 36, **los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°83:**

“Intercálase en el literal b del inciso primero del artículo 34, entre la expresión “a petición de parte” y la coma que le sigue, la palabra “afectada”.

Al artículo 34, que ha pasado a ser 36**, el diputado señor José Miguel Castro, formuló la siguiente indicación sustitutiva:**

“Artículo 36. Infracciones. Las infracciones a las obligaciones que esta ley prescribe a los sujetos obligados por ella se califican en leves, graves y gravísimas.

Se considerarán infracciones leves las siguientes:

1. Entregar fuera de plazo la información que se le requiera cuando ella no fuere necesaria para la gestión de un incidente de ciberseguridad;

2. Incumplir las instrucciones generales o particulares impartidas por la Agencia en los casos que no esté sancionado como infracción grave o gravísima; y

3. Cualquier infracción a las obligaciones que esta ley establece y que no tenga señalada una sanción especial.

Se considerarán infracciones graves las siguientes:

1. No haber implementado los protocolos y estándares establecidos por la Agencia para prevenir, reportar y resolver incidentes de ciberseguridad;
2. No haber implementado los estándares particulares de ciberseguridad;
3. Entregar fuera de plazo la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de ciberseguridad;
4. Entregar a la Agencia de información manifiestamente falsa o errónea.
5. Incumplir la obligación de reportar establecida en el artículo 9;
6. Negarse injustificadamente a cumplir una instrucción de la Agencia o entorpecer deliberadamente el ejercicio de las atribuciones de la Agencia durante la gestión de un incidente de ciberseguridad, siempre que la atribución no cuente con una sanción especial; y
7. La reincidencia en una misma infracción leve dentro de un año.

Se considerarán infracciones gravísimas las siguientes:

1. Entregar a la Agencia información manifiestamente falsa o errónea, cuando ella sea necesaria para la gestión de un incidente de ciberseguridad;
2. Incumplir las instrucciones generales o particulares impartidas por la Agencia durante la gestión de un incidente de impacto significativo;
3. No entregar la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de impacto significativo; y
4. La reincidencia en una infracción grave dentro de un año.

Puesta en votación **la indicación sustitutiva del diputado señor José Miguel Castro, formulada al artículo 34 que ha pasado a ser 36, se aprueba por unanimidad.** Votan a favor las y los diputados señores Jorge Alessandri (presidente), Cristián Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Alejandra Placencia y Hugo Rey en reemplazo de Diego Schalper. Sin votos en contra ni abstenciones. **(7-0-0).**

Por aprobarse la indicación sustitutiva del diputado señor José Miguel Castro, formulada al artículo 34 que ha pasado a ser 36**, reglamentariamente se rechazan, el artículo 34 aprobado por el Senado y todas las indicaciones formuladas al referido texto.**

****

El **diputado señor José Miguel Castro, formuló la siguiente indicación que incorpora un nuevo artículo 37:**

“Artículo 37. De las infracciones de los Operadores de Importancia Vital. Sin perjuicio de lo prescrito en el artículo precedente, los Operadores de Importancia Vital podrán ser sancionados por infringir las disposiciones del artículo 8º, las que se califican en leves, graves y gravísimas.

Se considerarán infracciones leves las siguientes:

1. No mantener el registro de las acciones de seguridad que señala la letra b);
2. No comunicar al CSIRT Nacional la realización continua de operaciones de revisión, ejercicios y demás acciones que señala el literal d);
3. No contar con programas de capacitación, formación y educación continua para los trabajadores, según dispone el literal g);
4. No designar un delegado de ciberseguridad, según dispone la letra i);
5. No dar cumplimiento a la instrucción particular de la Agencia en orden a certificar los planes de continuidad operacional del párrafo segundo de la letra c); y
6. No contar con las certificaciones que exija la ley, de acuerdo al literal f).

Se considerarán infracciones graves las siguientes:

1. No haber implementado el sistema de gestión de seguridad de la información continuo al que se refiere el literal a);

2. No haber elaborado o implementado los planes de continuidad operacional y ciberseguridad a los que se refiere la letra c);

3. No informar a los potenciales afectados sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos, en los casos que señala la letra g);

4. No adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o un ciberataque, según señala la letra e); y

5. La reincidencia en una misma infracción leve dentro del periodo de un año.

Se considerarán infracciones gravísimas las siguientes:

1. No adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o un ciberataque, según señala la letra e), cuando este posea un impacto significativo; y

2. La reincidencia en una misma infracción grave dentro del periodo de un año."

Puesta en votación la indicación del diputado señor José Miguel Castro, que incorpora un nuevo artículo 37, se aprueba por unanimidad. Votan a favor las y los diputados señores Jorge Alessandri (presidente), Cristián Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Alejandra Placencia y Hugo Rey en reemplazo de Diego Schalper. Sin votos en contra ni abstenciones**. (7-0-0).**

****

El **diputado señor José Miguel Castro, formuló la siguiente indicación que incorpora un nuevo artículo 38:**

"Artículo 38. De las sanciones. La infracción a los preceptos de esta ley conlleva la imposición de una multa a beneficio fiscal, de acuerdo a la siguiente escala:

1. Las infracciones leves serán sancionadas con multa de hasta 5.000 unidades tributarias mensuales; o con hasta 10.000 unidades tributarias mensuales si se tratare de un operador de importancia vital;

2. Las infracciones graves serán sancionadas con multa de hasta 10.000 unidades tributarias mensuales; o con hasta 20.000 unidades tributarias mensuales si se tratare de un operador de importancia vital; y

3. Las infracciones gravísimas serán sancionadas con multa de hasta 20.000 unidades tributarias mensuales; o con hasta 40.000 unidades tributarias mensuales si se tratare de un operador de importancia vital.

La multa será fijada teniendo en consideración el grado en que el infractor adoptó las medidas necesarias para resguardar la seguridad informática de las operaciones, la probabilidad de ocurrencia del incidente, el grado de exposición del infractor a los riesgos, la gravedad de los efectos de los ataques incluidas sus repercusiones sociales o económicas, la reiteración en la infracción dentro del plazo de 3 años contado desde el momento en que se produjo el incidente, el tamaño y la capacidad económica del infractor."

Las y los **diputados señores Jorge Alessandri, Cristián Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Alejandra Placencia y Hugo Rey**, por sugerencia del abogado experto señor Claudio Magliona, complementaron la indicación antes leída, agregando al texto los tres últimos incisos del artículo 33 aprobado por el Senado, para evitar que, por unos mismos hechos y fundamentos jurídicos, se apliquen dos o más sanciones administrativas, quedando el artículo 38 nuevo de la siguiente manera:

“Artículo 38. De las sanciones. La infracción a los preceptos de esta ley conlleva la imposición de una multa a beneficio fiscal, de acuerdo a la siguiente escala:

1. Las infracciones leves serán sancionadas con multa de hasta 5.000 unidades tributarias mensuales; o con hasta 10.000 unidades tributarias mensuales si se tratare de un operador de importancia vital;

2. Las infracciones graves serán sancionadas con multa de hasta 10.000 unidades tributarias mensuales; o con hasta 20.000 unidades tributarias mensuales si se tratare de un operador de importancia vital; y

3. Las infracciones gravísimas serán sancionadas con multa de hasta 20.000 unidades tributarias mensuales; o con hasta 40.000 unidades tributarias mensuales si se tratare de un operador de importancia vital.

La multa será fijada teniendo en consideración el grado en que el infractor adoptó las medidas necesarias para resguardar la seguridad informática de las operaciones, la probabilidad de ocurrencia del incidente, el grado de exposición del infractor a los riesgos, la gravedad de los efectos de los ataques incluidas sus repercusiones sociales o económicas, la reiteración en la infracción dentro del plazo de 3 años contado desde el momento en que se produjo el incidente, el tamaño 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.”

Puesta en votación **la indicación del diputado señor José Miguel Castro, que incorpora un nuevo artículo 38, en complemento con los tres últimos incisos del artículo 33 aprobado por el Senado, se aprueba por la mayoría de los votos.** Votan a favor las y los diputados señores Jorge Alessandri (presidente), Cristián Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Alejandra Placencia y Hugo Rey en reemplazo de Diego Schalper. Sin votos en contra. Con la abstención del diputado señor Cristián Araya. **(6-0-1).**

***

Se da lectura al artículo 36 aprobado por el Senado:

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 contado desde que la respectiva resolución quede firme.”.

Al artículo 36, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°87:

“Introdúcense las siguientes modificaciones al artículo 36:

a) Introdúcense las siguientes modificaciones al inciso primero:
i. Sustitúyese la frase “público” por “de la Administración del Estado”;
ii. Sustitúyese la frase “los principios y obligaciones establecidos en los Títulos I y II de esta ley, respectivamente” por “lo establecido en esta ley”;
b) En el inciso segundo, sustitúyese la palabra “someterse” por “adoptar”;
c) Introdúcense las siguientes modificaciones al inciso tercero:
i. Sustitúyse la frase “los principios y” por el artículo “las”;
ii. Reemplázase la frase “veinte por ciento a cincuenta” por “diez por ciento a treinta”.
d) En el inciso cuarto, intercálase entre la expresión “impuesta” y la conjunción “y” una coma, seguida de lo siguiente: “la cual no podrá superar el cincuenta por ciento”;
e) Sustitúyase el inciso quinto por el siguiente:
“Las sanciones serán aplicadas según las reglas generales de la responsabilidad administrativa y procederá el reclamo de ilegalidad establecido en el artículo 35.”
f) Suprímase el inciso sexto.”

La **asesora legislativa del Ministerio del Interior, abogada señora Michelle Bordachar,** señaló que la mesa de trabajo técnica integrada por el Ejecutivo y abogados asesores de las y los diputados de la comisión, llegó a un acuerdo de aprobar sólo los dos primeros incisos del artículo 36 del texto del Senado, complementado solo a las letras a) y b) de la indicación N°87.

Puesta en votación **los incisos 1 y 2 del artículo 36 del texto aprobado por el Senado, complementado con las letras a) y b) de la indicación N°87, se aprueba por unanimidad.** Votan a favor las y los diputados señores Jorge Alessandri (presidente), Cristián Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Alejandra Placencia y Hugo Rey en reemplazo de Diego Schalper. Sin votos en contra ni abstenciones. **(7-0-0).**

Por lo anterior, reglamentariamente se rechaza, el resto del artículo 36 aprobado por el Senado y todas las otras letras de la indicación N°87.

Se da lectura al artículo 37 aprobado por el Senado:

“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.”

El **presidente diputado señor Jorge Alessandri,** aclaró que, en consecuencia, a lo votado en el artículo anterior, y según los acuerdos arribados este debe ser rechazado.

Puesto en votación **el artículo 37 del texto aprobado por el Senado, se rechaza por unanimidad.** Sin votos a favor. Votan en contra las y los diputados señores Jorge Alessandri (presidente), Cristián Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Alejandra Placencia y Hugo Rey en reemplazo de Diego Schalper. Sin abstenciones. **(0-7-0).**

****

Se da lectura al artículo 38 aprobado por el Senado:

“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.”

La **asesora legislativa del Ministerio del Interior, abogada señora Michelle Bordachar,** manifestó que este artículo establece una agravante especial para el caso de que un ciberdelincuente a un operador de importancia vital y a consecuencia de ese ataque se vean paralizadas sus operaciones. Sin embargo, por un tema de técnica legislativa, esta agravante no se debería establecer en esta ley, sino que en la que fija este tipo delitos como es la ley de delitos informáticos, por ello es que se sugiere rechazar.

Puesto en votación **el artículo 38 del texto aprobado por el Senado, se rechaza por unanimidad.** Sin votos a favor. Votan en contra las y los diputados señores Jorge Alessandri (presidente), Cristián Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Alejandra Placencia y Hugo Rey en reemplazo de Diego Schalper. Sin abstenciones. **(0-7-0).**

****

Se da lectura al artículo 44 aprobado por el Senado:

“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.”

Al artículo 44 aprobado por el Senado, **el Ejecutivo formuló las siguientes indicaciones N°s 19 y 20:**

19. “Para intercalar, a continuación del Título VIII, el siguiente título IX, nuevo, readecuándose el orden correlativo de los títulos y artículos siguientes:

“Título IX

De los servicios esenciales.

Artículo 44. Servicios esenciales. Para todos los efectos de la presente ley, se considerarán como servicios esenciales para el mantenimiento de actividades sociales o económicas cruciales, que dependen de las redes y sistemas informáticos, a los siguientes:

1. Los servicios de telecomunicaciones.

2. Los servicios de infraestructura digital, incluyendo los servicios de intercambio de tráfico de internet; servicios de computación en la nube; servicios de alojamiento o procesamiento de datos; servicios de redes de distribución de contenidos; servicios de registro de nombres del dominio .CL; servicios de certificación acreditados a que se refiere la Ley N°19.799.

3. Los servicios de ciberseguridad;

4. Los servicios de generación, transmisión y distribución eléctrica.

5. Los servicios de producción, transporte, almacenamiento y distribución de combustibles.

6. Los servicios sanitarios y de suministro de agua potable.

7. Los servicios comerciales de transportes aéreos, ferroviarios y marítimos.

8. Los servicios portuarios.

9. Los servicios aeroportuarios.

10. Los servicios bancarios y financieros.

11. Los servicios de administración de fondos previsionales, de fondos de cesantía y los servicios de salud previsional.

12. Los servicios de prestaciones de salud.

La Agencia identificará, mediante resolución exenta dictada conforme el procedimiento dispuesto en el artículo 4° de esta ley, las infraestructuras, procesos o funciones específicas que serán calificadas como esenciales, y que quedarán sujetas a las obligaciones establecidas en el artículo 6° de esta ley.

Asimismo, conforme al mismo procedimiento, la Agencia podrá calificar como esenciales otros servicios distintos a los señalados precedentemente, para lo cual deberá considerar, entre otros factores, la entidad del impacto cuya afectación o interrupción podría tener en la defensa nacional o en el mantenimiento de actividades sociales y económicas fundamentales; la dependencia del servicio de las redes y sistemas informáticos; la interconexión, interoperabilidad o interdependencia que tenga con otros servicios esenciales.”.

20. “Para agregar, en el inciso tercero del artículo 44, que ha pasado a ser 45, a continuación de la expresión “conformación o participación” la expresión “, si así se acordare,”.

Al artículo 44 aprobado por el Senado, **los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°88:**

“Agrégase en el inciso primero del artículo 44, entre las expresiones “Televisión” y “adoptar”, la palabra “podrán”.

Al artículo 44 aprobado por el Senado, **los diputados señores Cristián Araya, José Miguel Andrés Jouannet y Andrés Longton, formularon la siguiente indicación sustitutiva:**

“Artículo 44. Regímenes especiales. El Senado y la Cámara de Diputados, el Poder Judicial, la Contraloría General de la República, el Banco Central, el Ministerio Público, el Servicio Electoral y el Consejo Nacional de Televisión deberán adoptar las medidas de seguridad de sus redes y sistemas informáticos que sean pertinentes. Para estos efectos, la Corte Suprema, el respectivo jefe de servicio o los órganos colegiados que ejerzan dicha función, podrán dictar la normativa que sea conveniente a tales efectos, pudiendo considerar en su formulación las recomendaciones que efectúe la Agencia.

Las instituciones y órganos señalados en este artículo no estarán sujetos en modo alguno a la regulación, fiscalización o supervigilancia de la Agencia; sin perjuicio de que deberán convenir mecanismos de reporte de incidentes de ciberseguridad y de coordinación y cooperación para la respuesta a incidentes de ciberseguridad.

Asimismo, si el órgano autónomo constitucional revistiera el carácter de autoridad sectorial, deberá considerársele para los efectos de los artículos 6, 23 y 24.”

Puesta en votación **la indicación sustitutiva del artículo 44, formulada por los diputados señores Cristián Araya, José miguel castro y Andrés Jouannet, se aprueba por unanimidad.** Votan a favor las y los diputados señores Jorge Alessandri (presidente), Cristián Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet y Alejandra Placencia. Sin votos en contra ni abstenciones. **(6-0-0).**

Por ende, **se rechazan reglamentariamente el artículo 44 del texto aprobado por el Senado y las indicaciones N°s 19 y 20.**

***

Se da lectura al artículo 45 aprobado por el Senado:

"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.".".

Puesto en votación **el artículo 45 aprobado por el Senado, se aprueba por la mayoría de los votos.** Votan a favor las y los diputados señores Jorge Alessandri (presidente), José Miguel Castro, Lorena Fries, Andrés Jouannet, Alejandra Placencia y Hugo Rey en reemplazo de Diego Schalper. Vota en contra el diputado señor Cristián Araya. Sin abstenciones. **(6-1-0).**

****

Se da lectura al artículo 24 del texto aprobado por el Senado:

"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."

Al artículo 24 que ha pasado a ser 27**, el Ejecutivo formuló la siguiente indicación N°16:**

"Para reemplazar los incisos segundo, tercero y cuarto, del artículo 24, por el siguiente inciso segundo, nuevo, readecuando el orden correlativo de los incisos siguientes: "La Agencia podrá homologar certificaciones técnicas internacionales o extranjeras sobre ciberseguridad mediante resolución fundada de su director o directora."."

Al artículo 24 que ha pasado a ser 27, **el diputado señor Andrés Jouannet, formuló las siguientes indicaciones N°39 y 40:**

39. "Incorpórense el siguiente inciso tercero en el artículo 24° propuesto, pasando el actual inciso tercero a ser cuarto y así sucesivamente, del siguiente tenor:

“Asimismo, los centros de certificación acreditados serán los únicos habilitados para homologar otros esquemas de certificación o certificaciones internacionalmente reconocidas, acreditando que cumplen con los estándares y normas de seguridad establecidos por esta ley y su normativa complementaria. Los centros de certificación acreditados deberán certificar automáticamente los esquemas de certificación o certificaciones internacionalmente reconocidas que se encuentren homologadas y adoptadas por los entes que soliciten la certificación”.”

40. Reemplácese en el inciso cuarto del artículo 24°, que ha pasado a ser quinto, la expresión “deberán” por “podrán”.”

Al artículo 24 que ha pasado a ser 27, **los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°73:**

“Suprímase el artículo 24.”

Al inciso primero del artículo 24 que ha pasado a ser 27, **los diputados señores Jorge Alessandri, José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación que lo reemplaza:**

“Los operadores de importancia vital deberán obtener las certificaciones de ciberseguridad que señala esta ley y las que determine la Agencia mediante reglamento. Para estos efectos, sólo los organismos que sean parte del registro de entidades certificadoras autorizadas, a cargo de la Agencia, estarán habilitadas para emitir certificaciones válidas que esta ley exija. Para formar parte de este registro bastará acreditar el cumplimiento de los requisitos que establezca el reglamento, pudiendo mantenerse en tanto cumplan los referidos requisitos.”

Al existir acuerdo por la mesa técnica de aprobar la indicación que reemplaza el inciso primero del artículo 24 del texto aprobado por el Senado, formulada por los diputados señores Jorge Alessandri, José Miguel Castro, Andrés Longton y Diego Schalper, complementada a la indicación N°16 del Ejecutivo, se puso en votación conjunta lo descrito.

Puesta en votación la indicación que reemplaza el inciso primero del artículo 24 del texto aprobado por el Senado, formulada por los diputados señores Jorge Alessandri, José Miguel Castro, Andrés Longton y Diego Schalper, complementada a la indicación N°16 del Ejecutivo, se aprueban por unanimidad. Votan a favor las y los diputados señores Jorge Alessandri, José Miguel Castro, Lorena Fries, Andrés Longton (presidente) y Alejandra Placencia. Sin votos en contra ni abstenciones**. (5-0-0).**

Por aprobarse la indicación que reemplaza el inciso primero del artículo 24 del texto aprobado por el Senado, formulada por los diputados señores Jorge Alessandri, José Miguel Castro, Andrés Longton y Diego Schalper, complementada con la indicación N°16 del Ejecutivo, reglamentariamente se rechaza el artículo 24 del texto aprobado por el Senado y las indicaciones N°s 39, 40 y 73.

***

Los diputados señores Jorge Alessandri, José Miguel Castro y Andrés Longton, formularon una indicación que incorpora los nuevos artículos 39, 40, 41, 42 y 43 siguientes:

“Para incorporar los nuevos artículos 39 y siguientes:

“Artículo 39. Procedimiento administrativo sancionador. El procedimiento administrativo se regirá por lo prescrito por la ley Nº19.880, que establece bases de los procedimientos

administrativos que rigen los actos de los organismos de la Administración del Estado, sin perjuicio de las siguientes disposiciones:

a) Toda sanción deberá fundarse en un procedimiento que se iniciará con la formulación precisa y fundada de los cargos y contendrá la descripción de los hechos en los que se fundamentan y de cómo éstos constan en la investigación, la indicación de por qué se consideran una infracción a la normativa, especificando la o las normas que se estimen infringidas y el presunto responsable de la infracción. Además, se designará al funcionario a cargo de la instrucción del procedimiento. Se fijará un plazo para la formulación de descargos que no podrá ser inferior a quince ni superior a treinta días. Las notificaciones del procedimiento deberán realizarse a la dirección de correo electrónico que haya sido proporcionada a la Agencia, de conformidad al reglamento.

b) En los descargos deberán señalarse todas las circunstancias o antecedentes de hecho y de derecho que eximan o atenúen la presunta responsabilidad de la persona objeto de cargos, así como aquellas que nieguen la efectiva ocurrencia de los hechos, o que demuestren que éstos no constituyen infracción. Todo ello, sin perjuicio de otras presentaciones o antecedentes posteriores que se hagan valer en el curso del procedimiento sancionatorio con el mismo objetivo. Asimismo, deberán solicitarse las diligencias probatorias que correspondieren.

c) Vencido el plazo para formular descargos, se abrirá un término probatorio por un plazo no inferior a diez ni superior a veinte días, según la naturaleza y complejidad del asunto. Dicho plazo podrá prorrogarse por una sola vez y hasta por un máximo de quince días. Se podrá rendir prueba mediante cualquier medio admisible en Derecho, los que se apreciarán de acuerdo a las reglas de la sana crítica.

d) Excepcionalmente, se realizarán las diligencias que, decretadas de oficio o a petición de parte, se estimen estrictamente necesarias para la resolución del asunto. Las diligencias podrán solicitarse dentro de los cinco días siguientes al vencimiento del término probatorio.

e) Una vez transcurrido el plazo mencionado en el literal previo, el procedimiento deberá concluir. El instructor del procedimiento emitirá un informe en el cual deberá incluir un análisis detallado de todas las defensas, alegatos y pruebas presentadas durante el procedimiento sancionatorio a partir del cual se determinará si se ha infringido la normativa vigente y si procede la imposición de la sanción respectiva o la absolución de los cargos. El informe deberá emitirse dentro del plazo de quince días.

f) Una vez recibido el informe del instructor del procedimiento, corresponderá al Subdirector de la Agencia resolver los procesos sancionatorios en el plazo de quince días hábiles, dictando al efecto resolución fundada en la cual absolverá al infractor o aplicará la sanción, en su caso. La resolución del Subdirector deberá incluir el mismo contenido que el informe señalado en el literal precedente.

Artículo 40. De los recursos. En contra de la resolución del Subdirector mediante la cual se concluye el procedimiento administrativo procederán los recursos que establezca la ley Nº19.880. El recurso deberá resolverse dentro del plazo de quince días. La interposición del recurso suspenderá el plazo para reclamar de ilegalidad, siempre que se trate de materias por las cuales procede dicho recurso.

Artículo 41. Forma de pago de las multas. Las multas deberán pagarse dentro de los diez días siguientes contados desde que el acto administrativo que las impone quede firme. Vencido ese plazo, la resolución que establezca la sanción tendrá mérito ejecutivo y se hará exigible por la Tesorería General de la República. Para su cobro se aplicará el inciso segundo del artículo 35 del decreto ley N°1.263, de 1975, orgánico de Administración Financiera del Estado.

El pago de toda multa deberá ser acreditado ante la Agencia, dentro de los diez días siguientes a la fecha en que ésta debió ser pagada.

El retardo en el pago de estas multas devengará los intereses y reajustes establecidos en el artículo 53 del Código Tributario.

Artículo 42. Procedimiento simplificado. Tratándose de la formulación de cargos por infracciones calificadas como leves en conformidad al artículo 39, la Agencia estará facultada para proponer de manera inmediata la sanción a aplicar, la cual quedará firme si el presunto infractor opta por allanarse a los cargos formulados en su contra. En caso contrario, si el presunto infractor decide rechazar la imputación y presentar descargos, se procederá conforme a lo indicado en el artículo 40 de la presente ley.

Artículo 43. Pronto pago. El sancionado que no interponga recurso alguno podrá, dentro de los cinco días hábiles siguientes a que le sea notificada la resolución del Subdirector que le impone la sanción, pagar directamente en la Tesorería General de la República en cuyo caso, el monto de la misma será reducido en un veinticinco por ciento. Una vez ejercido este derecho, se entenderán renunciado todos los recursos.

Lo dicho en este artículo no será aplicable para el caso previsto en el artículo anterior.”.”

El presidente diputado señor Andrés Longton, manifestó la eliminación de la expresión “hábiles” de la letra f) de la propuesta de artículo 39 nuevo, ya que el artículo 30 de la ley N°19.880 sobre bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado, establece que siempre serán días hábiles, por ello es mejor no explicitarlo, ya que puede ocurrir que en otro lugar de la ley no se exprese y se puede entender que en ese caso no sería días hábiles.

La **asesora legislativa del Ministerio del Interior, abogada señora Michelle Bordachar**, indicó que efectivamente es como lo indica el presidente Longton, ya que, en otros artículos de la ley, cuando se quiere que sean días corridos se explicita, sin embargo, cuando no lo son se aplica la regla general, de los días hábiles, por lo que se pone solo la palabra “días”. Por lo anterior, sugirió también, que se elimine la palabra “hábiles”, de la letra f) del nuevo artículo 39 propuesto.

Puesta en votación **la indicación que incorpora los artículos 39, 40, 41, 42 y 43 nuevos, con la corrección de la letra f) de la propuesta del artículo 39, formulada por los diputados señores Jorge Alessandri, José Miguel Castro y Andrés Longton, se aprueban por unanimidad.** Votan a favor las y los diputados señores Jorge Alessandri, José Miguel Castro, Lorena Fries, Andrés Longton (presidente) y Alejandra Placencia. Sin votos en contra ni abstenciones**. (5-0-0).**

***

Se da lectura al artículo 46 del texto aprobado por el Senado:

Artículo 46. Introdúcense las siguientes enmiendas en 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:

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 utilizando 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 sobre 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.”.

Derógase el artículo 16.”.

Al artículo 46, **el diputado señor Andrés Joaunnet, formuló la siguiente indicación N°50:**

“Suprímase el artículo 46 que incorpora modificaciones a la ley 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.”

Al artículo 46, **los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°89:**

“Suprímese el artículo 46.”

Al artículo 46, **el diputado señor Jorge Alessandri y la diputada señora Gloria Naveillán, formularon la siguiente indicación N°90:**

“Para eliminar el artículo 46.”

Al numeral 1 del artículo 46**, las y los diputados señores Jorge Alessandri, José Miguel Castro, Lorena Fries, Andrés Longton y Alejandra Placencia, formularon la siguiente indicación que lo reemplaza:**

“Para reemplazar el numeral 1 del artículo 46, por el siguiente:

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

“No será objeto de sanción penal por haber incurrido en los hechos tipificados en el inciso primero, el que habiendo accedido a un sistema informático cuyo responsable tenga domicilio en Chile, lo hiciera cumpliendo con las siguientes condiciones:

1) Encontrarse inscrito en el registro que al efecto lleve la Agencia Nacional de Ciberseguridad;

2) Que el acceso se haya realizado habiendo informado previamente de ello a la Agencia;

3) Que el acceso y las vulnerabilidades de seguridad detectadas hayan sido reportadas al responsable del sistema informático y a la Agencia, tan pronto se hubiere realizado;

4) 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 utilizando métodos que pudieran conducir a denegación de servicio, a pruebas físicas, utilización de código malicioso, ingeniería social y alteración, eliminación, exfiltración o destrucción de datos;

5) No haber divulgado públicamente la información relativa a la potencial vulnerabilidad;

6) Que se trate de un acceso a un sistema informático de un organismo del Estado o sus proveedores de servicios de telecomunicaciones; infraestructura digital; servicios digitales o servicios de tecnología de la información gestionados por terceros. En el resto de los casos, requerirá del consentimiento del responsable del sistema informático.

7) Haber dado cumplimiento a las demás condiciones sobre comunicación responsable de vulnerabilidades que al efecto hubiere dictado la Agencia.”.”

La asesora legislativa del Ministerio del Interior, abogada señora Michelle Bordachar, explicó que la norma sobre hacking ético que venía aprobada del Senado, había sido objeto de indicaciones y ciertos reparos, especialmente por el tema del consentimiento. En esta redacción, señaló, busca que se notifiquen siempre las vulnerabilidades de un sistema informático, esto es cuando un código puede ser explotado para acceder a un sistema, y no así exigir la notificación de los errores de código, ya que sería desproporcionado.

Sí bien no se llegó a un acuerdo con la mesa técnica de trabajo de prescindir del consentimiento de los privados, sí se logró consensuar agregar dos requisitos nuevos, relativos a que las personas que hayan detectado la vulnerabilidad se hayan inscrito previamente en un registro que al efecto lleva la Agencia, y además que antes de explotar la vulnerabilidad le avisen a la Agencia.

El presidente diputado señor Andrés Longton, expresó que desde un comienzo no se estaba de acuerdo con el hacking ético, por una variedad de razones que tiene que ver con la privacidad de ingresar a los sistemas informáticos de los cuales no se tiene autorización con independencia de la responsabilidad que se pueda tener aquellos organismos por la negligencia o eventual comisión de delito por haber expuesto datos de personas que tenían a su cargo.

El diputado señor José Miguel Castro, manifestó su acuerdo y consideró un avance tener una lista y que se ejecute un aviso previo, sin embargo, no está de acuerdo con la idea establecida en el numeral 6, sobre el auditar a las empresas que presenten servicios a la administración del Estado, ya que se sobredimensiona el objetivo.

La Comisión llegó al acuerdo de aprobar la indicación de reemplazo al numeral 1 del artículo 46, siempre y cuando se elimine de su número 6, la frase “o sus proveedores de servicios de telecomunicaciones; infraestructura digital; servicios digitales o servicios de tecnología de la información gestionados por terceros”, además de reemplazar en el mismo numeral, la frase “de un organismo del Estado” por la siguiente “de los organismos de la administración del Estado”.

Puesto en votación **el artículo 46 en conjunto con la indicación y sus modificaciones que reemplaza su numeral 1, se aprueba por unanimidad**. Votan a favor las y los diputados señores Jorge Alessandri, José Miguel Castro, Lorena Fries, Andrés Longton (presidente) y Alejandra Placencia. Sin votos en contra ni abstenciones. **(5-0-0).**

Por aprobarse el artículo 46 en conjunto con la indicación y sus modificaciones que reemplaza su numeral 1, reglamentariamente se rechaza el numeral 1 original del artículo 46 del texto aprobado por el Senado y las indicaciones N°s 50, 89 y 90.

Luego se da lectura al numeral 2 del artículo 46 aprobado por el Senado:

“2. Derógase el artículo 16”.

La asesora legislativa del Ministerio de Interior, señora Michelle Bordachar, expuso que, según lo aprobado hasta el momento, lo relativo al artículo 16 de

la ley de delitos informáticos, establece lo mismo que el artículo 2, por lo que no tiene ningún efecto práctico aprobar el numeral 2 del artículo 46, por lo que sugirió rechazarlo.

Puesto en votación el **numeral 2 del artículo 46, se aprueba por unanimidad.** Votan a favor las y los diputados señores Jorge Alessandri, Cristián Araya, Jaime Araya, José Miguel Castro, Lorena Fries, Andrés Longton (presidente), Andrés Jouannet, Henry Leal, Raúl Leiva, Gloria Naveillán, Maite Orsini, Alejandra Placencia y Diego Schalper. Sin votos en contra ni abstenciones. **(13-0-0).**

***

Se da lectura al artículo 47 aprobado por el Senado:

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 éste debe proveer. Asimismo, el informe se pronunciará sobre los operadores que resultan de importancia vital para la provisión de esos servicios esenciales.".

Al artículo 47, **los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°91:**

"Suprímese el artículo 47".

La **asesora legislativa del Ministerio de Interior, señora Michelle Bordachar,** señaló que, en virtud de lo aprobados con anterioridad, sugiere se rechace este artículo, por cuanto quedaría como letra muerta, ya que esa atribución ya fue trasladada desde la Agencia a las autoridades sectoriales.

Puesta en votación **la indicación N°91, se aprueba por unanimidad.** Votan a favor las y los diputados señores Jorge Alessandri, Cristián Araya, Jaime Araya, José Miguel Castro, Lorena Fries, Andrés Longton (presidente), Andrés Jouannet, Henry Leal, Raúl Leiva, Gloria Naveillán, Maite Orsini, Alejandra Placencia y Diego Schalper. Sin votos en contra ni abstenciones. **(13-0-0).**

Por aprobarse la indicación 91, reglamentariamente se rechaza el artículo 47 del texto aprobado por el Senado.

***

Se da lectura al artículo 48 aprobado por el Senado:

"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".

Al artículo 48, los diputados señores **José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°92:**

"Suprímese el artículo 48"

Puesta en votación **la indicación N°92, se aprueba por unanimidad.** Votan a favor las y los diputados señores Jorge Alessandri, Cristián Araya, Jaime Araya, José Miguel Castro, Lorena Fries, Andrés Longton (presidente), Andrés Jouannet, Henry Leal, Raúl Leiva, Gloria Naveillán, Maite Orsini, Alejandra Placencia y Diego Schalper. Sin votos en contra ni abstenciones. **(13-0-0).**

Por aprobarse la indicación 92, reglamentariamente se rechaza el artículo 48 del texto aprobado por el Senado.

***

Nuevas indicaciones formuladas por el Ejecutivo:

La **asesora legislativa del Ministerio de Interior, señora Michelle Bordachar,** comentó que hace un par de semanas fue reemplazado el artículo 21 que establecía la existencia de los CSIRT sectoriales, y a este varias referencias, los que pasaron a ser CSIRT que pertenezcan a organismos de la Administración del Estado. Por lo anterior, por un tema de concordancia, se debe reabrir debate de aquellos que establecían la expresión de CSIRT sectorial y armonizarlo con el resto del texto aprobado.

Por lo reseñado, el Ejecutivo formuló las siguientes indicaciones de adecuación formal:

“1.- Al actual artículo 23, que ha pasado a ser artículo 26 (27): Para reemplazar, en el inciso tercero (segundo), el vocablo "Sectoriales" por la frase "que pertenezcan a organismos de la Administración del Estado".

2.- Al actual artículo 29, que ha pasado a ser artículo 32 (33): Para modificar el actual artículo 29, que ha pasado a ser artículo 32 (33), en el siguiente sentido:

a) Reemplázase, en el inciso primero, la expresión "o Sectoriales" por "o que pertenezcan a organismos de la Administración del Estado”.

b) Reemplázase, en el inciso tercero, la expresión “o Sectoriales" por "o que pertenezcan a organismos de la Administración del Estado”.

3.- Al Título VIII, para reemplazar en su encabezado la frase “de Ciberseguridad” por la frase “sobre Ciberseguridad”.

El **presidente diputado señor Andrés Longton**, propuso a la Comisión, poner en votación reabrir el debate de estos dos artículos, que son meramente adecuatorios, y en caso de aprobarse la reapertura, someter la votación inmediata de la votación de las indicaciones recientemente leídas.

Puesta en votación **la reapertura de la discusión y votación de los artículos 23 y 29 originales al texto aprobado por el Senado, se aprueba por unanimidad.** Votan a favor las y los diputados señores Jorge Alessandri, Cristián Araya, Jaime Araya, José Miguel Castro, Lorena Fries, Andrés Longton (presidente), Andrés Jouannet, Henry Leal, Raúl Leiva, Gloria Naveillán, Maite Orsini, Alejandra Placencia y Diego Schalper. Sin votos en contra ni abstenciones. **(13-0-0).**

Puestas en votación **las indicaciones adecuatorias formuladas por el Ejecutivo a los artículos 23 y 29 originales al texto aprobado por el Senado, se aprueban por unanimidad.** Votan a favor las y los diputados señores Jorge Alessandri, Cristián Araya, Jaime Araya, José Miguel Castro, Lorena Fries, Andrés Longton (presidente), Andrés Jouannet, Henry Leal, Raúl Leiva, Gloria Naveillán, Maite Orsini, Alejandra Placencia y Diego Schalper. Sin votos en contra ni abstenciones. **(13-0-0).**

Además, **el Ejecutivo, formuló una indicación para reabrir la discusión y votación del actual artículo 44 que ha pasado a ser 52 (53), en el siguiente sentido:**

“a) Incorpórase en el inciso primero, a continuación del punto aparte, que pasa a ser coma, la expresión “de conformidad con lo previsto en los artículos 4 a 8 y en las demás disposiciones aplicables de la presente ley. Las referencias al reglamento contenidas en el artículo 8 se entenderán efectuadas a las normas que adopten los respectivos órganos internos de las instituciones antes referidas.”.

b) Reemplázase, en el inciso segundo, la expresión “dicha función” por la expresión “la función de dirección y administración de la respectiva institución u organismo”.

c) Reemplázase el inciso cuarto por el siguiente: Asimismo, si aluna de las instituciones u órganos señalados en este artículo revistiere el carácter de autoridad sectorial o contare por otro concepto legal con competencias reguladoras o fiscalizadoras, deberá considerársele, para los efectos de los artículos 6, 24 y 25, en lo que proceda respecto del sector o actividad correspondiente”.

d) Incorpórase el siguiente inciso final: En todo caso, la Agencia requerirá al respectivo organismo o entidad señalada en el presente artículo el informe previo fundado a que se refiere el artículo 6, tratándose de la calificación que la Agencia pueda efectuar de alguno de ellos en la condición de prestador de servicios esenciales, o en cuanto a su calidad de organismo de importancia vital, en los términos previstos en esta ley”.

Puesta en votación **la reapertura de la discusión y votación del artículo 44 original al texto aprobado por el Senado, se rechaza por unanimidad**. No hay votos a favor. Votan en contra las y los diputados señores Jorge Alessandri, Cristián Araya, Jaime Araya, José Miguel Castro, Lorena Fries, Andrés Longton (presidente), Andrés Jouannet, Henry Leal, Raúl Leiva, Gloria Naveillán, Maite Orsini, Alejandra Placencia y Diego Schalper. Sin abstenciones. **(0-13-0).**

Nueva indicación formulada por la diputada doña Alejandra Placencia y el diputado señor Cristián Araya, formuló una indicación que incorpora un nuevo artículo 18, a continuación del actual artículo 17 o artículo 14 del texto del proyecto aprobado por el Senado, pasando el actual artículo 18 a ser el artículo 19 y así sucesivamente, del siguiente tenor:

“Artículo 18. Notificación responsable de vulnerabilidades. No serán aplicables las obligaciones previstas en el artículo 175 del Código Procesal Penal y en el artículo 61, literal k) del Estatuto Administrativo, a los trabajadores de la Agencia respecto de la información que reciban por parte de las personas que les notifiquen vulnerabilidades de ciberseguridad. La Agencia deberá mantener en secreto la notificación, sus antecedentes y la identidad de quien la realice, no pudiendo esta última ser revelada sin el consentimiento expreso de la persona que la realizó.”

Señaló, la **diputada Alejandra Placencia**, que esta redacción no es una novedad, es aplicada a nivel comparado y es conocido como “puerto seguro”.

Puesta en votación la **indicación de la diputada señora Alejandra Placencia, recientemente leída, se aprueba por unanimidad.** Votan a favor las y los diputados señores Jorge Alessandri, Cristián Araya, Jaime Araya, José Miguel Castro, Lorena Fries, Andrés Longton (presidente), Andrés Jouannet, Henry Leal, Raúl Leiva, Gloria Naveillán, Maite Orsini, Alejandra Placencia y Diego Schalper. Sin votos en contra ni abstenciones. **(13-0-0).**

****

Artículos transitorios.

A continuación, se discuten y votan las ocho disposiciones transitorias aprobadas por el Senado.

El **presidente diputado señor Andrés Longton,** sugirió dar discusión y votación, conjunta, primeramente, a los artículos tercero, cuarto, sexto y séptimo, por ser meramente formales y existir consenso respecto a ellos.

Se da lectura a los artículos tercero, cuarto, sexto y séptimo transitorios del texto aprobado por el Senado:

“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 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.”

Puestos en **votación conjunta, los artículos tercero, cuarto, sexto y séptimos transitorios, se aprueban por unanimidad.** Votan a favor las y los diputados señores Jorge Alessandri, Cristián Araya, Jaime Araya, José Miguel Castro, Lorena Fries, Andrés Longton (presidente), Andrés Jouannet, Henry Leal, Raúl Leiva, Gloria Naveillán, Maite Orsini, Alejandra Placencia y Diego Schalper. Sin votos en contra ni abstenciones. **(13-0-0).**

***

Se da lectura al artículo primero transitorio del texto aprobado por el Senado:

“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 párrafos 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 párrafo anterior cumpla con los requisitos respectivos y dé su consentimiento, las modificaciones de estatuto laboral señaladas en el mencionado párrafo 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 párrafo 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.

Al artículo primero transitorio, **el Ejecutivo formuló la siguiente indicación N°21:**

“Para agregar en el artículo primero transitorio, el siguiente numeral 2, nuevo, readecuándose el orden correlativo de los numerales siguientes: “2. Determinar un periodo para la vigencia de las normas establecidas por la presente ley el cual no podrá ser inferior a seis meses desde su publicación.".”.

Al artículo primero transitorio, **el diputado señor Andrés Jouannet, formuló la siguiente indicación N°51:**

“Incorpórese un nuevo inciso primero al artículo primero transitorio, pasando el actual a ser segundo y así sucesivamente, del siguiente tenor: “La presente ley entrará en vigencia para los organismos de la Administración del Estado e instituciones públicas y privadas calificadas como operadores de importancia vital, así como para sus proveedores, el día primero del mes vigésimo segundo posterior a su publicación en el Diario Oficial”.”.

Puesto en **votación el artículo primero transitorio con la indicación N°21 formulada por el Ejecutivo, se aprueban por unanimidad**. Votan a favor las y los diputados señores Jorge Alessandri, Cristián Araya, José Miguel Castro, Lorena Fries, Andrés Longton (presidente), Henry Leal, Gloria Naveillán y Alejandra Placencia. Sin votos en contra ni abstenciones. **(8-0-0).**

Por ende**, se rechaza reglamentariamente la indicación N° 51.**

***

Se da lectura al artículo quinto transitorio del texto aprobado por el Senado:

“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 éstos, 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.”

Acto seguido, **se da lectura al artículo octavo transitorio del texto aprobado por el Senado:**

“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.”.

Al artículo octavo transitorio, **el Ejecutivo formuló la siguiente indicación N°22:**

“Para suprimir el artículo octavo transitorio.”

Al artículo octavo transitorio**, los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon las siguientes indicaciones N°95 y 96:**

95.- “Suprímase el artículo octavo transitorio.”

96.- “Agrégase un nuevo Artículo Octavo Transitorio, nuevo, del siguiente tenor: “Artículo octavo. Las disposiciones permanentes de la ley entrarán en vigencia un año después de la fecha en que, según las disposiciones del Artículo Primero Transitorio, la Agencia entre en funciones. Con todo, la implementación de los diversos CSIRT sectoriales que se señalan en la presente ley podrán comenzar a implementarse desde su publicación, sujetos a la disponibilidad presupuestaria de cada servicio.

La asesora legislativa del Ministerio de Interior, señora Michelle Bordachar, explicó que mientras no existieran los CSIRT sectoriales, el CSIT Nacional haría las veces de CSIT sectorial, pero al eliminarse la norma que establecía los CSIT sectoriales, el artículo quinto transitorio deja de tener efectividad. Respecto al artículo octavo transitorio, ocurre lo mismo, ya que establecía los servicios esenciales, pero como se consensuo finalmente que este tema se regule en el artículo 4, este artículo se vuelve igualmente innecesario.

El presidente diputado señor Andrés Longton, propuso poner en votación conjunta ambos artículos transitorios, y rechazarlos.

Puestos en **votación conjunta, los artículos quinto y octavo transitorios, se rechazan por unanimidad.** No hay votos a favor. Votan en contra las y los diputados

señores Jorge Alessandri, Cristián Araya, José Miguel Castro, Lorena Fries, Andrés Longton (presidente), Henry Leal, Gloria Naveillán, Maite Orsini y Alejandra Placencia. Sin votos en contra ni abstenciones**. (0-9-0).**

Por rechazarse, los artículos quinto y octavo transitorios del texto aprobado por el Senado, las indicaciones N°s 22, 95 y 96, reglamentariamente se rechazan.

***

Se da lectura al artículo segundo transitorio del texto aprobado por el Senado:

“Artículo segundo: El Presidente de la República, sin sujetarse a lo dispuesto en el título VI de la ley Nº19.882, 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.”

Al artículo segundo transitorio, **los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, formularon la siguiente indicación N°93:**

“Intercálase en el Artículo Segundo Transitorio entre la palabra “personal” y el punto aparte, lo siguiente: “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.”

Al artículo segundo transitorio, **el diputado señor Jorge Alessandri, formuló la siguiente indicación N°94:**

“En el artículo segundo, para añadir un inciso segundo, nuevo, del siguiente tenor: “Con todo, no podrá ser nombrado en el cargo de Director o Directora de la Agencia conforme al inciso primero de este artículo, quien hubiere prestado servicios en la Administración del Estado bajo la modalidad de planta, contrata, honorarios o conforme a las normas del Código del Trabajo, dentro del período de tres años anteriores a la publicación de esta ley en el Diario Oficial”.”.

“En el artículo segundo, para añadir un inciso tercero, nuevo, del siguiente tenor: “La prohibición dispuesta en el inciso anterior aplicará también para el primer nombramiento del Director o Directora de la Agencia que deba realizarse de acuerdo al Sistema de Alta Dirección Pública”.”.

Al artículo segundo transitorio, **los diputados señores Cristián Araya y Henry Leal, formularon la siguiente indicación:**

“Con todo, no podrá ser nombrado en el cargo de Director o Directora de la Agencia conforme a este artículo, 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."

El **señor Subsecretario del Interior, don Manuel Monsalve,** expresó que entendiendo el contenido de la norma y sus indicaciones, al Ejecutivo le parece razonable y atendible la indicación N°93, formulada por los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper, por cuanto ya existe lo propuesto en el sistema público, sin embargo el resto de la indicaciones le parece que persiguen 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 presidente diputado señor Andrés Longton, consideró que la indicación formulada en conjunto con otros diputados es compatible con el texto de la norma por lo que podrían someterse en votación conjunta.

El diputado señor Jorge Alessandri, señaló que la figura de prohibiciones en el sistema público para participar de un proceso de alta dirección pública, hay varias, y los costos de ser parte del sistema también son muchos, como por ejemplo que quien está a cargo del diseño o creación de un servicio u órgano o entidad, no puede ser quien en un futuro lo lidere, ya que se corre el riesgo que lo establece a su medida. Por todo, las propuestas no son incompatibles y sí son atendibles pensando en el bien del país.

La **asesora legislativa del Ministerio de Interior, señora Michelle Bordachar,** comentó que si bien está de acuerdo con lo expuesto en relación con la indicación N°93, no así con la N°94, ya que excluye a toda persona que hubiere prestado servicios en la Administración del Estado bajo la modalidad de planta, contrata, honorarios o conforme a las normas del Código del Trabajo, y no solo a quien lo haya establecido el servicio u organismo, en este caso la Agencia, que por un tema de resguardo a que al diseñarla lo haya hecho como traje a la medida.

Además, respecto a la indicación formulada por los diputados señores Cristián Araya y Henry Leal, consideró ser discriminatoria.

El **diputado señor Jorge Alessandri,** indicó que entiende lo señalado con anterioridad, por lo que está de acuerdo con la indicación N°93 y la formulada por los diputados señores Cristián Araya y Henry Leal, y por ello **retiró su indicación N°94.**

La **diputada señora Lorena Fries,** expresó que bajo su parecer nunca ha estado de acuerdo con la cancelación de las personas, y una de estas indicaciones hace aquello.

Puestos en **votación conjunta, el artículo segundo transitorio con la indicación N°93, se aprueban por unanimidad.** Votan a favor las y los diputados señores Jorge Alessandri, Cristián Araya, José Miguel Castro, Lorena Fries, Andrés Longton (presidente), Henry Leal, Gloria Naveillán, Maite Orsini y Alejandra Placencia. Sin votos en contra ni abstenciones. **(9-0-0).**

Luego, **p**uestos en **votación conjunta, el artículo segundo transitorio con la indicación complementaria formulada por los diputados señores Cristián Araya y Henry Leal, se aprueban por la mayoría de votos.** Votan a favor las y los diputados señores Jorge Alessandri, Cristián Araya, José Miguel Castro, Henry Leal y Gloria Naveillán. Votan en contra las diputadas señoras Lorena Fries, Maite Orsini y Alejandra Placencia. Se abstuvo el diputado señor Andrés Longton (presidente). **(5-3-1).**

En virtud del artículo 15 del reglamento de la Corporación, la Secretaría de la Comisión realizará las adecuaciones y correlaciones numéricas y de referencia de los artículos, numerales y letras aprobadas por esta Comisión,

V. ARTÍCULOS E INDICACIONES RECHAZADAS POR LA COMISIÓN.

ARTÍCULOS RECHAZADOS:

1.- 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 éstos 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, las Fuerzas 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 éste 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.

2.- Los siguientes numerales del artículo 2º:

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 éste 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.

3.- 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 éstos, sólo 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.

4.- Artículo 4°. Determinación de los servicios esenciales e identificación de los operadores de importancia vital. En el ejercicio de la facultad establecida en la letra g) del artículo 9° de esta ley, la Agencia determinará aquellos servicios que sean considerados esenciales para los efectos de esta ley, y dentro de éstos 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 éstos, 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 contado 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.

5.- 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

6.- 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 éste 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.

7.- Inciso segundo del artículo 8º:

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.

8.- 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, sobre protección de la vida privada.

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 mencionada 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 éstos, 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, que declara el mes de octubre como el mes nacional de la ciberseguridad.

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

9.- Literal g) del artículo 11.

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

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

10.- 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 ésta lo solicite.

En el ejercicio de sus funciones, los CSIRT Sectoriales deberán dar cumplimiento a todos 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.

11.- 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 éstos 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.

12.-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.

13.- 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 contado 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.

14.- 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.

15.- -incisos tercero y siguientes del artículo 36:

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 contado desde que la respectiva resolución quede firme.

16.- 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.

17.- 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.

18.- Artículo 46. Introdúcense las siguientes enmiendas en 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 utilizando 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 sobre 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.".

INDICACIONES RECHAZADAS:

1.- Del diputado señor Jorge Alessandri:

En el artículo 1° del proyecto de ley, para reemplazarlo por el siguiente:

"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 éstos 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 efectos de esta ley, la Administración del Estado estará constituida por los Ministerios, las delegaciones presidenciales regionales y provinciales, los Gobiernos Regionales, las Municipalidades, las Fuerzas Armadas, de Orden y Seguridad Pública, las empresas públicas creadas por ley, y los órganos y servicios públicos creados para el cumplimiento de la función administrativa.

Los organismos autónomos constitucionales se ajustarán a las disposiciones de esta ley que expresamente ésta señale, y a las de sus respectivas leyes orgánicas que versen sobre los asuntos a que se refiere el inciso primero de este artículo.

Las disposiciones de esta ley serán aplicables a las empresas del Estado y sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio.

La institucionalidad establecida por esta ley velará por la protección, promoción y respeto del derecho a la seguridad informática de las personas y sus familias, que comprende la adopción de 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.”.

2.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Reemplázase, en el inciso primero del artículo 1° la palabra “privadas” por “que prestan servicios esenciales y las calificadas como operadores de importancia vital”.

3.- Del diputado señor Andrés Jouannet:

Reemplácese en el inciso primero del artículo 1° propuesto, la expresión “, así como los deberes de las instituciones privadas” por “y los deberes de las instituciones públicas y privadas calificadas como operadores de importancia vital, así como la normativa que regula las relaciones entre estos y sus proveedores”.

4.- Del diputado señor Jorge Alessandri y la diputada señora Gloria Naveillan:

Para agregar, en el artículo 1°, al final del primer inciso la siguiente frase; “Asimismo, se deberá, en coordinación con el Ministerio de Relaciones Exteriores, establecer los convenios de cooperación internacional en materias de ciberseguridad.”

5.- Del Ejecutivo:

Para eliminar, en el artículo primero, inciso segundo, la siguiente frase: “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 éste tenga participación accionaria superior al 50% o mayoría en el directorio, salvo que sean calificadas como operadores de importancia vital.”.

6.- Del diputado señor Cristián Araya:

Al artículo primero del proyecto de ley: Para agregar en el inciso primero del artículo 1° a continuación de la expresión “, así como los deberes de las instituciones privadas” la expresión “calificadas como operadores de importancia vital

7.- Del diputado señor Andrés Jouannet:

Suprímase en el inciso segundo del artículo 1° propuesto, la expresión "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 éste tenga participación accionaria superior al 50% o mayoría del directorio, salvo que sean calificadas como operadores de importancia vital".

8.- Del diputado señor Jorge Alessandri y la diputada señora Gloria Naveillan:

Para eliminar en el artículo 1°, el párrafo final del 2° inciso y reemplazarlo por la siguiente frase: “Se aplicarán las disposiciones de esta ley a las empresas o instituciones calificadas como operadores de importancia vital, sean estas públicas creadas por ley o empresas del Estado en cuyas sociedades el Estado tenga una participación accionaria superior al 50% o mayoría en el directorio, y a las empresas de sector privado calificadas como operadores de importancia vital.”

9.- Del diputado señor Jorge Alessandri:

Para eliminar en el artículo 1°, el párrafo final del 2° inciso y reemplazarlo por el siguiente: “Asimismo, las disposiciones de esta ley serán aplicables a las empresas

públicas creadas por ley y a las empresas del Estado y sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio".

10.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Introdúcense las siguientes modificaciones al inciso segundo del artículo 1°:

i. Sustitúyase la frase "a los ministerios, las delegaciones presidenciales regionales y provinciales, los gobiernos regionales, las municipalidades, las Fuerzas Armadas, las Fuerzas de Orden y Seguridad Pública y los órganos y servicios públicos creados para el cumplimiento de la función administrativa" por "aquellos indicados en el inciso segundo del artículo 1º del DFL Nº1-19.653 que fija texto refundido, coordinado y sistematizado de la ley Nº 18.575, orgánica constitucional de Bases Generales de la Administración del Estado y las empresas del Estado y sociedades en que éste tiene una participación accionaria superior al 50% o designa a la mayoría de los miembros de su Directorio.";

ii. Sustitúyase la oración: "Los órganos autónomos constitucionales se ajustarán a las disposiciones de esta ley que así lo señalen" por "Los órganos autónomos constitucionales dictarán su propia normativa y quedarán sujetos a su propia tutela, sin perjuicio de la cooperación y asistencia que sus normativas propias dispongan";

iii. Suprímase lo siguiente "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 éste tenga participación accionaria superior al 50% o mayoría en el directorio, salvo que sean calificadas como operadores de importancia vital".

11.- Del diputado señor Andrés Jouannet:

Suprímase en el inciso tercero del artículo 1° propuesto las expresiones "y sus familias" e ", incluyendo las herramientas de cifrado".

12.- Del diputado señor Andrés Jouannet:

Suprímase en el inciso tercero del artículo 1° propuesto las expresiones "y sus familias" e ", incluyendo las herramientas de cifrado".

13.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Sustitúyase el inciso tercero del artículo 1° por el siguiente:

La institucionalidad establecida por esta ley orientará sus acciones para lograr el más alto nivel de ciberseguridad con el objetivo de mejorar el funcionamiento de los mercados y los servicios que las instituciones públicas y privadas entregan a la ciudadanía."

14.- Del Ejecutivo:

Para reemplazar en el epígrafe del párrafo 1° la frase "Servicios esenciales y operadores" por la palabra "Operadores".

15.- Del diputado señor Jorge Alessandri:

En el artículo 2° numeral 5 del proyecto de ley, para sustituirlo por el siguiente: "5. Autoridad sectorial: aquellos servicios públicos dotados de facultades regulatorias, fiscalizadoras y sancionatorias respecto de sus regulados.

16.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

“Sustitúyese el numeral 5 del artículo 2°, por el siguiente: “5. Autoridad sectorial: aquellos servicios públicos cuya finalidad es la regulación y/o supervigilancia de un determinado sector de la economía o de actividades realizadas por particulares en ejercicio de la libertad económica.”

17.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

En el numeral 13 del artículo 2°, intercálase entre la palabra “competente” y la frase “de conformidad”, entre comas, lo siguiente: “en el ámbito de sus respectivas competencias”.

18.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

“Suprímase el numeral 17 del artículo 2°.”

19.- Del diputado señor Jorge Alessandri:

En el artículo 2° numeral 17 del proyecto de ley, para suprimirlo.

20.- Del diputado señor Cristián Araya:

Al artículo segundo del proyecto de ley: Para suprimir en el numeral 17 la expresión “imposibles de lograr de forma independiente”.

21.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

“Sustitúyese el numeral 18 del artículo 2°, por el siguiente: 18. Interoperabilidad: capacidad de los sistemas informáticos de ser capaces de interactuar y operar entre sí, a través de estándares abiertos que permitan una segura y expedita interconexión entre ellos.”

22.- Del diputado señor Jorge Alessandri:

En el artículo 2° numeral 18 del proyecto de ley, para añadir después del punto aparte, que pasa ser una coma “,” la siguiente frase: “con pleno respeto de las normas sobre protección de datos personales”.

23.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

“Sustitúyese el numeral 20 del artículo 2°, por el siguiente: “20. Operadores de importancia vital: son operadores de importancia vital los organismos de la Administración del Estado, el Coordinador Eléctrico Nacional, aquellos agentes privados de los sectores de energía, servicios sanitarios; telecomunicaciones, servicios postales y mensajería; transporte, banca, infraestructura de los mercados financieros, infraestructura digital, gestión de servicios de tecnologías de la información, determinados como tales por el procedimiento del artículo 4º, así como otros que, en virtud del mismo procedimiento, deban tener tal calidad, siempre que dependan de las redes y sistemas informáticos para su funcionamiento y su afectación, interceptación, interrupción o destrucción puede tener un impacto crítico en la seguridad nacional, en la seguridad interior y el orden público, en la provisión continua y regular de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que éste debe proveer o garantizar.”

24.- Del diputado señor Jorge Alessandri:

En el artículo 2° numeral 20 del proyecto de ley, para sustituirlo por el siguiente: “20. Operadores de importancia vital: son tales los órganos de la Administración del Estado, las empresas del Estado y sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio, y aquellos agentes privados que así sean calificados por la Agencia de conformidad con esta ley, cuyo funcionamiento dependa de las redes y sistemas informáticos, y siempre que su afectación, interceptación, interrupción o destrucción pueda producir graves efectos en la seguridad nacional, en la provisión de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que éste debe proveer o garantizar.”.

25.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Sustitúyase, en el numeral 24 del artículo 2°, la frase “sometido a la supervigilancia de un órgano público con facultades suficientes para regular, fiscalizar y eventualmente sancionar” por “bajo la regulación y/o supervigilancia de una autoridad sectorial”.

26.- Del diputado señor Jorge Alessandri:

Para suprimir, en el numeral 24 del artículo 2°, la palabra “eventualmente”.

27.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Sustitúyase el numeral 25 del artículo 2°, por el siguiente: “25. Servicios esenciales: son servicios esenciales aquellos provistos por los organismos de la Administración del Estado, por el Coordinador Eléctrico Nacional y por aquellos agentes privados de los sectores de energía, servicios sanitarios; telecomunicaciones, servicios postales y mensajería; transporte, banca, infraestructura de los mercados financieros, infraestructura digital, gestión de servicios de tecnologías de la información y de otros que se determinen en virtud del procedimiento del artículo 4º, cuya afectación, de cualquier manera, cause un grave daño a la salud o al abastecimiento de la población, a actividades económicas esenciales, al medioambiente o a la seguridad del país.”

28.- Del diputado señor Jorge Alessandri:

En el artículo 2° numeral 25 del proyecto de ley, para sustituir la frase “tendría”, por la siguiente: “pueda producir”.

29.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Incorpórese un nuevo numeral 28 al artículo 2°, del siguiente tenor: “28. Consulta pública y recepción de observaciones: proceso participativo en cuya virtud antes de la emisión de un acto administrativo, éste se da a conocer públicamente, por medios digitales; se disponen los mecanismos necesarios para que los interesados puedan formularle observaciones; y se publican tanto las observaciones como las respuestas de la autoridad a ellas.”

Suprímase el numeral 1 del inciso primero del artículo 2° propuesto.

30.- Del diputado señor Andrés Jouannet:

Suprímase el numeral 8 del inciso primero del artículo 2° propuesto.

31.- Del diputado señor Andrés Jouannet:

Suprímase el numeral 10 del inciso primero del artículo 2° propuesto.

32.- Del diputado señor Andrés Jouannet:

Suprímase el numeral 11 del inciso primero del artículo 2° propuesto.

33.- Del diputado señor Andrés Jouannet:

Suprímase el numeral 16 del inciso primero del artículo 2° propuesto.

34.- Del diputado señor Andrés Jouannet:

Suprímase el numeral 17 del inciso primero del artículo 2° propuesto.

35.- Del diputado señor Andrés Jouannet:

Suprímase el numeral 18 del inciso primero del artículo 2° propuesto.

36.- Del diputado señor Andrés Jouannet:

Suprímase el numeral 19 del inciso primero del artículo 2° propuesto.

37.- Del diputado señor Andrés Jouannet:

Reemplácese en el artículo 2° Numeral N°20 propuesto, la expresión “tener una repercusión importante en” por “amenazar”.

38.- Del diputado señor Andrés Jouannet:

Incorpórese en el artículo 2° Numeral N°20 propuesto, luego de “actividades sociales o económicas cruciales,”, la expresión “en alguno de los sectores o subsectores regulados de alta criticidad para el país establecidos o identificados en conformidad con la presente ley”,

39.- Del diputado señor Andrés Jouannet:

Suprímase en el artículo 2° Numeral N°20 propuesto, la expresión “, en general, de”.

40.- Del diputado señor Andrés Jouannet:

“Artículo 2°, N°25. Servicios Esenciales. Todo servicio identificado como tal de conformidad con el procedimiento establecido en el artículo 4° de la presente ley, que se provea o preste en sectores o subsectores regulados de alta criticidad para el país, incluyendo los sectores de energía y combustibles, sanitario, salud, telecomunicaciones, transporte, bancario y financiero, así como por la administración del Estado, el Poder Legislativo y el Poder Judicial”.

41.- Del diputado señor Andrés Jouannet:

Suprímase en el artículo 2° Numeral 26 propuesto.

42.- Del diputado señor Cristián Araya:

Al artículo tercero del proyecto de ley: Para suprimir el numeral 11.

43. De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Para sustituir el artículo 3º por el siguiente:

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

1. Principio de subsidiariedad regulatoria. Si una autoridad sectorial dicta normativa más exigente que la contemplada en esta ley, se preferirá aquella por sobre ésta;

2. Principio de especialidad sectorial. Frente a la existencia de una autoridad sectorial que cuente con atribuciones establecidas por ley en el ámbito regulatorio, supervisor y sancionatorio, se respetará la prevalencia de las potestades sectoriales en cada caso, en el ámbito de sus competencias. En caso de duda, se privilegiará a la autoridad sectorial respectiva.

3. Principio de coordinación. De conformidad a lo dispuesto por el inciso segundo del artículo 5º del DFL Nº1-19.653 que fija texto refundido, coordinado y sistematizado de la ley Nº18.575, orgánica constitucional de Bases Generales de la Administración del Estado, la Agencia y las autoridades sectoriales deberán cumplir sus cometidos coordinadamente y propender a la unidad de acción, evitando la duplicación o interferencia de funciones.

Asimismo, para la dictación de actos administrativos, se tendrá especialmente en cuenta lo dispuesto por el artículo en el artículo 37 bis de la Ley Nº19.880 que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.”

44.- Del diputado señor Jorge Alessandri:

Para sustituir, en el numeral 6 del artículo 3°, la frase “niñas, niños, jóvenes, personas de la tercera edad y disidencias sexogenéricas”, por la siguiente: “niños, niñas y adolescentes y personas de la tercera edad”.

45.- Del Ejecutivo:

Para reemplazar en el artículo 4°, el inciso primero por el siguiente: “Artículo 4°. Identificación de los operadores de importancia vital. En el ejercicio de la facultad establecida en el literal g) del artículo 9° de esta ley, la Agencia determinará los operadores de importancia vital dentro de los servicios esenciales identificados en el Título IX, conforme los siguientes criterios y procedimiento:”.

46. Del Ejecutivo:

Para suprimir en el artículo 4°, el inciso segundo, readecuando el orden correlativo de los incisos siguientes.

47. De los diputados señores José Miguel Castro y Andrés Jouannet

Para incorporar un inciso penúltimo en el artículo cuarto: En el caso del servicio esencial de telecomunicaciones previsto en el artículo cuarto, para efectos de esta ley, la calificación respecto de qué servicios, redes o elementos de red y sistemas específicos tendrán dicha calidad, se sujetará a la declaración mediante resolución fundada que realice la Subsecretaría de Telecomunicaciones conforme a lo señalado en la norma técnica sectorial resolución exenta número 1318 del año 2020, dictada por este mismo organismo o aquella que la reemplace, quien además notificará a la Agencia dicha calificación.

48. Del Ejecutivo:

Para modificar en el artículo 4°, el inciso quinto, que ha pasado a ser cuarto, en el siguiente sentido:

a. Reemplázase la frase “los servicios que deban calificarse como esenciales e identifique, para cada uno de éstos, aquellos operadores que resultan de importancia vital

para su provisión” por la frase “las entidades que deban calificarse como operadores de importancia vital”.

b. Reemplázase la frase “podrá requerir informes similares a otros organismos públicos o instituciones privadas.” por la frase “deberá requerir informes similares a las autoridades sectoriales competentes y a las entidades que puedan ser calificadas como operadores de importancia vital.”.

49. Del Ejecutivo:

Para reemplazar los incisos sexto y séptimo, del artículo 4°, que han pasado a ser quinto y sexto, por el siguiente inciso quinto y final: “Transcurrido este plazo, con los antecedentes que hubiere recibido, la Agencia, mediante resolución fundada de su Director o Directora, determinará los operadores de importancia vital dentro de los servicios esenciales. Esta resolución quedará exenta del trámite de toma de razón de la Contraloría General de la República y contra ella procederá el recurso de reclamación judicial contemplado en el artículo 35 de la presente ley.”.

50. De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Sustitúyase, en el inciso primero del artículo 4° la frase “En el ejercicio de la facultad establecida en la letra g) del artículo 9° de esta ley” por la frase “Cada dos años”.

51. De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Reemplázase el inciso segundo del artículo 4° por el siguiente:

“Para determinar los servicios provistos por agentes privados que deben calificarse como esenciales, se deberá considerar fundadamente:

a) Lo dispuesto en el numeral 25 del artículo 2º de esta ley;

b) La gravedad del daño que la afectación, interceptación, interrupción o destrucción del servicio podría causar a la vida o integridad física de las personas, al abastecimiento de la población, a las actividades económicas, a la defensa nacional, al normal funcionamiento de la sociedad, al medioambiente o a la seguridad del país;

c) La condición de prestarse el servicio bajo concesión de servicio público;

d) La posibilidad de sustitución del servicio, tal que ello no implique perturbación en su acceso;

e) La magnitud de los usuarios en relación al área o sector que se verían afectados en caso de afectarse, interceptarse, interrumpirse o destruirse el servicio;

f) De modo general, el grado de afectación del normal desarrollo y bienestar de la población.”

52. De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Reemplázase el inciso tercero del artículo 4° por los siguientes incisos tercero, cuarto y quinto nuevos:

“Para determinar que agentes privados prestadores esenciales tienen la calidad de operador de importancia vital, se deberán reunir los siguientes requisitos:

a) La prestación de dicho servicio depende para su provisión de las redes y sistemas informáticos; y

b) La afectación, interceptación, interrupción o destrucción del servicio puede tener un impacto crítico en la seguridad nacional, en la seguridad interior y el orden público, en la provisión continua y regular de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado y, en general, de los servicios que éste debe proveer o garantizar.

Además, podrán tener la calidad de operador de importancia vital aquellos agentes privados que, aun cuando no tengan la calidad de prestadores de servicios esenciales, reúnan los requisitos indicados en el inciso anterior y su inclusión sea indispensable, por motivos fundados, por haber adquirido un rol crítico para el abastecimiento por la población, la distribución de bienes o la producción de aquellos indispensables o estratégicos para el país.

En cualquier caso, siempre se deberá tener en consideración el tamaño del agente privado, teniendo especialmente en consideración las características y necesidades de las micro, pequeñas y medianas empresas, tal como se definen en la ley N°20.416, que fija normas especiales para las empresas de menor tamaño.

53. De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Introdúcense las siguientes modificaciones al inciso tercero **(cuarto ?)** del artículo 4° que ha pasado a ser sexto:

i. Intercálase un nuevo literal c), pasando el actual c) a ser d), del siguiente tenor: “c) El grado de exposición de la entidad a los riesgos, la probabilidad de que se produzcan incidentes de ciberseguridad y su gravedad, incluidas sus repercusiones sociales y económicas.”

ii. Suprímese el literal h).

54.- Del diputado señor Cristián Araya:

Al artículo cuarto del proyecto de ley:

Uno) En el inciso segundo, para sustituirlo por uno del siguiente tenor: “A fin de determinar qué servicios resultan esenciales, se deberá atender a la entidad del impacto o interrupción podría poner en grave riesgo la seguridad, el orden público, la defensa nacional, la vida de las personas o que estas puedan ejercer sus derechos fundamentales”

Dos) En el inciso quinto, para agregar, a continuación de la expresión “informe fundado”, la expresión “y de carácter secreto”.

55. Del diputado señor Jorge Alessandri:

En el artículo 4° inciso tercero del proyecto de ley, para sustituir la frase “la identificación de” por la siguiente palabra: “identificar”.

56. Del diputado señor Jorge Alessandri:

En el artículo 4° inciso tercero literal c) del proyecto de ley, para sustituir la palabra “tendría”, por la siguiente: “podría producir”.

57. De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Introdúcense las siguientes modificaciones al inciso cuarto, que ha pasado a ser séptimo:

i. Reemplázase la oración “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 éstos, aquellos operadores que resultan de importancia vital para su provisión” por “Para dar cumplimiento a lo prescrito en este artículo, se observará rigurosamente lo dispuesto en el artículo 37 bis de la Ley Nº19.880 que establece bases de

los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado".

ii. Suprímase la oración "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."

58. Del diputado señor Jorge Alessandri y la diputada señora Gloria Naveillán:

Para insertar en el inciso quinto del artículo 4° y a continuación de la frase "de Inteligencia," la siguiente frase "las Autoridades Sectoriales de cada uno de los sectores regulados". En el mismo inciso y a continuación de la frase vital para su provisión… insertar como punto aparte lo siguiente "Dichos informes serán vinculantes para los efectos de las definiciones de los servicios esenciales que promulgue la Agencia"

59. De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Introdúcense las siguientes modificaciones al inciso sexto, que ha pasado a ser octavo:

i.Sustitúyase la frase "para que" por una coma seguida de la frase "previa consulta pública y recepción de observaciones" y la coma que le sigue por un punto seguido.

ii. Sustitúyase la coma que precede a la frase "se pronuncie" y a esta última locución por "dicho organismo se pronunciará".

60. De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Introdúcense las siguientes modificaciones al inciso séptimo. que ha pasado a ser noveno:

i.- Intercálase entre la coma que sigue a la palabra "Ciberseguridad" y la frase "el Ministerio", lo siguiente: "procederá la interposición del recurso de reposición del artículo 59 de la ley Nº19.880 que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado, sin perjuicio de los demás que dicha ley y otros cuerpos legales autoricen, los cuales se regirán por los plazos establecidos en sus respectivas leyes. Encontrándose firme el acto", seguido de una coma;

ii. Suprímase la oración "Este decreto quedará exento del trámite de toma de razón de la Contraloría General de la República."

61. De diputado señor Jorge Alessandri:

En el artículo 4° incisos sexto y séptimo, para sustituirlos por el siguiente inciso final: "Transcurrido este plazo, con los antecedentes que hubiere recibido y mediante resolución fundada de su Director o Directora, la Agencia determinará los operadores de importancia vital dentro de los servicios esenciales. Contra esta resolución procederá el reclamo de ilegalidad contemplado en el artículo 35 de la presente ley".

62. Del diputado señor Jorge Alessandri y la diputada Gloria Naveillan:

Para reemplazar en el inciso final del artículo 4° la frase "quedará exento del" por "será sometido a**"**

63. De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Para incorporar los nuevos incisos décimo, décimo primero y décimo segundo, del siguiente tenor:

“Podrá reclamarse de los fundamentos de hecho y Derecho del decreto señalado en el inciso precedente dentro del plazo de quince días hábiles ante la Corte de Apelaciones del domicilio del reclamante. La Corte dará traslado de la reclamación a la Agencia y ésta dispondrá del plazo de quince días hábiles contados desde que se notifique la reclamación interpuesta, para formular observaciones.

Evacuado el traslado por la Agencia, o vencido el plazo de que dispone para formular observaciones, el tribunal ordenará traer los autos en relación y la causa se agregará extraordinariamente a la tabla de la audiencia más próxima, previo sorteo de la Sala. La Corte podrá, si lo estima pertinente, abrir un término probatorio que no podrá exceder de siete días hábiles, y escuchar los alegatos de las partes.

La Corte dictará sentencia dentro del término de quince días. Contra la resolución de la Corte de Apelaciones se podrá apelar ante la Corte Suprema, dentro del plazo de diez días hábiles, la que conocerá en la forma prevista en los incisos anteriores.”

64. Del diputado señor Andrés Jouannet:

Reemplácese el inciso segundo del artículo 4° propuesto por el siguiente:

“A fin de determinar qué servicios resultan esenciales para efectos de esta ley, la Agencia deberá:

a) Identificar los sectores o subsectores regulados de alta criticidad que son cruciales para mantener actividades sociales y económicas vitales, y determinar los servicios que se presten en estos.

b) Evaluar el eventual impacto que la falta, interrupción o afectación de estos servicios podría tener en la defensa nacional, la seguridad pública, el bienestar económico y social, otros sectores o subsectores regulados de alta criticidad y los servicios públicos que el Estado debe proveer o garantizar.

c) Considerar la presencia o uso de infraestructura crítica de la información necesaria para proporcionar los servicios en los sectores o subsectores identificados en virtud de esta ley.

d) Que la magnitud del eventual impacto sea de tal gravedad como para: causar daños catastróficos en la salud o víctimas masivas; obstaculizar u impedir el ejercicio de las facultades de los organismos de la administración del Estado u otros Poderes del Estado; poner en riesgo gravemente el orden y la seguridad pública; impedir el ejercicio legítimo de los derechos fundamentales de las personas garantizados por la Constitución Política de la República; o afectar negativamente la confianza o legitimidad de la institucionalidad pública”.

65. Del diputado señor Andrés Jouannet:

Intercálese un nuevo literal d) en el inciso tercero del artículo 4° propuesto del siguiente tenor: “d) El tamaño del operador, teniendo especialmente en consideración las características y necesidades de las micro, pequeñas y medianas empresas, tal como se definen en la ley N°20.416, que fija normas especiales para las empresas de menor tamaño”.

66. Del diputado señor Andrés Jouannet:

Incorpórese un nuevo inciso quinto en el artículo 4° propuesto, pasando el actual a ser sexto y así sucesivamente, del siguiente tenor:

“Los factores anteriormente listados deberán ser ponderados en conjunto con criterios sectoriales atendiendo los sectores o subsectores regulados específicos de alta

criticidad establecidos o identificados en conformidad a esta ley. Se deberán utilizar, al menos, los siguientes criterios sectoriales según corresponda:

a) La magnitud de los operadores identificados, por ejemplo, en términos de participación en el mercado. Para estos efectos, se podrán considerar factores tales como el volumen, proporción y número de operaciones de las entidades en periodos de tiempo a nivel nacional, regional o municipal.

b) La importancia sistémica, valorada según los activos totales o la razón entre estos y el producto interno bruto.

c) El tipo y número de usuarios o público específicos a los que van dirigidos los servicios".

67. Del diputado señor Andrés Jouannet:

Reemplácese el inciso quinto, sexto y séptimo del artículo 4° propuesto, que han pasado a ser sexto, séptimo y octavo, respectivamente, por los siguientes incisos sexto, séptimo y octavo:

"La Agencia requerirá a la Agencia Nacional de Inteligencia un informe fundado que identifique aquellos operadores que resultan de importancia vital para la provisión de servicios esenciales identificados de conformidad a esta ley, y podrá requerir informes similares a otros organismos públicos o instituciones privadas. De igual manera, la Agencia requerirá informes fundados a las autoridades sectoriales que regulan, supervisan y fiscalizan los sectores o subsectores regulados de alta criticidad establecidos o determinados de conformidad con la presente ley, los que tendrán el carácter de vinculantes para la Agencia. 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 elaborará una primera propuesta de lista actualizada de operadores de importancia vital. Los posibles operadores de importancia vital que se encuentren en la primera propuesta serán notificados por la Agencia, y dispondrán de un plazo de treinta días hábiles a contar desde el día siguiente a la recepción de la notificación para remitir a la Agencia las alegaciones que considere procedentes, transcurrido el cual la Agencia dictará una resolución dentro un plazo de treinta días hábiles en el que podrá acoger o rechazar su inclusión como operador de importancia vital.

Luego de que la Agencia haya dictado las resoluciones acogiendo o rechazando, según corresponda, las alegaciones de los eventuales operadores de importancia vital de la primera propuesta, y hayan sido resueltas las reclamaciones judiciales que los posibles operadores de importancia vital hayan hecho valer contra estas resoluciones en virtud del procedimiento establecido en el artículo 35° de esta Ley, la Agencia propondrá una segunda propuesta de lista actualizada de posibles operadores de importancia vital al Comité Interministerial de Ciberseguridad para que, dentro del plazo de treinta días hábiles, se pronuncie fundadamente, pudiendo aprobar o sugerir las enmiendas que considere necesarias para su aprobación, las que serán comunicadas a la Agencia".

68. Del Ejecutivo

Para intercalar, en el artículo 5°, inciso primero, entre la expresión "ciberseguridad" y el punto que le sigue, la frase "incluyendo aquellas contenidas en instrucciones generales y particulares dictadas por la Agencia".

69. Del Ejecutivo:

Para incorporar en el artículo 5°, el siguiente inciso final, nuevo: "En todo caso, las obligaciones de ciberseguridad contenidas en las instrucciones generales o particulares dictadas por la Agencia, 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.”.

70. De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Sustitúyese el inciso primero del artículo 5° por el siguiente: “Artículo 5. Deberes generales. La Administración del Estado, así como los agentes privados calificados como prestadores de servicios esenciales y operadores de importancia vital, deben aplicar de manera permanente las medidas necesarias para prevenir, reportar y resolver incidentes de ciberseguridad que pudieran afectarlos. Estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso.”

71. De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Incorpórese, en el inciso quinto del artículo 5° después del punto aparte, que pasa a ser seguido, lo siguiente: “Dichos protocolos y estándares deberán someterse a consulta pública y recepción de observaciones.”

72. Del diputado señor Andrés Jouannet:

Incorpórese al inciso primero del artículo 5° propuesto, luego de “instituciones privadas” la siguiente expresión “y públicas calificadas como operadores de importancia vital”.

73. Del diputado señor Andrés Jouannet:

Suprímase en el inciso tercero del artículo 5° propuesto la expresión “En el caso de los organismos de la Administración del Estado e instituciones privadas que presten servicios esenciales,”.

74. Del diputado señor Andrés Jouannet:

Incorpórese en el inciso cuarto del artículo 5° propuesto, luego del punto final, que pasa a ser punto y seguido, lo siguiente: “Para estos efectos, las necesidades de las micro, pequeñas y medianas empresas deberán ser abordadas a través de, especialmente, la Política Nacional de Ciberseguridad, y la prestación de servicios por parte de la Agencia u otros organismos del Estado competentes, para que les proporcionen orientación y asistencia acerca de cuestiones relacionadas con la ciberseguridad”.

75- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Introdúcense las siguientes modificaciones al artículo 6º: Sustitúyase oración “Todos los organismos del Estado con competencias específicas sobre servicios esenciales y las instituciones privadas calificadas como operadores de importancia vital deberán” por lo siguiente: “La Administración del Estado y las instituciones calificadas como operadores de importancia vital adoptarán las medidas de naturaleza tecnológica, organizacional, física o informativa, según sea el caso, mencionadas en el artículo anterior, y estas garantizarán un nivel de seguridad de los sistemas de redes y de información adecuado en relación con los riesgos planteados. Al evaluar la proporcionalidad de dichas medidas, se tendrá debidamente en cuenta el grado de exposición de la entidad a los riesgos, el tamaño de la entidad y la probabilidad de que se produzcan incidentes y su gravedad, incluidas sus repercusiones sociales y económicas. Tales medidas se fundamentarán en un enfoque basado en riesgos que tenga por objeto proteger los sistemas de redes y de información y el entorno físico de dichos sistemas frente a incidentes y consistirán en”.

76. De la diputada señorita Maite Orsini y del diputado señor Jaime Araya:

Para agregar en la letra a) del artículo 6°, la palabra "riesgos" a continuación de la palabra "aquellos".

77.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

i. En el literal b) del inciso primero del artículo 6° suprímese la frase: “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.”

ii.Reemplázase el literal c) por el siguiente: “c) Elaborar e implementar planes de continuidad operacional y ciberseguridad, debiendo ser acreditados ante la Agencia cuando corresponda.”

78.- Del diputado señor Jorge Alessandri y la diputada señora Gloria Naveillan:

Para reemplazar el literal c) del artículo 6°, por el siguiente: “c) Elaborar e implementar planes de continuidad operacional y ciberseguridad, certificados por un centro o entidades de certificación nacional o internacional. Para estos efectos la Agencia, en conjunto con las Autoridades Sectoriales de los sectores regulados, deberán establecer el procedimiento y los requisitos para la implementación de un registro público de centros o entidades certificadoras. Dichos planes deberán ser actualizados y certificados anualmente.

79.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

“Suprímese el literal f) del artículo 6°”.

80.- Del diputado señor Jorge Alessandri y la diputada señora Gloria Naveillan:

Para reemplazar el literal f) del artículo 6° por el siguiente: “f) Contar con las certificaciones nacionales o internacionales de los sistemas de gestión y procesos”.

81.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Sustitúyase el literal g) del artículo 6° por el siguiente: “g) Informar sin demora a los destinatarios de sus servicios de las medidas o soluciones que pueden aplicar para reducir el riesgo resultante de un incidente de efecto negativo, en los términos artículo 23º de esta ley. En su caso, y en particular cuando sea probable que se materialice un incidente de efecto significativo, también debe informarse a los destinatarios de sus servicios del propio incidente de efecto significativo. La exigencia de informar de tales amenazas a los destinatarios debe cumplirse en la medida de lo posible, pero no exime a las entidades de la obligación de tomar a sus expensas medidas inmediatas y adecuadas para prevenir o subsanar cualquier incidente de efecto significativo y restablecer el nivel normal de seguridad del servicio. La mencionada información sobre los incidentes de efectos significativos a los destinatarios del servicio debe facilitarse de forma gratuita y la información debe estar redactada en un lenguaje fácil de comprender.”

82.-Del diputado don Cristián Araya:

Al artículo sexto, letra g, del proyecto de ley: Para reemplazar la expresión “la comunidad” por una expresión del siguiente tenor: “los usuarios afectados de los servicios esenciales**”.**

83.- Del diputado señor Jorge Alessandri y la diputada señora Gloria Naveillan:

“Para reemplazar el literal i) del artículo 6°, por el siguiente texto: “Designar un representante de ciberseguridad, quien será la contraparte de la Agencia y de las Autoridades Sectoriales”.”

Para agregar en el último inciso de la letra a) del artículo 6 y a continuación de la palabra reglamento, la frase “que deberá ser sometido a trámite de toma de razón de la Contraloría General de la República.”

“Para eliminar completamente el texto final del artículo 6.”

84.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

“Suprímese el inciso final del artículo 6°.”

85.- De la diputada señorita Maite Orsini y del diputado señor Jaime Araya:

Para agregar una nueva letra j) al artículo 6°, del siguiente tenor: j) En el caso de las instituciones privadas que sean calificadas como operadores de importancia vital, y que estén organizadas como sociedades anónimas, al menos un miembro de su directorio, deberá contar con experiencia o conocimientos en materia de ciberseguridad.

86.- Del diputado señor Andrés Jouannet:

Reemplácese en el inciso primero del artículo 6° propuesto la expresión “instituciones privadas” por “instituciones públicas y privadas”.

87.- Del Ejecutivo:

Para reemplazar en el artículo 7°, los incisos primero y segundo por los siguientes: “Todos los organismos de la Administración del Estado, así como los operadores de servicios esenciales y los operadores de importancia vital, así como las demás instituciones privadas que determine la Agencia, tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos en los términos del artículo 23, tan pronto hayan tenido constancia del incidente, sin demora indebida y conforme el siguiente esquema:

a) Dentro del plazo máximo de 12 horas, deberá enviarse una alerta temprana sobre la ocurrencia del evento, junto a una breve caracterización técnica de él;

b) Dentro del plazo máximo de 72 horas, una actualización de la información contemplada en la letra a), que incluya una evaluación inicial del incidente, su gravedad e impacto, así como indicadores de compromiso, si estuvieran disponibles;

c) A requerimiento del CSIRT Nacional o, en su caso, del CSIRT sectorial existente, un informe intermedio con las actualizaciones pertinentes sobre la situación;

d) A más tardar dentro del plazo máximo de quince días corridos, un informe que contenga, al menos:

i) una descripción detallada del incidente, incluyendo su gravedad e impacto;

ii) el tipo de amenaza o causa principal que probablemente haya causado el incidente;

iii) las medidas de mitigación aplicadas y en curso;

iv) si procede, las repercusiones transfronterizas del incidente;

e) En el caso de que el incidente siga en curso con posterioridad a la presentación del informe contemplado en el literal d), la institución afectada deberá presentar un informe final dentro del plazo de un mes contados desde el primer día que comenzó la gestión del incidente.

Sin perjuicio de lo anterior, los operadores de importancia vital que vean afectada la prestación de sus servicios esenciales a causa de un incidente, deberán notificarlo al CSIRT Nacional tan pronto les sea posible y, en cualquier caso, deberán entregar la información señalada en las letras a y b anteriores, en un plazo máximo de tres horas desde que haya tenido constancia del incidente.”.

88. Del Ejecutivo

Para agregar en el artículo 7°, un inciso final, nuevo, del siguiente tenor: “El esquema anterior no será aplicable a las instituciones financieras y demás entidades fiscalizadas por la Comisión para el Mercado Financiero, siempre y cuando la normativa sectorial fuere más exigente que la presente ley, o en aquellas materias no reguladas por la misma.”

89.- Del diputado señor Jorge Alessandri y la diputada señora Gloria Naveillan:

Para reemplazar el inciso primero del artículo 7° por el siguiente: “Deber de reportar. Todas las instituciones, sean públicas o privadas, definidos como operadores de servicios esenciales, 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.”

90.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

i. Sustitúyese el inciso primero por el siguiente: “Artículo 7. Deber de reportar. Será obligación de la Administración del Estado y de los agentes privados calificados como servicios esenciales y operadores de importancia vital 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, y de la posibilidad de que agentes privados no sujetos a las disposiciones de esta ley puedan, de manera voluntaria, reportar al CSIRT nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos, en cuyo caso se estarán a la forma dispuesta en este artículo.”

ii.Sustitúyese el inciso segundo por el siguiente:

“El deber de reportar comprende:

a) La emisión de una alerta temprana dentro de las primeras veinticuatro horas desde que se haya tenido constancia del incidente significativo en la que se indicará, cuando proceda, si cabe sospechar que el incidente significativo responde a una acción ilícita o malintencionada;

b) Dentro de las 72 horas desde que se haya tenido constancia del incidente significativo, la actualización de la alerta temprana, exponiéndose una evaluación inicial del incidente significativo, incluyendo su gravedad e impacto, así como indicadores de compromiso, cuando estén disponibles;

c) Un informe final, a más tardar un mes después de presentar la notificación del incidente contemplada en la letra b), en el que se recojan los siguientes elementos:

i) Una descripción detallada del incidente, incluyendo su gravedad e impacto;

ii) El tipo de amenaza o causa principal que probablemente haya desencadenado el incidente; y

iii) Las medidas paliativas aplicadas y en curso.

d) Si el incidente siguiera en curso al momento de la presentación del informe final contemplado en la letra c) precedente, éste se reemplazará por un informe de situación en ese momento y un informe final, que se presentará en el plazo de un mes a partir de que se haya gestionado el incidente.

Tanto el CSIRT respectivo como la autoridad sectorial competente podrán requerir informes intermedios con las actualizaciones pertinentes sobre la situación."

91. Del diputado señor Jorge Alessandri y la diputada señora Gloria Naveillan:

Para reemplazar el inciso segundo del artículo 7° por el siguiente: "La obligación de reportar, como primera alerta, deberá cumplirse en un plazo inferior a tres horas contadas desde que se tuvo conocimiento del evento respectivo. La entidad informante deberá entregar en un plazo no superior a 48 horas información complementaria respecto al incidente referido. 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."

92. Del diputado señor Jorge Alessandri y la diputada señora Gloria Naveillan:

Para eliminar en el inciso tercero del artículo 7° las palabras "sean" y "o no".

93. Del diputado señor Jorge Alessandri y la diputada señora Gloria Naveillan:

Para insertar en el inciso cuarto del artículo 6, después de los jefes de servicio, la frase "En el caso de las Instituciones del Estado"

94.- Del diputado señor Jorge Alessandri y Naveillan:

Para reemplazar el inciso final del artículo 7° por el siguiente texto: "La Agencia en conjunto con las Autoridades Sectoriales dictarán las instrucciones que sean necesarias para la debida realización y recepción de los reportes a que se refiere el presente artículo, procurando simplificar y no duplicar el reporte de información en los casos de empresas reguladas".

95. Del diputado señor Andrés Jouannet:

Reemplácese en el inciso primero del artículo 7 propuesto la expresión "Todas las instituciones, sean públicas o privadas, e independiente de si son o no operadores de servicios esenciales" por "Todas las instituciones públicas y privadas calificadas como operadores de importancia vital".

96.- Del diputado señor Andrés Jouannet:

Reemplácese en el inciso tercero la expresión ", todos los operadores de servicios esenciales, sean de importancia vital o no," por ", todos los operadores de importancia vital".

97. Del diputado señor Andrés Jouannet:

Reemplácese el inciso cuarto del artículo 7° propuesto por uno del siguiente tenor: "Los organismos de la Administración del Estado, las instituciones públicas y privadas calificadas como operadores de importancia vital, y, cuando proceda, sus proveedores, podrán intercambiar entre sí de forma voluntaria información relevante sobre ciberseguridad, incluyendo la ocurrencia de incidentes de ciberseguridad y vulnerabilidades, siempre que dicho intercambio de información se haga con el objetivo de prevenir, detectar o responder a incidentes, recuperarse de ellos o reducir su repercusión; o refuerce el nivel de

ciberseguridad de los organismos de la administración del Estado y operadores de importancia vital. Dicho intercambio se pondrá en práctica a través de mecanismos de intercambio de información sobre ciberseguridad que respeten la posible naturaleza delicada de la información compartida".

98.- Del diputado señor Andrés Jouannet:

Incorpórese el siguiente inciso final al artículo 7° propuesto: "No obstante el deber de reportar los ciberataques e incidentes de ciberseguridad al CSIRT Nacional establecido en este artículo, adicionalmente los operadores de importancia vital deberán cooperar eficazmente con el Ministerio Público poniendo a su disposición datos o informaciones precisas, verídicas y comprobables y denunciar, cuando corresponda, en el caso de que el incidente de ciberseguridad que pueda tener efectos significativos corresponda a la comisión de alguno de los delitos establecidos en 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".

99.- Del diputado señor Jorge Alessandri y la diputada señora Gloria Naveillan:

Para insertar en el inciso segundo del artículo 8°, después de la palabra ciberseguridad, la siguiente frase; "en coordinación con las autoridades sectoriales de las industrias reguladas"

100.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Introdúcense las siguientes modificaciones al inciso segundo del artículo 8º:

a) Suprímese la frase "de los organismos de la Administración del Estado";

b) Intercálese, entre las palabras "privadas" y "en materia de seguridad", la frase "calificadas como operadores de importancia vital"; y

c) Sustitúyese la frase "incluida la facultad de impartir instrucciones generales y particulares" por "dentro del ámbito de su competencia y de conformidad a lo dispuesto en el artículo 3".

101- Del diputado señor Andrés Jouannet:

Incorpórese en el inciso segundo del artículo 8° propuesto, luego de "instituciones privadas", la expresión "y públicas calificadas como operadores de importancia vital".

102- Del Ejecutivo:

Para reemplazar el literal g) del artículo 9°, por el siguiente: "g) Determinar y calificar los servicios esenciales, en la forma prevista en el título IX de esta ley; y determinar a los operadores de importancia vital, en la forma prevista en el artículo 4° de la presente ley.".

103.- Del Ejecutivo:

Para modificar el literal j) del artículo 9°, en el siguiente sentido:

a. Elimínase, en el literal j), la frase ", así como los consagrados por la ley N°19.628, sobre protección de la vida privada".

b. Agrégase, a continuación del punto final, la frase: "Cuando la información a la que tenga acceso la Agencia incluya datos personales estos deberán ser anonimizados siempre que ello sea posible y no entorpezca el ejercicio de las funciones de la Agencia. En cualquier caso, los datos personales sólo podrán ser tratados dando estricto cumplimiento a lo dispuesto en la ley 19.628.".

104.- Del Ejecutivo

Para reemplazar el literal k) del artículo 9°, por el siguiente:

“k) Cooperar con organismos públicos e instituciones privadas, 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 autoridades nacionales de ciberseguridad extranjeras o sus equivalentes y con los organismos internacionales con competencia en materia de ciberseguridad.

Cuando se trate de la cooperación con Estados y organizaciones internacionales, dicha actividad deberá realizarse en coordinación con el Ministerio de Relaciones Exteriores, en conformidad a lo previsto en el inciso primero del artículo 2 de la ley N°21.080.”.

105.- Del Ejecutivo:

Para reemplazar el segundo párrafo del literal n) del artículo 9°, por el siguiente:

“Para el cumplimiento de su función fiscalizadora, la Agencia podrá examinar sin restricción alguna y por los medios que estime pertinentes todas las actividades, archivos y documentos de las entidades o actividades fiscalizadas o de sus matrices, filiales o coligadas, y requerir de ellas o de sus administradores, asesores o personal, los antecedentes y explicaciones que juzgue necesarios para obtener información acerca de cualquier punto que convenga esclarecer para efectos de determinar el cumplimiento de la normativa aplicable por parte de la entidad fiscalizada. Asimismo, la Agencia podrá realizar inspecciones; auditorías; análisis de seguridad o evaluar un sistema de gestión de seguridad de la información; requerir el acceso a sistemas; citar a declarar a cualquier persona que, a cualquier título, preste o haya prestado servicios para las entidades fiscalizadas y a toda otra persona que hubiere ejecutado y celebrado con ellas actos y convenciones de cualquier naturaleza; establecer la forma, plazos y procedimientos para que las entidades fiscalizadas cumplan la obligación de presentar los antecedentes y explicaciones referidos precedentemente; y, en general, requerir la adopción de todas las medidas preventivas o correctivas que se estimen necesarias y sean pertinentes, proporcionales y adecuadas para evitar o resolver incidentes de ciberseguridad. La Agencia también podrá solicitar información de otros organismos públicos, la que en caso de ser secreta o reservada.”.

106.- Del Ejecutivo:

Para intercalar, en el literal r), entre la expresión “para estos efectos” y la coma que le sigue, la frase “las instituciones que no siendo operadores de servicios esenciales estarán obligadas a reportar incidentes de conformidad con lo dispuesto en el artículo 7, así como”.

107.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Introdúcense las siguientes modificaciones al literal b) del artículo 9°:

i. Intercálase entre la expresión “instituciones públicas y privadas” y la coma que le sigue, la expresión “calificadas como operadores de importancia vital”;

ii. Intercálase entre la palabra “ciberseguridad” y el punto aparte, un coma seguido de lo siguiente: “dentro del ámbito de su competencia”.

108.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Intercálase en el literal d) del artículo 9°, entre las frases “instituciones privadas” y “y al CSIRT Nacional”, lo siguiente “calificadas como operadores de importancia vital”;

109.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

En el literal h) del artículo 9°, suprímase la frase “y que se encuentre en posesión de estas instituciones”;

110.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Introdúcense las siguientes modificaciones al literal j) del artículo 9°:

i. Intercálase entre las frases “instituciones privadas” y “cualquier documento” la expresión “calificadas como operadores de importancia vital”;

ii. Suprímase la frase “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, sobre protección de la vida privada”;

iii. Incorpórese el siguiente párrafo segundo, nuevo: “Los requerimientos realizados por la Agencia deberán ser fundados y expresar el objeto de la solicitud y detallar claramente los documentos, antecedentes o información solicitada, según corresponda. Queda prohibido a la Agencia formular solicitudes genéricas.”

111.- Del diputado señor Jorge Alessandri y la diputada señora Gloria Naveillan:

Para agregar al final de la letra j) del artículo 9, lo siguiente, a continuación de N°19.628; “y a lo que define la presente ley y sus reglamentos”.

112.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Introdúcense las siguientes modificaciones al literal m) del artículo 9°:

i. Suprímase la expresión “coordinar”;

ii. Suprímase la expresión “interagencialmente”.

113.- Del diputado señor Jorge Alessandri:

Para sustituir el artículo 9° literal n) inciso segundo del proyecto de ley, por el siguiente: “Para el cumplimiento de su función fiscalizadora, la Agencia podrá realizar inspecciones; auditorías; análisis de seguridad o evaluar un sistema de gestión de seguridad de la información; requerir el acceso a sistemas; citar a declarar a cualquier persona que, a cualquier título, preste o haya prestado servicios para las entidades fiscalizadas y a toda otra persona que hubiere ejecutado y celebrado con ellas actos y convenciones de cualquier naturaleza; establecer la forma, plazos y procedimientos para que las entidades fiscalizadas cumplan la obligación de presentar los antecedentes y explicaciones referidos precedentemente, además de las facultades que esta ley le encomiende con el objeto evitar o resolver incidentes de ciberseguridad”.

114.- Del diputado señor Jorge Alessandri y la diputada señora Gloria Naveillan:

Para insertar en la letra o) inciso 2 del artículo 9°, a continuación de las palabras “función fiscalizadora” lo siguiente: “de acuerdo a lo que define la presente ley y sus reglamentos”

115.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Introdúcense las siguientes modificaciones al párrafo segundo del literal n) del artículo 9°:

i. Sustitúyese la expresión “todas las facultades que fueren necesarias” por “las facultades que le señale la ley”;

ii. Sustitúyese el siguiente la coma que sigue a la palabra “fiscalizadora” por un punto seguido y el texto “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” por el que se indica a continuación: “Para el cumplimiento de su función podrá:

1. Llevar a cabo inspecciones, incluyendo las realizadas por vía remota.

2. Realizar o establecer auditorías de seguridad periódicas o específicas, por medio de sus empleados. Tras la evaluación de la información o del resultado de cualquier auditoría de seguridad la Agencia podrá dictar instrucciones particulares a la entidad auditada para subsanar las deficiencias detectadas.

3. Realizar análisis de seguridad basados en criterios de evaluación de riesgos objetivos, no discriminatorios, justos y transparentes, con la cooperación de la entidad en cuestión cuando fuere necesario.

4. Solicitar pruebas de la implementación de los planes de continuidad operacional y ciberseguridad, referidos en la letra c) del artículo 6°.

5. 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, incluyendo especialmente el conocimiento de la información necesaria para prevenir, identificar, eliminar o contrarrestar un incidente de ciberseguridad.

No estarán obligadas a concurrir a declarar las personas indicadas en el artículo 361 del Código de Procedimiento Civil, a las cuales la Agencia, para los fines expresados en el párrafo precedente, deberá pedir declaración por escrito.

6. Adoptar o solicitar la adopción de las medidas tendientes a corregir las deficiencias que observare, en general, en el ejercicio de sus atribuciones de fiscalización.

7. Requerir a las entidades fiscalizadas que proporcionen al público, por las vías que señale, información veraz, suficiente y oportuna sobre determinados aspectos del incumplimiento de la presente ley de una manera específica.”

116.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Intercálase en el literal ñ) del artículo 9°, entre las palabras “privadas” y “respecto”, la frase “calificadas como operadores de importancia vital”.

117.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Intercálase en el literal p) del artículo 9°, entre la palabra “funciones” y el punto aparte, lo siguiente: “dentro del ámbito de sus competencias.”

118.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

“Suprímase el literal t) del artículo 9°.”

119.- Del diputado Andrés Jouannet:

Incorpórese en el literal b) del inciso primero del artículo 9° propuesto, luego de “instituciones públicas y privadas”, la expresión “calificadas como operadores de importancia vital, así como la normativa que regula las relaciones entre estos y sus proveedores”.

120.- Del diputado señor Andrés Jouannet:

Incorpórese en el literal d) del inciso primero del artículo 9° propuesto, luego de “instituciones privadas”, la expresión “y públicas calificadas como operadores de importancia vital”.

121.- Del diputado señor Andrés Jouannet:

Incorpórese en el literal j) del inciso primero del artículo 9° propuesto, luego de “instituciones privadas”, la siguiente expresión “y públicas calificadas como operadores de importancia vital”.

122.- Del diputado señor Andrés Jouannet:

Incorpórese en el literal j) del inciso primero del artículo 9°, luego del punto final, que pasa a ser punto y aparte, lo siguiente:

“Los requerimientos realizados por la Agencia deberán expresar el objeto de la solicitud, estar debidamente fundamentados, detallar los documentos, antecedentes o información solicitados y establecer un plazo razonable para su entrega, según corresponda, para efectos de determinar el cumplimiento de la normativa aplicable por parte del operador de importancia vital, y siempre y cuando no se altere el normal desenvolvimiento de sus actividades.

El requerimiento de acceso a redes o sistemas informáticos, así como la restricción de su acceso o uso, podrá efectuarse previa resolución fundada dictada por la Agencia, cuando resulte indispensable para fiscalizar el cumplimiento de la normativa aplicable al operador de importancia vital o contrarrestar ciberataques o incidentes de ciberseguridad, según corresponda. Se entenderá que el requerimiento es indispensable cuando se cumpla con los siguientes requisitos:

1. Un incidente de ciberseguridad comprometa o dañe otra red o sistema informático.

2. El operador de importancia vital esté imposibilitado de contrarrestar las amenazas originadas por el incidente de ciberseguridad.

3. No es posible utilizar una medida menos gravosa que permita contrarrestar el incidente de ciberseguridad.

4. El acceso a la red o sistemas informáticos, así como la restricción de su acceso o uso, según corresponda, no cause un daño desproporcional a terceros o al titular de la red o sistema informático”.

123.- Del diputado señor Andrés Jouannet:

Reemplácese el párrafo segundo del literal n) del inciso primero del artículo 9° propuesto por el siguiente: “La Agencia contará con las facultades necesarias para el cumplimiento de su función fiscalizadora, comprendiendo:

1. Llevar a cabo inspecciones, incluyendo las realizadas por vía remota, por medio de sus empleados o centros de certificación acreditados.

En las inspecciones que la Agencia realice en el marco de la fiscalización, podrá integrar su propio personal con el de la entidad fiscalizada.

2. Realizar o establecer auditorías de seguridad periódicas o específicas, por medio de sus empleados o centros de certificación acreditados.

Los resultados de cualquier auditoría de seguridad específica se pondrán a disposición de la Agencia. Los costos de dicha auditoría de seguridad específica realizada

por un centro de certificación acreditado serán costeados por la entidad auditada, salvo en aquellos casos debidamente fundamentados en los que la Agencia establezca lo contrario.

Tras la evaluación de la información o del resultado de cualquier auditoría de seguridad la Agencia podrá dictar instrucciones particulares a la entidad auditada para subsanar las deficiencias detectadas.

3. Realizar auditorías específicas, por medio de sus empleados, que estén justificadas por la ocurrencia de un incidente de ciberseguridad que pueda tener efectos significativos, de conformidad con el artículo 23, o una infracción a las disposiciones de la presente ley.

4. Realizar análisis de seguridad basados en criterios de evaluación de riesgos objetivos, no discriminatorios, justos y transparentes, con la cooperación de la entidad en cuestión cuando fuere necesario.

5. Solicitar pruebas de la implementación de los planes de continuidad operacional y ciberseguridad, referidos en la letra c) del artículo 6°.

6. 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, incluyendo especialmente el conocimiento de la información necesaria para prevenir, identificar, eliminar o contrarrestar un incidente de ciberseguridad.

No estarán obligadas a concurrir a declarar las personas indicadas en el artículo 361 del Código de Procedimiento Civil, a las cuales la Agencia, para los fines expresados en el párrafo precedente, deberá pedir declaración por escrito.

7. Designar empresas de auditoría externa o centros de certificación acreditados en las entidades fiscalizadas, para que realicen las tareas que específicamente les encomiende, con las facultades que estime necesarias, comprendiendo la supervisión, durante un período determinado, del cumplimiento por parte de las entidades fiscalizadas de las obligaciones previstas en los artículos 5° y 6° de la presente ley.

Para estos efectos, las empresas de auditoría externa o centros de certificación acreditados designados por la Agencia deberán observar de manera estricta el deber de reserva que esta ley impone, así como los consagrados por la ley N°19.628, sobre protección de la vida privada, y serán remunerados por la entidad fiscalizada. La remuneración gozará del privilegio establecido en el Nº4 del artículo 2472 del Código Civil.

8. Contratar o hacer contratar por las entidades fiscalizadas los servicios de peritos o técnicos para los trabajos que les encomiende, los que serán de cargo de dichas personas o entidades fiscalizadas.

9. Adoptar o solicitar la adopción de las medidas tendientes a corregir las deficiencias que observare, en general, en el ejercicio de sus atribuciones de fiscalización.

10. Solicitar a los centros de certificación acreditados que suspendan temporalmente una certificación referente a una parte o la totalidad de los servicios o actividades de que se trate prestados por la entidad fiscalizada, cuando esta no adopte las medidas referidas en el párrafo tercero del número 2 o el número 10 anterior.

11. Requerir a las entidades fiscalizadas que proporcionen al público, por las vías que señale, información veraz, suficiente y oportuna sobre determinados aspectos del incumplimiento de la presente ley de una manera específica. La Agencia podrá efectuar directamente las publicaciones que fueren necesarias para los fines precisados en este numeral, con cargo a las entidades fiscalizadas".

124.- Del diputado señor Andrés Jouannet:

Incorpórese en el literal ñ) del inciso primero del artículo 9° propuesto, luego de "instituciones públicas y privadas", la siguiente expresión "calificadas como operadores de importancia vital".

125.- Del diputado señor Andrés Jouannet:

Incorpórese los siguientes literales antepenúltimo y penúltimo al inciso primero del artículo 9° propuesto, del siguiente tenor:

“x) Formular las denuncias que correspondieren al Ministerio Público por los hechos de que tomare conocimiento en el ejercicio de sus atribuciones y que pudieren revestir caracteres de delito, sin perjuicio de los deberes generales que sobre la materia determine la ley.

y) Evacuar los informes que le requieran los fiscales del Ministerio Público que estén dirigiendo investigaciones criminales, siempre que correspondan a materias de su competencia y se refieran a información que esté disponible en sus archivos”.

126.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

“Suprímase el artículo 24.”

127.- Del diputado señor Andrés Jouannet:

Incorpórense el siguiente inciso tercero en el artículo 24° propuesto, pasando el actual inciso tercero a ser cuarto y así sucesivamente, del siguiente tenor: “Asimismo, los centros de certificación acreditados serán los únicos habilitados para homologar otros esquemas de certificación o certificaciones internacionalmente reconocidas, acreditando que cumplen con los estándares y normas de seguridad establecidos por esta ley y su normativa complementaria. Los centros de certificación acreditados deberán certificar automáticamente los esquemas de certificación o certificaciones internacionalmente reconocidas que se encuentren homologadas y adoptadas por los entes que soliciten la certificación”.

128.- Del diputado señor Andrés Jouannet:

Reemplácese en el inciso cuarto del artículo 24°, que ha pasado a ser quinto, la expresión “deberán” por “podrán”.

129.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Intercálase en el inciso primero del artículo 33, entre las palabras “privadas” y “serán” lo siguiente “señaladas en los artículos 5 y 6”.

130.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Sustitúyanse los literales a), b) y c) del inciso primero del artículo 33, por los siguientes:

“a) Las infracciones leves serán sancionadas con amonestación escrita o multa de hasta 5.000 unidades tributarias mensuales.

b) Las infracciones graves serán sancionadas con multa de hasta 10.000 unidades tributarias mensuales.

c) Las infracciones gravísimas serán sancionadas con multa de hasta 20.000 unidades tributarias mensuales.”

131.- Del diputado señor Jorge Alessandri:

Para sustituir el inciso primero del literal c) del artículo 33, por el siguiente: “c) Las infracciones gravísimas serán sancionadas con multa de 5.001 a 10.000 unidades tributarias mensuales. En caso de que el infractor sea un operador de importancia vital, la multa podrá ser de hasta 20.000 unidades tributarias mensuales.”.

132.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Sustitúyese el inciso segundo del artículo 33, por el siguiente:

“Se considerarán infracciones leves las siguientes:

a) Incumplir total o parcialmente los deberes generales de ciberseguridad establecido en el artículo 5 en los casos que no esté sancionado como infracción grave o gravísima;
b) Incumplir las instrucciones generales o particulares impartidas por la agencia en los casos que no esté sancionado como infracción grave o gravísima;
c) No haber actualizado los planes de continuidad operacional y ciberseguridad, previa instrucción particular en general de la agencia;
d) No haber designado un delegado de ciberseguridad;
e) No contar con programas de capacitación, formación y educación de sus trabajadores;
f) Cometer cualquier otra infracción a las obligaciones y principios establecidos en esta ley que no sea calificada como una infracción grave o gravísima."

133.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

"Sustitúyese el inciso tercero del artículo 33, por el siguiente:
"Se considerarán infracciones graves la siguientes:
a) Entregar fuera de plazo a 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, en los casos que no esté sancionado como infracción gravísima;
c) Incumplir con el deber de garantizar un nivel de seguridad a los sistemas de redes y de información adecuado en relación con los riesgos planteados, establecido en el artículo 6;
d) Incumplir injustificadamente con el deber de informar sin demora a los destinatarios de sus servicios de las medidas o soluciones que pueden aplicar para reducir el riesgo resultante de un incidente de efecto significativo, establecido en el literal g) del artículo 6;
e) No haber adoptado de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad coma según lo establecido en el artículo 6;
f) Negar injustificadamente la ejecución o implementación de alguna de las facultades de la agencia establecidas en el literal n) del artículo noveno.
g) La reincidencia en una infracción leve dentro del periodo de un año."

134.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Sustitúyese el inciso cuarto del artículo 33, por el siguiente:

"Se considerarán infracciones gravísimas las siguientes:
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 injustificada o maliciosamente el deber de reportar establecido en el artículo 7;
d) Incumplir con las obligaciones prescritas en los literales a), c) y d) del artículo 6;
e) La reincidencia en una infracción grave dentro del periodo de dos años."

135.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Para sustituir el inciso quinto del artículo 33, por el siguiente: "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, el grado de exposición del infractor a los riesgos, la gravedad de los efectos de los ataques incluidas sus repercusiones sociales o económicas, la reiteración en la infracción

dentro del plazo de 3 años contado desde el momento en que se produjo el incidente, el tamaño y la capacidad económica del infractor.”

136.- Del diputado señor Jorge Alessandri:

Para suprimir**,** en el inciso séptimo del artículo 33, la frase: “y fundamentos jurídicos”.

137.- Del diputado señor Jorge Alessandri:

En el artículo 33 inciso octavo del proyecto de ley, para sustituir la frase “a los tres años de cometidas” por la siguiente: “en el plazo de tres años desde que hubieren sido cometidas”.

138.- Del diputado señor Andrés Jouannet:

Reemplácese el inciso primero del artículo 33° propuesto por el siguiente: “Artículo 33. De las infracciones. Las sanciones a las infracciones de la presente ley cometidas por instituciones públicas y privadas calificadas como operadores de importancia vital serán las siguientes:”

139.- Del diputado señor Andrés Jouannet:

Reemplácese el literal a) del inciso primero del artículo 33° por el siguiente: “a) Las infracciones leves serán sancionadas con amonestación escrita o multa de hasta 5.000 unidades tributarias mensuales”

140.- Del diputado señor Andrés Jouannet:

Reemplácese el literal b) del inciso primero del artículo 33° por el siguiente: “b) Las infracciones graves serán sancionadas con multa de hasta 10.000 unidades tributarias mensuales”.

141.- Del diputado señor Andrés Jouannet:

Reemplácese el literal c) del inciso primero del artículo 33° por el siguiente: “c) Las infracciones gravísimas serán sancionadas con multa de hasta 20.000 unidades tributarias mensuales”.

142.- Del diputado señor Andrés Jouannet:

Reemplácese el inciso segundo del artículo 33° por el siguiente:

“Se consideran infracciones leves las siguientes:

a) Incumplir las instrucciones generales o particulares impartidas por la Agencia en los casos que no esté sancionado como infracción grave o gravísima.

b) Incumplir total o parcialmente con los protocolos y estándares diferenciados establecidos por la Agencia en virtud del artículo 5°.

c) No haber designado un delegado de ciberseguridad en conformidad con el literal i) del artículo 6°.

d) No contar con programas de capacitación, formación y educación de sus trabajadores, en conformidad con el literal h) del artículo 6°.

e) No contar con las certificaciones requeridas por la ley o el Reglamento, de conformidad con los literales c) y f) del artículo 6°.

f) Cometer cualquier otra infracción a las obligaciones y principios establecidos en esta ley, que no sea calificada como una infracción grave o gravísima”.

143.- Del diputado señor Andrés Jouannet:

Reemplácese el inciso tercero del artículo 33° por el siguiente:

“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°, en los casos que no esté sancionado como infracción gravísima.

c) Incumplir con el deber general de no realizar pagos de cualquier tipo por rescate ante ataques de secuestro digital o ransomware, establecido en el artículo 5°.

d) Incumplir injustificadamente con el deber de informar a la comunidad sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente sus redes y sistemas informáticos, de conformidad con el literal g) del artículo 6°.

e) No haber adoptado de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad, en conformidad con lo establecido en el literal e) del artículo 6°.

f) No mantener un registro de las acciones ejecutadas que compongan el sistema de seguridad de la información, de conformidad al literal b) del artículo 6°.

g) Incumplir con el deber de elaborar e implementar planes de continuidad operacional y ciberseguridad, según lo señalado por el literal c) del artículo 6°.

h) La reiteración de una misma infracción calificada como leve de acuerdo con este artículo”.

144.- Del diputado señor Andrés Jouannet:

Reemplácese el inciso tercero del artículo 33° por el siguiente:

“Las siguientes infracciones se consideran gravísimas:

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 injustificada o maliciosamente con el deber de reportar establecido en el artículo 7°.

d) Incumplir injustificadamente con los deberes establecidos en los literales a) y d) del artículo 6°.

e) La reiteración de infracciones calificadas como graves de acuerdo con este artículo”.

145.- Del diputado señor Andrés Jouannet:

Intercálese en el inciso cuarto (quinto?) del artículo 33°, luego de “la gravedad de los efectos de los ataques” la expresión “incluidas sus repercusiones sociales o económicas, la gravedad de la infracción, el grado de exposición del infractor a los riesgos, el tamaño del infractor, el beneficio económico obtenido con motivo de la infracción en caso que lo hubiese, la intencionalidad en la comisión de la infracción y el grado de participación en el hecho, acción u omisión constitutiva de la misma, las sanciones aplicadas con anterioridad por la Agencia en las mismas circunstancias, el porcentaje de usuarios afectados por la infracción”.

146.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Intercálase en el literal b del inciso primero del artículo 34, entre la expresión “a petición de parte” y la coma que le sigue, la palabra “afectada”.

147.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Intercálase en el literal b del inciso primero del artículo 34, entre la expresión “a petición de parte” y la coma que le sigue, la palabra “afectada”.

148.- Del Ejecutivo.

Para reemplazar el literal b) del actual artículo 34, que ha pasado a ser artículo 36, por el siguiente: “b) La Agencia podrá iniciar un procedimiento sancionatorio, de oficio o a petición de parte, o como resultado de un proceso de fiscalización. Sin perjuicio de lo anterior, deberá abstenerse cuando exista un procedimiento administrativo en curso, o dejar de conocer si se iniciare un procedimiento administrativo por la autoridad sectorial correspondiente dentro de los plazos legales, respecto de los mismos hechos y fundamentos jurídicos, en ejercicio de las atribuciones que correspondan a una autoridad sectorial de conformidad con lo establecido en el artículo 24.

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. Transcurridos tres meses desde recibida dicha comunicación sin que la autoridad sectorial hubiere iniciado un procedimiento sancionatorio, la Agencia podrá iniciarlo, informando a la autoridad sectorial que deberá abstenerse de hacerlo.

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. 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.”.

149.- Del Ejecutivo:

Para intercalar, a continuación del Título VIII, el siguiente título IX, nuevo, readecuándose el orden correlativo de los títulos y artículos siguientes:

“Título IX
De los servicios esenciales.
Artículo 44. Servicios esenciales**.** Para todos los efectos de la presente ley, se considerarán como servicios esenciales para el mantenimiento de actividades sociales o económicas cruciales, que dependen de las redes y sistemas informáticos, a los siguientes:
1. Los servicios de telecomunicaciones.
2. Los servicios de infraestructura digital, incluyendo los servicios de intercambio de tráfico de internet; servicios de computación en la nube; servicios de alojamiento o procesamiento de datos; servicios de redes de distribución de contenidos; servicios de registro de nombres del dominio .CL; servicios de certificación acreditados a que se refiere la Ley N°19.799.
3. Los servicios de ciberseguridad;
4. Los servicios de generación, transmisión y distribución eléctrica.
5. Los servicios de producción, transporte, almacenamiento y distribución de combustibles.
6. Los servicios sanitarios y de suministro de agua potable.
7. Los servicios comerciales de transportes aéreos, ferroviarios y marítimos.
8. Los servicios portuarios.
9. Los servicios aeroportuarios.
10. Los servicios bancarios y financieros.
11. Los servicios de administración de fondos previsionales, de fondos de cesantía y los servicios de salud previsional.
12. Los servicios de prestaciones de salud.
La Agencia identificará, mediante resolución exenta dictada conforme el procedimiento dispuesto en el artículo 4° de esta ley, las infraestructuras, procesos o funciones específicas que serán calificadas como esenciales, y que quedarán sujetas a las obligaciones establecidas en el artículo 6° de esta ley.

Asimismo, conforme al mismo procedimiento, la Agencia podrá calificar como esenciales otros servicios distintos a los señalados precedentemente, para lo cual deberá considerar, entre otros factores, la entidad del impacto cuya afectación o interrupción podría tener en la defensa nacional o en el mantenimiento de actividades sociales y económicas

fundamentales; la dependencia del servicio de las redes y sistemas informáticos; la interconexión, interoperabilidad o interdependencia que tenga con otros servicios esenciales.”.

150.- Del Ejecutivo:

Para agregar, en el inciso tercero del artículo 44, que ha pasado a ser 45, a continuación de la expresión “conformación o participación” la expresión “, si así se acordare,”.

151.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Agrégase en el inciso primero del artículo 44, entre las expresiones “Televisión” y “adoptar”, la palabra “podrán”.

152.- Del diputado señor Andrés Jouannet:

Incorpórese un nuevo inciso primero al artículo primero transitorio, pasando el actual a ser segundo y así sucesivamente, del siguiente tenor: “La presente ley entrará en vigencia para los organismos de la Administración del Estado e instituciones públicas y privadas calificadas como operadores de importancia vital, así como para sus proveedores, el día primero del mes vigésimo segundo posterior a su publicación en el Diario Oficial”.

153.- Del Ejecutivo:
“Para suprimir el artículo octavo transitorio.”

154.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Para suprimir el artículo octavo transitorio.”

155.- De los diputados señores José Miguel Castro, Andrés Longton y Diego Schalper:

Para agregar un nuevo Artículo Octavo Transitorio, nuevo, del siguiente tenor: “Artículo octavo. Las disposiciones permanentes de la ley entrarán en vigencia un año después de la fecha en que, según las disposiciones del Artículo Primero Transitorio, la Agencia entre en funciones. Con todo, la implementación de los diversos CSIRT sectoriales que se señalan en la presente ley podrán comenzar a implementarse desde su publicación, sujetos a la disponibilidad presupuestaria de cada servicio.

VI. INDICACIONES DECLARADAS INADMISIBLES.

No hubo.

VII. MENCIÓN DE ADICIONES Y ENMIENDAS QUE LA COMISIÓN APROBÓ EN LA DISCUSIÓN PARTICULAR.

De conformidad a lo establecido en el N° 7° del artículo 304 del Reglamento de la Corporación, la Comisión deja constancia que introdujo las siguientes enmiendas el texto propuesto por el Senado:

Al Artículo 1°.

Lo ha sustituido por el siguiente:

“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 éstos 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 determinadas en el artículo 4°, y los mecanismos de control, supervisión y de responsabilidad ante infracciones.

Para efectos de esta ley, la Administración del Estado estará constituida por los Ministerios, las delegaciones presidenciales regionales y provinciales, los Gobiernos Regionales, las Municipalidades, las Fuerzas Armadas, de Orden y Seguridad Pública, las empresas públicas creadas por ley, y los órganos y servicios públicos creados para el cumplimiento de la función administrativa.

Las disposiciones de esta ley serán aplicables a las empresas del Estado y sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio.”

Al Artículo 2°.

Ha sustituido los numerales 5 al 27 por los siguientes:

“5. Ciberataque: “intento de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático.

6. 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.

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

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

9. 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.

10. 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 de los procesos ejecutados o implementados en las redes y sistemas informáticos.

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

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

13. 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.

14. 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.

15. Vulnerabilidad: debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.”

Al artículo 3º.

Lo ha sustituido por el siguiente:

“Artículo 3. Principios rectores. Para alcanzar los objetivos de esta ley se deberán observar los siguientes principios:

1. Principio de control de daños: frente a un ciberataque o a un incidente de ciberseguridad siempre se deberá actuar coordinada y diligentemente, adoptando las medidas necesarias para evitar la escalada del ciberataque o del incidente de ciberseguridad y su posible propagación a otros sistemas informáticos.

2. Principio de cooperación con la autoridad: para resolver los incidentes de ciberseguridad se deberá prestar la cooperación debida con la autoridad competente y, si es necesario, cooperar entre diversos sectores, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios.

3. Principio de coordinación: de conformidad a lo dispuesto por el inciso segundo del artículo 5º del DFL Nº1-19.653 que fija texto refundido, coordinado y sistematizado de la ley Nº18.575, orgánica constitucional de Bases Generales de la Administración del Estado, la Agencia y las autoridades sectoriales deberán cumplir sus cometidos coordinadamente y propender a la unidad de acción, evitando la duplicación o interferencia de funciones.

4. Principio de seguridad en el ciberespacio: es deber del Estado resguardar la seguridad en el ciberespacio. El Estado velará porque todas las personas puedan participar de un ciberespacio seguro otorgando especial protección a las redes y sistemas informáticos que contengan información de aquellos grupos de personas que suelen ser en mayor medida objeto de ciberataques.

5. 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.

6. Principio de seguridad informática: toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere necesarias, incluyendo el cifrado.

7. Principio de racionalidad: las medidas para la gestión de incidentes de ciberseguridad, las obligaciones de ciberseguridad y el ejercicio de las facultades de la Agencia deberán ser necesarias y proporcionales al grado de exposición a los riesgos, así como al impacto social y económico que tendría.

8. Principio de seguridad y privacidad por defecto y desde el diseño: Los sistemas informáticos, aplicaciones y tecnologías de la información deben diseñarse, implementarse y gestionarse teniendo en cuenta la seguridad y la privacidad de los datos personales que procesan.”

Al Artículo 4°.

Lo ha reemplazado por el siguiente:

“Artículo 4. Ámbito de aplicación. La presente ley se aplicará a las instituciones que presten servicios calificados como esenciales según lo establecido en los incisos segundo y tercero de este artículo y a aquellas que sean calificadas como operadores de importancia vital, de conformidad con lo dispuesto en los artículos 5 y 6 de esta ley.

Son servicios esenciales aquellos provistos por los organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional; los prestados bajo concesión de servicio público; y los proveídos por instituciones privadas que realicen las siguientes actividades: generación, transmisión o distribución eléctrica; transporte, almacenamiento o distribución de combustibles; suministro de agua potable o saneamiento; telecomunicaciones; infraestructura digital; servicios de tecnología de la información gestionados por terceros; transporte terrestre, aéreo, ferroviario o marítimo, así como la operación de su infraestructura respectiva; banca, servicios financieros y medios de pago; administración de prestaciones de seguridad social; servicios postales y de mensajería; prestación institucional de salud por entidades tales como hospitales, clínicas, consultorios y centros médicos; y la producción y/o investigación de productos farmacéuticos.

La Agencia podrá calificar otros servicios como esenciales mediante resolución fundada del o la Directora Nacional cuando su afectación puede causar un grave daño a la vida o integridad física de la población o a su abastecimiento, a sectores relevantes de las actividades económicas, al medioambiente, al normal funcionamiento de la sociedad, de la Administración del Estado, a la defensa nacional, o a la seguridad y el orden público.

Dicha calificación deberá someterse al proceso de consulta pública y se regirá por las disposiciones de la ley Nº19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.

La Agencia identificará, mediante resolución exenta dictada conforme el procedimiento dispuesto en este artículo, las infraestructuras, procesos o funciones específicas que serán calificadas como esenciales, y que quedarán sujetas a las obligaciones establecidas en el artículo 8° de esta ley.”

Artículos nuevos.

Ha intercalado los siguientes artículos 5º y 6º, nuevos, pasando los actuales artículos 5º y 6º a ser artículos 7º y 8º, y así sucesivamente.

“Artículo 5. Operadores de Importancia Vital. La Agencia establecerá mediante resolución dictada por el o la Directora Nacional, según se establece en el artículo siguiente, a los prestadores de servicios esenciales que sean calificados como operadores de importancia vital.

La Agencia podrá calificar como operadores de importancia vital a quienes reúnan los siguientes requisitos:

1.- que la provisión de dicho servicio dependa de las redes y sistemas informáticos; y,

2.- que la afectación, interceptación, interrupción o destrucción de sus servicios tenga un impacto significativo en la seguridad y el orden público; en la provisión continua y regular de servicios esenciales; en el efectivo cumplimiento de las funciones del Estado; o, en general, de los servicios que éste debe proveer o garantizar.

Además, la Agencia podrá calificar como operadores de importancia vital a instituciones privadas que, aunque no tengan la calidad de prestadores de servicios esenciales, reúnan los requisitos indicados en el inciso anterior y cuya calificación sea indispensable por haber adquirido un rol crítico en el abastecimiento de la población, la distribución de bienes o la producción de aquellos indispensables o estratégicos para el país; o por el grado de exposición de la entidad a los riesgos y la probabilidad de incidentes de ciberseguridad, incluyendo su gravedad y las consecuencias sociales y económicas asociadas.

En cualquier caso, siempre se deberá tener en consideración el tamaño de la institución privada, especialmente las características y necesidades de las micro, pequeñas y medianas empresas, tal como se definen en la ley N° 20.416."

"Artículo 6. Procedimiento de calificación de los operadores de importancia vital. Al menos cada tres años, la Agencia deberá revisar y actualizar la calificación de operadores de importancia vital mediante una resolución dictada por la Directora o el Director Nacional.

Para los efectos del inciso anterior, la Agencia requerirá informe fundado a los organismos públicos con competencia sectorial para que se pronuncien sobre aquellas instituciones públicas y privadas que deban calificarse como operadores de importancia vital. Dichos informes deberán evacuarse en la forma prescrita en el artículo 37 bis de la ley Nº19.880.

Recibidos los informes indicados precedentemente la Agencia dispondrá de un plazo de treinta días corridos para evacuar un informe que contendrá la nómina preliminar de las instituciones calificadas como operadores de importancia vital. Esta nómina preliminar deberá ser sometida a consulta pública por un plazo de treinta días corridos sólo respecto de las instituciones privadas, en la forma que determine el reglamento de la presente ley. Respecto de las instituciones públicas, se deberá requerir informe del Ministerio de Hacienda, en los términos del inciso precedente.

Terminado el proceso de consulta pública y recibido el informe del Ministerio de Hacienda, la Agencia dispondrá de treinta días corridos para elaborar el informe que contendrá la nómina final de instituciones que deban ser calificadas como operadores de importancia vital, individualizándolas en la forma que señale el reglamento.

Cumplidas las etapas anteriores, la Agencia, mediante resolución fundada de su Director o Directora, determinará los operadores de importancia vital.

En contra de la resolución que se dicte podrán deducirse aquellos recursos a que se refiere la ley N° 19.880, sin perjuicio de ejercer el recurso establecido en el artículo 37 de la presente ley.

Un reglamento expedido por el ministerio a cargo de la seguridad pública contemplará los demás aspectos del procedimiento que sean necesarios para su correcta ejecución."

Al artículo 5º que ha pasado a ser artículo 7º.

a) Ha reemplazado los incisos primero, segundo, tercero, cuarto y quinto por los siguientes:

"Las instituciones obligadas por la presente ley deberán aplicar de manera permanente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad. Estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso.

El cumplimiento de estas obligaciones exige 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. El objeto de estos protocolos y estándares será la prevención y gestión de los riesgos asociados a la ciberseguridad, así como la contención y mitigación del impacto que los incidentes pueden tener sobre la continuidad operacional del servicio prestado o la confidencialidad y la integridad de la información o de las redes o sistemas informáticos de conformidad con lo prescrito en la presente ley.

Para efectos de emitir las medidas de seguridad a que se refiere el inciso primero, la Agencia deberá observar lo prescrito en el artículo 23, según corresponda. Dichos protocolos y estándares deberán someterse a consulta pública, en la misma forma y plazo señalados en el inciso tercero del artículo 6. La medida deberá publicarse junto con el informe en que se justifique el rechazo o modificación de las observaciones que correspondan.

La Agencia deberá establecer medidas de seguridad diferenciadas según el tipo de organización de que se trate, teniendo especialmente en consideración las características y posibilidades de las pequeñas y medianas empresas definidas por la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño.”

b) Ha suprimido el inciso final.

Al artículo 6º que ha pasado a ser artículo 8º.

Lo ha sustituido por el siguiente:

“Artículo 8º. Deberes específicos de los operadores de importancia vital.

Todos los operadores de importancia vital deberán:

a) Implementar un sistema de gestión de seguridad de la información continuo con el fin de determinar aquellos riesgos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y la continuidad operacional del servicio.

Este sistema deberá permitir evaluar tanto la probabilidad como el potencial impacto de un incidente de ciberseguridad.

b) Mantener un registro de las acciones ejecutadas que compongan el sistema de gestión de seguridad de la información, de conformidad a lo que señale el reglamento.

c) Elaborar e implementar planes de continuidad operacional y ciberseguridad, los cuales deberán certificarse en conformidad al artículo 26 de la presente ley, y deberán someterse a revisiones periódicas por parte de los sujetos obligados, con una frecuencia mínima de dos años.

Con todo, la Agencia podrá instruir a uno o más operadores de importancia vital, fundadamente y por motivos sobrevinientes graves, la certificación de sus planes de continuidad operacional o ciberseguridad en un plazo menor al indicado en el párrafo precedente; sin embargo, la Agencia sólo podrá ejercer esta facultad, respecto de cada operador de importancia vital, siempre que la certificación tenga al menos un año de vigencia.

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 Nacional, 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 que señale el artículo 27 de la presente ley.

g) Informar a los potenciales afectados sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos, especialmente cuando involucren datos personales y no exista otra disposición legal que requiera su notificación; o cuando sea necesario para prevenir la ocurrencia de nuevos incidentes o para gestionar uno que ya hubiera ocurrido.

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 actuará como contraparte de la Agencia e informará a la autoridad o jefatura o jefe superior del órgano o servicio de la Administración del Estado o a los directores, gerentes, administradores o ejecutivos principales, según lo definan las instituciones privadas.”

Al artículo 7º que ha pasado a ser artículo 9º.

Lo ha reemplazado por el siguiente:

“Artículo 9°. Deber de reportar. Todas las instituciones públicas y privadas señaladas en el artículo 4° de la presente ley, tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos en los términos del artículo 25, tan pronto les sea posible y conforme el siguiente esquema:

a) Dentro del plazo máximo de 3 horas contadas desde que se tiene conocimiento de la ocurrencia del ciberataque o incidente de ciberseguridad que tiene impactos significativos, se deberá enviar una alerta temprana sobre la ocurrencia del evento,

b) Dentro del plazo máximo de 72 horas, una actualización de la información contemplada en la letra a), que incluya una evaluación inicial del incidente, su gravedad e impacto, así como indicadores de compromiso, si estuvieran disponibles.

Sin embargo, en caso que la institución afectada fuera un operador de importancia vital y este viera afectada la prestación de sus servicios esenciales a causa del incidente, la actualización de la información deberá entregarse al CSIRT Nacional en un plazo máximo de 24 horas contadas desde que haya tenido conocimiento del incidente;

c) Dentro del plazo máximo de quince días corridos contados desde el envío de la alerta temprana contemplada en la letra a), un informe final en el que se recojan al menos los siguientes elementos:

i) una descripción detallada del incidente, incluyendo su gravedad e impacto;

ii) el tipo de amenaza o causa principal que probablemente haya causado el incidente;

iii) las medidas de mitigación aplicadas y en curso;

iv) si procede, las repercusiones transfronterizas del incidente;

e) En el caso de que el incidente siga en curso con posterioridad a la presentación del informe contemplado en el literal c), éste se reemplazará por un informe de situación en ese momento, debiendo el informe final ser presentado en el plazo de 15 días corridos contados desde que se haya gestionado el incidente.

Sin perjuicio de lo anterior, tanto el CSIRT Nacional como la autoridad sectorial competente podrán requerir las actualizaciones pertinentes sobre la situación.

Los operadores de importancia vital deberán, además, 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 contados desde que se tuvo conocimiento de la ocurrencia del incidente.

En el caso de los organismos del Estado, 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, y siempre que tenga por objeto prevenir, detectar o responder a incidentes, recuperarse de ellos o reducir su repercusión; o reforzar el nivel de ciberseguridad, garantizando a su vez que se respete la posible naturaleza delicada de la información compartida. Con el objeto de cumplir con lo anterior, los contratos de prestación de servicios no podrán contener ninguna cláusula que pudiera restringir o dificultar de cualquier modo la comunicación de información sobre amenazas por parte del prestador de servicios, siempre y cuando con ello no se comprometa la seguridad y protección de datos, incluida la confidencialidad y protección de la propiedad intelectual.

La Agencia dictará las instrucciones que sean necesarias para la debida realización y recepción de los reportes a que se refiere el presente artículo. En caso de existir la obligación de notificar a más de una autoridad, la Agencia en conjunto con las autoridades involucradas y conforme lo dispuesto en el artículo 21 de la presente ley, procurará poner a disposición de los obligados un sistema de ventanilla única que permita la notificación simultánea a todas ellas.

Un reglamento expedido por el Ministerio encargado de la Seguridad Pública regulará el contenido del as diversas clases de aportes señalados en este artículo.”

Al artículo 8º, que ha pasado a ser artículo 10.

Ha eliminado el inciso segundo.

Al artículo 9º, que ha pasado a ser artículo 11.

Lo ha reemplazado por el siguiente:

“Artículo 11. 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 los protocolos y estándares que señala el artículo 7; las instrucciones generales y particulares, de carácter obligatorio, para las instituciones, tanto públicas como privadas obligadas por la presente ley; y las demás disposiciones necesarias para la aplicación y el cumplimiento de esta ley y sus reglamentos.

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 al CSIRT Nacional y a los demás pertenecientes a la Administración del Estado; y requerir de estos la información que sea necesaria para el cumplimiento de sus fines.

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) Calificar, mediante resolución fundada y en la forma prevista en los artículos 4, 5 y 6 de esta ley, a los servicios esenciales y a los operadores de importancia vital.

h) Requerir a 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, conforme lo dispuesto en el literal g) del artículo 8 de la presente ley.

i) Diseñar e implementar planes y acciones de formación ciudadana, capacitación, fortalecimiento, difusión y promoción de la cultura en ciberseguridad.

j) Requerir a los organismos de la Administración del Estado y a las instituciones privadas señaladas en el artículo 4 de la presente ley acceso a la información estrictamente necesaria para prevenir la ocurrencia de incidentes de ciberseguridad o para gestionar uno que ya hubiera ocurrido. Para lo anterior, podrá requerir la entrega del registro de actividades de las redes y sistemas informáticos que permitan comprender detalles de los incidentes de ciberseguridad que puedan haber ocurrido.

Para el ejercicio de esta atribución, la instrucción siempre tendrá carácter particular, debiendo especificarse la información solicitada y fundarse debidamente. Cuando la información referida en el inciso anterior pudiera incluir datos personales estos deberán ser anonimizados, siempre que ello sea posible sin entorpecer la gestión de incidentes. En cualquier caso, los datos personales sólo podrán ser tratados dando estricto cumplimiento a lo dispuesto en la ley 19.628, y en particular, al principio de finalidad, sin perjuicio de lo que define la presente ley y sus reglamentos.

Con todo, para efectos de lo dispuesto en esta ley, no se considerará que la dirección IP sea un dato personal.

k) Requerir, mediante instrucción de su Director o Directora, en casos de incidentes de impacto significativo cuya gestión lo haga imprescindible, el acceso a redes y sistemas informáticos. Este requerimiento deberá notificarse sin demora al requerido a través de la dirección de correo electrónico que haya sido proporcionada a la Agencia, de conformidad con lo establecido en el reglamento. Una vez notificado, el requerido deberá proporcionar todas las facilidades de acceso que sean necesarias. En caso de que el requerido sea una institución privada de las señaladas en el artículo 4, podrá oponerse. Formulada la oposición la Agencia solo podrá acceder previa autorización judicial conforme lo dispuesto en los párrafos siguientes y no procederá el reclamo establecido en el artículo 46.

Corresponderá a un ministro de la Corte de Apelaciones de Santiago conocer del requerimiento. Anualmente, el Presidente de la Corte de Apelaciones de Santiago deberá designar, por sorteo, a dos de sus miembros para cumplir esta labor. Si ninguno de los ministros estuviere en funciones, corresponderá otorgar la autorización al Presidente de la Corte o a quien lo subrogue. La autorización deberá solicitarse por escrito y fundarse en hechos específicos que justifiquen la necesidad del requerimiento. Para tales efectos todos los días y horas se entenderán hábiles.

La resolución que autorice o deniegue el acceso a las redes y sistemas, deberá dictarse previa audiencia en el más breve plazo en la que se escuchará a las partes.

En contra de la resolución que dicte el Ministro de Corte procederá el recurso de apelación ante la Corte de Apelaciones de Santiago,. Dicha Corte podrá resolver la apelación en cuenta sin más trámite. Los autos se agregarán de manera extraordinaria y con preferencia a la tabla del día siguiente; pero si este fuere inhábil, deberá el tribunal funcionar extraordinariamente para el solo conocimiento del recurso. Si producto de la interposición de recusaciones o implicancias no hubiere tribunal, los autos serán conocidos el día siguiente, según las reglas precedentes.

En caso de que se requiriera la restricción del acceso o uso de redes o sistemas informáticos se estará a lo dispuesto en este literal. No obstante, la Agencia deberá actuar conjuntamente con la autoridad sectorial correspondiente.

El procedimiento dispuesto en los incisos precedentes también será aplicable los requerimientos de acceso a redes y sistemas informáticos a que se refiere en el inciso tercero del literal ñ) del presente artículo.

l) Cooperar con organismos públicos e instituciones privadas, 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 autoridades nacionales de ciberseguridad extranjeras o sus homólogos y con los organismos internacionales con competencia en materia de ciberseguridad.

Cuando se trate de la cooperación con Estados y organizaciones internacionales, dicha actividad deberá realizarse en coordinación con el Ministerio de Relaciones Exteriores, en conformidad con lo previsto en el inciso primero del artículo 2 de la ley N° 21.080.

m) Prestar, cuando sus recursos humanos, técnicos y financieros así lo permitan, 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 mencionada ley N°19.628.

n) Colaborar 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.

ñ) 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.

Para el cumplimiento de su función fiscalizadora, la Agencia podrá realizar inspecciones; instruir de manera particular auditorías por sí o mediante terceros autorizados y análisis de seguridad basados en criterios de evaluación de riesgos

objetivos, los cuales deberán ser no discriminatorios, equitativos y transparentes. La entidad fiscalizada deberá cooperar en todo momento con los funcionarios de la Agencia o con los terceros autorizados por ella, según corresponda.

Asimismo, la Agencia podrá requerir el acceso a sistemas informáticos, datos, documentos y demás información que fuere necesaria para el desempeño de sus funciones de supervisión y fiscalización; instruir de manera particular a los sujetos obligados que realicen pruebas que demuestren la implementación de los planes de continuidad operacional y ciberseguridad, referidos en la letra c) del artículo 8°. Adicionalmente, podrá citar a declarar, respecto de hechos cuyo conocimiento estime necesario para el cumplimiento de sus funciones, a los socios, directores, administradores, representantes, empleados, y cualquier persona que, a cualquier título, preste o haya prestado servicios para las personas o entidades fiscalizadas, así como a toda persona que hubiere ejecutado o celebrado con ellas actos o convenciones de cualquier naturaleza. No obstante, no estarán obligadas a concurrir a declarar las personas indicadas en el artículo 361 del Código de Procedimiento Civil, a las cuales la Agencia, para los fines expresados en el párrafo precedente, deberá pedir declaración por escrito.

Para el ejercicio de esta atribución podrá establecer la forma, plazos y procedimientos para que las entidades fiscalizadas cumplan la obligación de presentar los antecedentes e informaciones referidos en los párrafos precedentes.

o) Instruir el inicio de procedimientos sancionatorios y sancionar las infracciones e incumplimientos en que incurran las instituciones obligadas por la presente ley respecto de sus disposiciones, reglamentos e instrucciones generales y particulares que emita la Agencia. Para tales efectos, y de manera fundada, podrá citar a declarar, en los términos señalados en el literal n) de este artículo, 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. La declaración podrá tomarse presencialmente o por otros medios que aseguren su integridad y fidelidad.

p) 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.

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

r) Informar al CSIRT de la Defensa Nacional y a los CSIRT de los organismos de la Administración del Estado 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.

s) 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.

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

u) 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.

v) 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.

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

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

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

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

Al Artículo 10, sin cambios, que ha pasado a ser artículo 12.

Al Artículo 11, que ha pasado a ser artículo 14.

Ha eliminado el literal g) del artículo 11, que ha pasado a ser artículo 14, readecuándose el orden correlativo del literal siguiente

Al Artículo 12, sin enmiendas, que ha pasado a ser artículo 15.

Artículo nuevo.

Ha agregado el siguiente artículo 13, nuevo, readecuándose el orden correlativo de los artículos siguientes:

“Artículo 13. Existirá un Subdirector o Subdirectora Nacional de la Agencia, quien dependerá del Director o Directora Nacional y lo subrogará, en caso de ausencia o impedimento, y además ejercerá las funciones de los literales ñ) y o) del artículo 11. Para ello, contará con la atribución de instruir la apertura de procedimientos administrativos sancionadores, designar a los funcionarios a cargo, determinar las sanciones e imponerlas.

El Subdirector o Subdirectora Nacional de la Agencia, estará afecto al Sistema de Alta Dirección Pública, establecido en la ley N° 19.882, como cargo de segundo nivel jerárquico.”

Al Artículo 13, sin cambios, que ha pasado a ser artículo 16.

Al Artículo 14, sin modificaciones, ha pasado a ser artículo 17.

Al Artículo 15, sin enmiendas, ha pasado a ser artículo 18.

Al artículo 16, que ha pasado a ser artículo 20.

Inciso segundo.

Ha intercalado entre la expresión “civil,” y “quienes” la frase “cuyo objeto o razón social se refiera a materias de esta ley,”

Al artículo 17, sin cambios, que ha pasado a ser artículo 21.

Al artículo 18, sin enmiendas, que ha pasado a ser artículo 22.

Artículo nuevo.

Ha agregado el siguiente artículo 19, nuevo, readecuándose el orden correlativo de los artículos siguientes:

“Artículo 19. Notificación responsable de vulnerabilidades. No serán aplicables las obligaciones previstas en el artículo 175 del Código Procesal Penal y en el artículo 61, literal k). del Estatuto Administrativo, a los trabajadores de la Agencia respecto de la información que reciban por parte de las personas que les notifiquen vulnerabilidades de ciberseguridad. La Agencia deberá mantener en secreto la notificación, sus antecedentes y la identidad de quien la realice, no pudiendo esta última ser revelada sin el consentimiento expreso de la persona que la realizó.”

Al artículo 19, sin cambios, que ha pasado a ser artículo 23.

Al artículo 20., que ha pasado a ser artículo 24.

Literal b).

i. Ha reemplazado la expresión “Sectoriales”, la primera vez que aparece, por la frase “que pertenezcan a organismos de la Administración del Estado”.

ii. Ha suprimido la expresión “por parte de los CSIRT Sectoriales,”.

iii. Ha añadido el siguiente párrafo final, nuevo:

“Cuando los ciberataques o incidentes puedan afectar el normal funcionamiento del sistema financiero, la respuesta del CSIRT Nacional deberá realizarse en coordinación con el Consejo de Estabilidad Financiera creado por la ley N° 20.789. Sin perjuicio de la obligación del CSIRT Nacional de comunicar al mencionado Consejo sobre el incidente, podrá tomar medidas sin esperar respuesta en casos de urgencia.”.

Literal d).

Ha sustituido la expresión “Sectoriales” por la frase “que pertenezcan a organismos de la Administración del Estado.”.

AL TÍTULO IV.

Ha reemplazado en el encabezado “Otras instituciones intervinientes” por “Coordinación regulatoria y otras disposiciones”.

Al artículo 21, que ha pasado a ser artículo 25.

Lo ha reemplazado por el siguiente:

“Artículo 25. Coordinación regulatoria. Cuando la Agencia deba dictar protocolos, estándares técnicos o instrucciones de carácter general en el ejercicio de sus funciones, y estos tengan efectos en las áreas de competencia de otra entidad sectorial, deberá previamente remitir la información relevante a dicha entidad y solicitar un informe con el propósito de prevenir posibles conflictos normativos y garantizar la coordinación, cooperación y colaboración efectivas entre ambas autoridades.

La autoridad sectorial requerida deberá evacuar su informe dentro de un plazo de treinta días corridos a partir de la fecha en que recibió la solicitud indicada en el inciso anterior. La Agencia considerará el contenido de este informe en la

motivación del acto administrativo de carácter general que emita. Transcurrido el plazo sin que se hubiere recibido el informe correspondiente, la Agencia procederá a emitir los protocolos, estándares técnicos o instrucciones generales requeridos.

Cuando una autoridad sectorial, en el ejercicio de sus atribuciones establecidas en sus leyes orgánicas, deba emitir actos administrativos de carácter general que tengan efectos en los ámbitos de competencia de la Agencia en conformidad a la presente ley, deberá remitir a la Agencia la información pertinente y solicitar un informe con el objeto de prevenir posibles conflictos normativos y garantizar la coordinación, cooperación y colaboración entre ambas entidades. Además, en el ejercicio de estas atribuciones, las autoridades sectoriales deben tener en cuenta, al menos, los protocolos, estándares técnicos e instrucciones generales previamente emitidos por la Agencia.

Lo establecido en los incisos anteriores no se aplicará en los casos en que el acto administrativo respectivo requiera una aplicación inmediata o en el plazo más breve posible atendida a su naturaleza y urgencia, siempre que se justifique dicha circunstancia y se deje constancia. No obstante, en estos casos, la Agencia deberá, en un plazo de tres días corridos, proporcionar a las autoridades sectoriales competentes, o viceversa según corresponda, todos los documentos tenidos a la vista y solicitar un informe con el fin de cumplir con los objetivos mencionados en los incisos primero y tercero.”

Al artículo 22, que ha pasado a ser artículo 26.

Lo ha sustituido por el siguiente:

“Artículo 26. Normativa Sectorial. Las autoridades sectoriales podrán emitir normativas generales, técnicas e instrucciones necesarias para fortalecer la ciberseguridad en las instituciones de su sector, en conformidad con la regulación respectiva y siguiendo lo dispuesto en el artículo anterior, cuando corresponda.

Las instituciones supervisadas deberán cumplir obligatoriamente con estas normas e instrucciones en la gestión de sus riesgos, de acuerdo con la autoridad sectorial que las haya emitido. La fiscalización y sanción relacionadas con estas disposiciones se regirán por las leyes respectivas de dicha autoridad sectorial.

Cuando las normas o instrucciones emitidas por una autoridad sectorial establezcan obligaciones para un sector a fin de prevenir incidentes de ciberseguridad, que tengan, al menos, efectos equivalentes a las obligaciones previstas en los protocolos, normas o instrucciones de la Agencia, prevalecerán las disposiciones de la autoridad sectorial. Esto no afectará los deberes de coordinación establecidos en el artículo 23 ni la aplicación de las normas de la presente ley. No obstante, si las normas o instrucciones de una autoridad sectorial no cubren a todas las entidades de un sector o solo se aplican a una parte de sus supervisados, los protocolos, normas o instrucciones de la Agencia seguirán siendo plenamente aplicables a las entidades no exceptuadas en los términos indicado en este inciso.

Para efectos de lo indicado en el inciso anterior, la Agencia y la autoridad sectorial correspondiente deberán previamente dictar una norma conjunta de carácter general. Dicha norma tendrá por objeto establecer criterios para la evaluación de la equivalencia de los efectos entre una normativa o instrucción.”

Al artículo 23, que ha pasado a ser artículo 27.

Inciso segundo.

Ha reemplazado el vocablo "Sectoriales" por la frase "que pertenezcan a organismos de la Administración del Estado"

Al artículo 24, que ha pasado a ser artículo 28.

Lo ha sustituido por el siguiente:

“Artículo 28. Centros de certificación. Los operadores de importancia vital deberán obtener las certificaciones de ciberseguridad que señala esta ley y las que determine la Agencia mediante reglamento. Para estos efectos, solo los organismos que sean parte del registro de entidades certificadoras autorizadas a cargo de la Agencia, estarán habilitadas para emitir certificaciones válidas que esta ley exija. Para formar parte de este registro bastará acreditar el cumplimiento de los requisitos que establezca el reglamento, pudiendo mantenerse en tanto cumplan los referidos requisitos.

La Agencia podrá homologar certificaciones técnicas internacionales o extranjeras sobre ciberseguridad mediante resolución fundada de su director o directora.”

Al artículo 25, sin cambios, que ha pasado a ser artículo 29.

Al artículo 26, sin modificaciones, que ha pasado a ser artículo 30.

Al artículo 27, sin enmiendas, que ha pasado a ser artículo 31.

Al artículo 28, que ha pasado a ser artículo 32.

Ha incorporado luego del punto final, que ha pasado a ser coma, la frase: “conforme a lo que determine el reglamento.”

Al artículo 29, que ha pasado a ser artículo 33

Inciso primero.

Ha reemplazado la expresión “o sectoriales” por “o que pertenezcan a organismos de la Administración del Estado”

Inciso tercero.

Ha sustituido la expresión “de los sectoriales” por “de los que pertenezcan a organismos de la Administración del Estado”

Al artículo 30, sin cambios, que ha pasado a ser artículo 34

Al artículo 31, que ha pasado a ser artículo 35.

Lo ha sustituido por el siguiente:

“Artículo 35. Deber de reserva de la Agencia. La Agencia deberá mantener y cautelar la reserva de la información que llegue a conocer en el desempeño de sus funciones cuando ella tenga tal calidad en virtud de una norma legal o porque, habiendo sido requerida por ella, le sea entregada bajo tal calidad. Asimismo, deberá procurar 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.

Sin perjuicio de lo anterior, no se incumple el deber de reserva en aquellos casos en que la Agencia o el CSIRT Nacional, en cumplimiento de sus funciones, deba difundir antecedentes que se encontraren sujetos a reserva, siempre que ello permita gestionar, prevenir o contener un incidente de ciberseguridad.”

Al artículo 32, sin enmiendas, que ha pasado a ser artículo 36

A los artículos 33 y 34.

Los ha sustituido por los siguientes artículos 37, 38, 39, 40, 41, 42, 43, 44 y 45.

“Artículo 37. Competencia de la autoridad sectorial. La autoridad sectorial será competente para fiscalizar, conocer y sancionar las infracciones, así como ejecutar las sanciones a la normativa sobre ciberseguridad que hubiere dictado y cuyos efectos sean al menos equivalentes al de la normativa dictada por la Agencia, conforme lo dispuesto en el artículo 24. Para este efecto, las sanciones y procedimientos sancionatorios serán los que correspondan a la autoridad sectorial de conformidad a su normativa. Fuera de dichos casos, corresponderá a la Agencia fiscalizar, conocer y juzgar las infracciones, así como ejecutar las sanciones a la presente ley, sin perjuicio de la facultad de los organismos de la Administración del Estado de poner en conocimiento del organismo competente las infracciones a la norma de que tomaren conocimiento.”

“Artículo 38. Infracciones. Las infracciones a las obligaciones que esta ley prescribe a los sujetos obligados por ella se califican en leves, graves y gravísimas.

Se considerarán infracciones leves las siguientes:

1. Entregar fuera de plazo la información que se le requiera cuando ella no fuere necesaria para la gestión de un incidente de ciberseguridad;
2. Incumplir las instrucciones generales o particulares impartidas por la Agencia en los casos que no esté sancionado como infracción grave o gravísima; y
3. Cualquier infracción a las obligaciones que esta ley establece y que no tenga señalada una sanción especial.

Se considerarán infracciones graves las siguientes:

1. No haber implementado los protocolos y estándares establecidos por la Agencia para prevenir, reportar y resolver incidentes de ciberseguridad;
2. No haber implementado los estándares particulares de ciberseguridad;
3. Entregar fuera de plazo la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de ciberseguridad;
4. Entregar a la Agencia de información manifiestamente falsa o errónea.
5. Incumplir la obligación de reportar establecida en el artículo 9;
6. Negarse injustificadamente a cumplir una instrucción de la Agencia o entorpecer deliberadamente el ejercicio de las atribuciones de la Agencia durante la gestión de un incidente de ciberseguridad, siempre que la atribución no cuente con una sanción especial; y
7. La reincidencia en una misma infracción leve dentro de un año.

Se considerarán infracciones gravísimas las siguientes:

1. Entregar a la Agencia información manifiestamente falsa o errónea, cuando ella sea necesaria para la gestión de un incidente de ciberseguridad;
2. Incumplir las instrucciones generales o particulares impartidas por la Agencia durante la gestión de un incidente de impacto significativo;
3. No entregar la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de impacto significativo; y
4. La reincidencia en una infracción grave dentro de un año.”

“Artículo 39. De las infracciones de los Operadores de Importancia Vital. Sin perjuicio de lo prescrito en el artículo precedente, los Operadores de Importancia Vital podrán ser sancionados por infringir las disposiciones del artículo 8º, las que se califican en leves, graves y gravísimas.

Se considerarán infracciones leves las siguientes:

1. No mantener el registro de las acciones de seguridad que señala la letra b);
2. No comunicar al CSIRT Nacional la realización continua de operaciones de revisión, ejercicios y demás acciones que señala el literal d);
3. No contar con programas de capacitación, formación y educación continua para los trabajadores, según dispone el literal g);
4. No designar un delegado de ciberseguridad, según dispone la letra i);
5. No dar cumplimiento a la instrucción particular de la Agencia en orden a certificar los planes de continuidad operacional del párrafo segundo de la letra c); y
6. No contar con las certificaciones que exija la ley, de acuerdo al literal f).

Se considerarán infracciones graves las siguientes:

1. No haber implementado el sistema de gestión de seguridad de la información continuo al que se refiere el literal a) d;
2. No haber elaborado o implementado los planes de continuidad operacional y ciberseguridad a los que se refiere la letra c);
3. No informar a los potenciales afectados sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos, en los casos que señala la letra g);
4. No adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o un ciberataque, según señala la letra e); y
5. La reincidencia en una misma infracción leve dentro del periodo de un año.

Se considerarán infracciones gravísimas las siguientes:

1. No adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o un ciberataque, según señala la letra e), cuando este posea un impacto significativo; y
2. La reincidencia en una misma infracción grave dentro del periodo de un año”.

“Artículo 40. De las sanciones. La infracción a los preceptos de esta ley conlleva la imposición de una multa a beneficio fiscal, de acuerdo a la siguiente escala:
1. Las infracciones leves serán sancionadas con multa de hasta 5.000 unidades tributarias mensuales; o con hasta 10.000 unidades tributarias mensuales si se tratare de un operador de importancia vital;
2. Las infracciones graves serán sancionadas con multa de hasta 10.000 unidades tributarias mensuales; o con hasta 20.000 unidades tributarias mensuales si se tratare de un operador de importancia vital; y
3. Las infracciones gravísimas serán sancionadas con multa de hasta 20.000 unidades tributarias mensuales; o con hasta 40.000 unidades tributarias mensuales si se tratare de un operador de importancia vital.

La multa será fijada teniendo en consideración el grado en que el infractor adoptó las medidas necesarias para resguardar la seguridad informática de las operaciones, la probabilidad de ocurrencia del incidente, el grado de exposición del infractor

a los riesgos, la gravedad de los efectos de los ataques incluidas sus repercusiones sociales o económicas, la reiteración en la infracción dentro del plazo de 3 años contado desde el momento en que se produjo el incidente, el tamaño 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 41. Procedimiento simplificado. Tratándose de la formulación de cargos por infracciones calificadas como leves en conformidad al artículo 37, la Agencia estará facultada para proponer de manera inmediata la sanción a aplicar, la cual quedará firme si el presunto infractor opta por allanarse a los cargos formulados en su contra. En caso contrario, si el presunto infractor decide rechazar la imputación y presentar descargos, se procederá conforme a lo indicado en el artículo 40 de la presente ley.”

“Artículo 42. Procedimiento administrativo sancionador. El procedimiento administrativo se regirá por lo prescrito por la ley Nº19.880, que establece bases de los procedimientos administrativos que rigen los actos de los organismos de la Administración del Estado, sin perjuicio de las siguientes disposiciones:

a) Toda sanción deberá fundarse en un procedimiento que se iniciará con la formulación precisa y fundada de los cargos y contendrá la descripción de los hechos en los que se fundamentan y de cómo éstos constan en la investigación, la indicación de por qué se consideran una infracción a la normativa, especificando la o las normas que se estimen infringidas y el presunto responsable de la infracción. Además, se designará al funcionario a cargo de la instrucción del procedimiento. Se fijará un plazo para la formulación de descargos que no podrá ser inferior a quince ni superior a treinta días. Las notificaciones del procedimiento deberán realizarse a la dirección de correo electrónico que haya sido proporcionada a la Agencia, de conformidad al reglamento.

b) En los descargos deberán señalarse todas las circunstancias o antecedentes de hecho y de derecho que eximan o atenúen la presunta responsabilidad de la persona objeto de cargos, así como aquellas que nieguen la efectiva ocurrencia de los hechos, o que demuestren que éstos no constituyen infracción. Todo ello, sin perjuicio de otras presentaciones o antecedentes posteriores que se hagan valer en el curso del procedimiento sancionatorio con el mismo objetivo. Asimismo, deberán solicitarse las diligencias probatorias que correspondieren.

c) Vencido el plazo para formular descargos, se abrirá un término probatorio por un plazo no inferior a diez ni superior a veinte días, según la naturaleza y complejidad del asunto. Dicho plazo podrá prorrogarse por una sola vez y hasta por un máximo de quince días. Se podrá rendir prueba mediante cualquier medio admisible en Derecho, los que se apreciarán de acuerdo a las reglas de la sana crítica.

d) Excepcionalmente, se realizarán las diligencias que, decretadas de oficio o a petición de parte, se estimen estrictamente necesarias para la resolución del asunto. Las diligencias podrán solicitarse dentro de los cinco días siguientes al vencimiento del término probatorio.

e) Una vez transcurrido el plazo mencionado en el literal previo, el procedimiento deberá concluir. El instructor del procedimiento emitirá un informe en el cual deberá incluir un análisis detallado de todas las defensas, alegatos y pruebas

presentadas durante el procedimiento sancionatorio a partir del cual se determinará si se ha infringido la normativa vigente y si procede la imposición de la sanción respectiva o la absolución de los cargos. El informe deberá emitirse dentro del plazo de quince días.

f) Una vez recibido el informe del instructor del procedimiento, corresponderá al Subdirector de la Agencia resolver los procesos sancionatorios en el plazo de quince días, dictando al efecto resolución fundada en la cual absolverá al infractor o aplicará la sanción, en su caso. La resolución del Subdirector deberá incluir el mismo contenido que el informe señalado en el literal precedente."

"Artículo 43. De los recursos. En contra de la resolución del Subdirector mediante la cual se concluye el procedimiento administrativo procederán los recursos que establezca la ley Nº19.880. El recurso deberá resolverse dentro del plazo de quince días. La interposición del recurso suspenderá el plazo para reclamar de ilegalidad, siempre que se trate de materias por las cuales procede dicho recurso."

"Artículo 44. Forma de pago de las multas. Las multas deberán pagarse dentro de los diez días siguientes contados desde que el acto administrativo que las impone quede firme. Vencido ese plazo, la resolución que establezca la sanción tendrá mérito ejecutivo y se hará exigible por la Tesorería General de la República. Para su cobro se aplicará el inciso segundo del artículo 35 del decreto ley N° 1.263, de 1975, orgánico de Administración Financiera del Estado.

El pago de toda multa deberá ser acreditado ante la Agencia, dentro de los diez días siguientes a la fecha en que ésta debió ser pagada.

El retardo en el pago de estas multas devengará los intereses y reajustes establecidos en el artículo 53 del Código Tributario."

"Artículo 45. Pronto pago. El sancionado que no interponga recurso alguno podrá, dentro de los cinco días hábiles siguientes a que le sea notificada la resolución del Subdirector que le impone la sanción, pagar directamente en la Tesorería General de la República en cuyo caso, el monto de la misma será reducido en un veinticinco por ciento. Una vez ejercido este derecho, se entenderán renunciado todos los recursos."

Al artículo 35, que ha pasado a ser artículo 46.

Inciso primero.

Ha sustituido la oración "El reclamo deberá interponerse dentro de los quince días hábiles siguientes a la notificación de la resolución impugnada, según las siguientes reglas:" por "El reclamo deberá interponerse dentro de los quince días hábiles siguientes a la notificación de la resolución impugnada, los que deberán computarse de acuerdo al artículo 25 de la ley N°19.880, según las siguientes reglas:"

Literal b).

Ha reemplazado la frase "le produzca", por "pueda ocasionar".

Literal h).

Ha sustituido la frase "no procederá recurso alguno", por "se podrá apelar ante la Corte Suprema, dentro del plazo de diez días hábiles, la que resolverá en cuenta".

Al artículo 36, que ha pasado a ser artículo 47.

Inciso primero.

a) Ha sustituido el vocablo “público” por “de la Administración del Estado”;

b) Ha reemplazado la frase “los principios y obligaciones establecidos en los Títulos I y II de esta ley, respectivamente” por “lo establecido en esta ley.”

Inciso segundo.

Ha sustituido la palabra “someterse” por “adoptar”.

Al artículo 37.

Lo ha eliminado.

Al artículo 38.

Lo ha suprimido.

AL TÍTULO VIII.

Ha reemplazado en el encabezado la frase “de Ciberseguridad por “sobre Ciberseguridad

Al artículo 39, que ha pasado a ser artículo 48.

Ha suprimido los literales d) y e), readecuándose el orden correlativo de los literales siguientes.

Al artículo 40, sin cambios, que ha pasado a ser artículo 49.

Al artículo 41, sin modificaciones, que ha pasado a ser artículo 50.

Al artículo 42, sin enmiendas, que ha pasado a ser artículo 51.

Al artículo 43 , sin enmiendas, que ha pasado a ser artículo 52.

Al artículo 44, que ha pasado a ser artículo 53.

Lo ha sustituido por el siguiente:

“Artículo 53. Regímenes especiales. El Senado y la Cámara de Diputados, el Poder Judicial, la Contraloría General de la República, el Banco Central, el Ministerio Público, el Servicio Electoral y el Consejo Nacional de Televisión deberán adoptar las medidas de seguridad de sus redes y sistemas informáticos que sean pertinentes. Para estos efectos, la Corte Suprema, el respectivo jefe de servicio o los órganos colegiados que ejerzan dicha función, podrán dictar la normativa que sea conveniente a tales efectos, pudiendo considerar en su formulación las recomendaciones que efectúe la Agencia.

Las instituciones y órganos señalados en este artículo no estarán sujetos en modo alguno a la regulación, fiscalización o supervigilancia de la Agencia; sin perjuicio de que deberán convenir mecanismos de reporte de incidentes de ciberseguridad y de coordinación y cooperación para la respuesta a incidentes de ciberseguridad.

Asimismo, si el órgano autónomo constitucional revistiera el carácter de autoridad sectorial, deberá considerársele para los efectos de los artículos 6, 25 y 26.”

Al artículo 45 , sin cambios, que ha pasado a ser artículo 54.

Al artículo 46, que ha pasado a ser artículo 55.

Ha reemplazado el N° 1 por el siguiente:

“1. Incorpórase, en el artículo 2°, el siguiente inciso final, nuevo:

“No será objeto de sanción penal por haber incurrido en los hechos tipificados en el inciso primero, el que habiendo accedido a un sistema informático cuyo responsable tenga domicilio en Chile, lo hiciera cumpliendo con las siguientes condiciones:

1) Encontrarse inscrito en el registro que al efecto lleve la Agencia Nacional de Ciberseguridad;

2) Que el acceso se haya realizado habiendo informado previamente de ello a la Agencia;

3) Que el acceso y las vulnerabilidades de seguridad detectadas hayan sido reportadas al responsable del sistema informático y a la Agencia, tan pronto se hubiere realizado;

4) 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 utilizando métodos que pudieran conducir a denegación de servicio, a pruebas físicas, utilización de código malicioso, ingeniería social y alteración, eliminación, exfiltración o destrucción de datos;

5) No haber divulgado públicamente la información relativa a la potencial vulnerabilidad;

6) Que se trate de un acceso a un sistema informático de los organismos de la administración del Estado. En el resto de los casos, requerirá del consentimiento del responsable del sistema informático.

7) Haber dado cumplimiento a las demás condiciones sobre comunicación responsable de vulnerabilidades que al efecto hubiere dictado la Agencia.”

Al artículo 47.

Lo ha eliminado.

Al artículo 48.

Lo ha suprimido.

ARTÍCULOS TRANSITORIOS.

Al artículo primero transitorio.

Ha añadido el siguiente numeral 2, nuevo, readecuándose el orden correlativo de los numerales siguientes:

“2. Determinar un periodo para la vigencia de las normas establecidas por la presente ley el cual no podrá ser inferior a seis meses desde su publicación."

Al artículo segundo transitorio.

Inciso primero.

Ha intercalado entre la palabra “personal” y el punto final, que ha pasado a ser punto seguido, la siguiente frase: “El primer Director do Directora de la Agencia Nacional de Ciberseguridad no podrá participar del primer proceso de selección por Alta Dirección Pública para la provisión de su cargo.”

Inciso segundo, nuevo.

Ha incorporado el siguiente inciso segundo, nuevo:

“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.

Al artículo tercero transitorio, sin enmiendas.

Al artículo cuarto transitorio, sin cambios.

Al artículo quinto transitorio.

Lo ha eliminado.

Al artículo sexto transitorio, que ha pasado a ser artículo quinto transitorio

Al artículo séptimo transitorio, que ha pasado a ser artículo sexto transitorio

Al artículo octavo transitorio

Lo ha suprimido.

VIII. MENCIÓN PRECISA DE LAS RESERVAS DE CONSTITUCIONALIDAD FORMULADAS

No hubo.

IX.- TEXTO DEL PROYECTO DE LEY TAL COMO QUEDARÍA EN VIRTUD DE LOS ACUERDOS ADOPTADOS POR LA COMISIÓN.

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 éstos 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 determinadas en el artículo 4°, y los mecanismos de control, supervisión y de responsabilidad ante infracciones.

Para efectos de esta ley, la Administración del Estado estará constituida por los Ministerios, las delegaciones presidenciales regionales y provinciales, los Gobiernos Regionales, las Municipalidades, las Fuerzas Armadas, de Orden y Seguridad Pública, las empresas públicas creadas por ley, y los órganos y servicios públicos creados para el cumplimiento de la función administrativa.

Las disposiciones de esta ley serán aplicables a las empresas del Estado y sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio.

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. Ciberataque: intento de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático.

6. 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.

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

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

9. 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.

10. 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 de los procesos ejecutados o implementados en las redes y sistemas informáticos.

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

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

13. 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.

14. 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.

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

Artículo 3°. Principios rectores.

Para alcanzar los objetivos de esta ley se deberán observar los siguientes principios:

1. Principio de control de daños: frente a un ciberataque o a un incidente de ciberseguridad siempre se deberá actuar coordinada y diligentemente, adoptando las medidas necesarias para evitar la escalada del ciberataque o del incidente de ciberseguridad y su posible propagación a otros sistemas informáticos.

2. Principio de cooperación con la autoridad: para resolver los incidentes de ciberseguridad se deberá prestar la cooperación debida con la autoridad competente y, si es necesario, cooperar entre diversos sectores, teniendo en cuenta la interconexión y la interdependencia de los sistemas y servicios.

3. Principio de coordinación: de conformidad a lo dispuesto por el inciso segundo del artículo 5º del decreto con fuerza de ley Nº1-19.653 que fija texto refundido, coordinado y sistematizado de la ley Nº 18.575, orgánica constitucional de Bases Generales de la Administración del Estado, la Agencia y las autoridades sectoriales deberán cumplir sus cometidos coordinadamente y propender a la unidad de acción, evitando la duplicación o interferencia de funciones.

4. Principio de seguridad en el ciberespacio: es deber del Estado resguardar la seguridad en el ciberespacio. El Estado velará porque todas las personas puedan participar de un ciberespacio seguro otorgando especial protección a las redes y sistemas informáticos que contengan información de aquellos grupos de personas que suelen ser en mayor medida objeto de ciberataques.

5. 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.

6. Principio de seguridad informática: toda persona tiene derecho a adoptar las medidas técnicas de seguridad informática que considere necesarias, incluyendo el cifrado.

7. Principio de racionalidad: las medidas para la gestión de incidentes de ciberseguridad, las obligaciones de ciberseguridad y el ejercicio de las facultades de la Agencia deberán ser necesarias y proporcionales al grado de exposición a los riesgos, así como al impacto social y económico que tendría.

8. Principio de seguridad y privacidad por defecto y desde el diseño: Los sistemas informáticos, aplicaciones y tecnologías de la información deben diseñarse, implementarse y gestionarse teniendo en cuenta la seguridad y la privacidad de los datos personales que procesan.

TÍTULO II
Obligaciones de ciberseguridad

Párrafo 1°
Servicios esenciales y operadores de importancia vital

Artículo 4°. Ámbito de aplicación. La presente ley se aplicará a las instituciones que presten servicios calificados como esenciales según lo establecido en los incisos segundo y tercero de este artículo y a aquellas que sean calificadas como operadores de importancia vital, de conformidad con lo dispuesto en los artículos 5 y 6 de esta ley.

Son servicios esenciales aquellos provistos por los organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional; los prestados bajo concesión de servicio público; y los proveídos por instituciones privadas que realicen las siguientes actividades: generación, transmisión o distribución eléctrica; transporte, almacenamiento o distribución de combustibles; suministro de agua potable o saneamiento; telecomunicaciones; infraestructura digital; servicios digitales, servicios de tecnología de la información gestionados por terceros; transporte terrestre, aéreo, ferroviario o marítimo, así como la operación de su infraestructura respectiva; banca, servicios financieros y medios de pago; administración de prestaciones de seguridad social; servicios postales y de mensajería; prestación institucional de salud por entidades tales como hospitales, clínicas, consultorios y centros médicos; y la producción y/o investigación de productos farmacéuticos.

La Agencia podrá calificar otros servicios como esenciales mediante resolución fundada del o la Directora Nacional cuando su afectación puede causar un grave daño a la vida o integridad física de la población o a su abastecimiento, a sectores relevantes de las actividades económicas, al medioambiente, al normal funcionamiento de la sociedad, de la Administración del Estado, a la defensa nacional, o a la seguridad y el orden público.

Dicha calificación deberá someterse al proceso de consulta pública y se regirá por las disposiciones de la ley Nº19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.

La Agencia identificará, mediante resolución exenta dictada conforme el procedimiento dispuesto en este artículo, las infraestructuras, procesos o funciones específicas que serán calificadas como esenciales, y que quedarán sujetas a las obligaciones establecidas en el artículo 8° de esta ley.

Artículo 5. Operadores de Importancia Vital. La Agencia establecerá mediante resolución dictada por el o la Directora Nacional, según se establece en el artículo siguiente, a los prestadores de servicios esenciales que sean calificados como operadores de importancia vital.

La Agencia podrá calificar como operadores de importancia vital a quienes reúnan los siguientes requisitos:

1.- que la provisión de dicho servicio dependa de las redes y sistemas informáticos; y,

2.- que la afectación, interceptación, interrupción o destrucción de sus servicios tenga un impacto significativo en la seguridad y el orden público; en la provisión continua y regular de servicios esenciales; en el efectivo cumplimiento de las funciones del Estado; o, en general, de los servicios que éste debe proveer o garantizar.

Además, la Agencia podrá calificar como operadores de importancia vital a instituciones privadas que, aunque no tengan la calidad de prestadores de servicios esenciales, reúnan los requisitos indicados en el inciso anterior y cuya calificación sea indispensable por haber adquirido un rol crítico en el abastecimiento de la población, la distribución de bienes o la producción de aquellos indispensables o estratégicos para el país; o por el grado de exposición de la entidad a los riesgos y la probabilidad de incidentes de ciberseguridad, incluyendo su gravedad y las consecuencias sociales y económicas asociadas.

En cualquier caso, siempre se deberá tener en consideración el tamaño de la institución privada, especialmente las características y necesidades de las micro, pequeñas y medianas empresas, tal como se definen en la ley N° 20.416.

Artículo 6. Procedimiento de calificación de los operadores de importancia vital. Al menos cada tres años, la Agencia deberá revisar y actualizar la calificación de operadores de importancia vital mediante una resolución dictada por la Directora o el Director Nacional.

Para los efectos del inciso anterior, la Agencia requerirá informe fundado a los organismos públicos con competencia sectorial para que se pronuncien sobre aquellas instituciones públicas y privadas que deban calificarse como operadores de importancia vital. Dichos informes deberán evacuarse en la forma prescrita en el artículo 37 bis de la ley Nº19.880.

Recibidos los informes indicados precedentemente la Agencia dispondrá de un plazo de treinta días corridos para evacuar un informe que contendrá la nómina preliminar de las instituciones calificadas como operadores de importancia vital. Esta nómina preliminar deberá ser sometida a consulta pública por un plazo de treinta días corridos sólo respecto de las instituciones privadas, en la forma que determine el reglamento de la presente ley. Respecto de las instituciones públicas, se deberá requerir informe del Ministerio de Hacienda, en los términos del inciso precedente.

Terminado el proceso de consulta pública y recibido el informe del Ministerio de Hacienda, la Agencia dispondrá de treinta días corridos para elaborar el informe que contendrá la nómina final de instituciones que deban ser calificadas como operadores de importancia vital, individualizándolas en la forma que señale el reglamento.

Cumplidas las etapas anteriores, la Agencia, mediante resolución fundada de su Director o Directora, determinará los operadores de importancia vital.

En contra de la resolución que se dicte podrán deducirse aquellos recursos a que se refiere la ley N° 19.880, sin perjuicio de la facultad de ejercer el recurso establecido en el artículo 46 de la presente ley.

Un reglamento expedido por el Ministerio encargado de la seguridad pública contemplará los demás aspectos del procedimiento que sean necesarios para su correcta ejecución.

Párrafo 2°
Obligaciones de ciberseguridad

Artículo 7°. Deberes generales. Las instituciones obligadas por la presente ley deberán aplicar de manera permanente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad. Estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso.

El cumplimiento de estas obligaciones exige 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. El objeto de estos protocolos y estándares será la prevención y gestión de los riesgos asociados a la ciberseguridad, así como la contención y mitigación del impacto que los incidentes pueden tener sobre la continuidad operacional del servicio prestado o la confidencialidad y la integridad de la información o de las redes o sistemas informáticos de conformidad con lo prescrito en la presente ley.

Para efectos de emitir las medidas de seguridad a que se refiere el inciso primero, la Agencia deberá observar lo prescrito en el artículo 25, según corresponda. Dichos protocolos y estándares deberán someterse a consulta pública, en la misma forma y plazo señalados en el inciso tercero del artículo 6. La medida deberá publicarse junto con el informe en que se justifique el rechazo o modificación de las observaciones que correspondan.

La Agencia deberá establecer medidas de seguridad diferenciadas según el tipo de organización de que se trate, teniendo especialmente en consideración las características y posibilidades de las pequeñas y medianas empresas definidas por la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño.

Artículo 8º. Deberes específicos de los operadores de importancia vital.

Todos los operadores de importancia vital deberán:

a) Implementar un sistema de gestión de seguridad de la información continuo con el fin de determinar aquellos riesgos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y la continuidad operacional del servicio.

Este sistema deberá permitir evaluar tanto la probabilidad como el potencial impacto de un incidente de ciberseguridad.

b) Mantener un registro de las acciones ejecutadas que compongan el sistema de gestión de seguridad de la información, de conformidad a lo que señale el reglamento.

c) Elaborar e implementar planes de continuidad operacional y ciberseguridad, los cuales deberán certificarse en conformidad al artículo 28 de la presente ley, y deberán someterse a revisiones periódicas por parte de los sujetos obligados, con una frecuencia mínima de dos años.

Con todo, la Agencia podrá instruir a uno o más operadores de importancia vital, fundadamente y por motivos sobrevinientes graves, la certificación de sus planes de continuidad operacional o ciberseguridad en un plazo menor al indicado en el párrafo precedente; sin embargo, la Agencia sólo podrá ejercer esta facultad, respecto de cada operador de importancia vital, siempre que la certificación tenga al menos un año de vigencia.

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 Nacional, 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 que señale el artículo 28 de la presente ley.

g) Informar a los potenciales afectados, en la medida que puedan identificarse y cunado así lo requiera la Agencia, sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos, especialmente cuando involucren datos personales y no exista otra disposición legal que requiera su notificación; o cuando sea necesario para prevenir la ocurrencia de nuevos incidentes o para gestionar uno que ya hubiera ocurrido.

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 actuará como contraparte de la Agencia e informará a la autoridad o jefatura o jefe superior del órgano o servicio de la Administración del Estado o a los directores, gerentes, administradores o ejecutivos principales, según lo definan las instituciones privadas.

Artículo 9°. Deber de reportar. Todas las instituciones públicas y privadas señaladas en el artículo 4° de la presente ley, tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos en los términos del artículo 27, tan pronto les sea posible y conforme el siguiente esquema:

a) Dentro del plazo máximo de 3 horas contadas desde que se tiene conocimiento de la ocurrencia del ciberataque o incidente de ciberseguridad que tiene impactos significativos, se deberá enviar una alerta temprana sobre la ocurrencia del evento,

b) Dentro del plazo máximo de 72 horas, una actualización de la información contemplada en la letra a), que incluya una evaluación inicial del incidente, su gravedad e impacto, así como indicadores de compromiso, si estuvieran disponibles.

Sin embargo, en caso que la institución afectada fuera un operador de importancia vital y este viera afectada la prestación de sus servicios esenciales a causa del incidente, la actualización de la información deberá entregarse al CSIRT Nacional en un plazo máximo de 24 horas contadas desde que haya tenido conocimiento del incidente;

c) Dentro del plazo máximo de quince días corridos contados desde el envío de la alerta temprana contemplada en la letra a), un informe final en el que se recojan al menos los siguientes elementos:

i) una descripción detallada del incidente, incluyendo su gravedad e impacto;

ii) el tipo de amenaza o causa principal que probablemente haya causado el incidente;

iii) las medidas de mitigación aplicadas y en curso;

iv) si procede, las repercusiones transfronterizas del incidente;

e) En el caso de que el incidente siga en curso con posterioridad a la presentación del informe contemplado en el literal c), éste se reemplazará por un informe de situación en ese momento, debiendo el informe final ser presentado en el plazo de 15 días corridos contados desde que se haya gestionado el incidente.

Sin perjuicio de lo anterior, tanto el CSIRT Nacional como la autoridad sectorial competente podrán requerir las actualizaciones pertinentes sobre la situación.

Los operadores de importancia vital deberán, además, 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 contados desde que se tuvo conocimiento de la ocurrencia del incidente.

En el caso de los organismos del Estado, 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, y siempre que tenga por objeto prevenir, detectar o responder a incidentes, recuperarse de ellos o reducir su repercusión; o reforzar el nivel de ciberseguridad, garantizando a su vez que se respete la posible naturaleza delicada de la información compartida. Con el objeto de cumplir con lo anterior, los contratos de prestación de servicios no podrán contener ninguna cláusula que pudiera restringir o dificultar de cualquier modo la comunicación de información sobre amenazas por parte del prestador de servicios, siempre y cuando con ello no se comprometa la seguridad y protección de datos, incluida la confidencialidad y protección de la propiedad intelectual.

La Agencia dictará las instrucciones que sean necesarias para la debida realización y recepción de los reportes a que se refiere el presente artículo. En caso de existir la obligación de notificar a más de una autoridad, la Agencia en conjunto con las autoridades involucradas y conforme lo dispuesto en el artículo 24_de la presente ley, procurará poner a disposición de los obligados un sistema de ventanilla única que permita la notificación simultánea a todas ellas.

Un reglamento expedido por el Ministerio encargado de la Seguridad Pública regulará el contenido de las diversas clases de reportes señalados en este artículo.

TÍTULO III
De la Agencia Nacional de Ciberseguridad

Párrafo 1°
Objeto, naturaleza y atribuciones

Artículo 10. Agencia Nacional de Ciberseguridad. Créase la Agencia Nacional de Ciberseguridad como un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propio, 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 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 11. 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 los protocolos y estándares que señala el artículo 7; las instrucciones generales y particulares, de carácter obligatorio, para las instituciones, tanto públicas como privadas obligadas por la presente ley; y las demás disposiciones necesarias para la aplicación y el cumplimiento de esta ley y sus reglamentos.

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 al CSIRT Nacional y a los demás pertenecientes a la Administración del Estado; y requerir de estos la información que sea necesaria para el cumplimiento de sus fines.

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) Calificar, mediante resolución fundada y en la forma prevista en los artículos 4, 5 y 6 de esta ley, a los servicios esenciales y a los operadores de importancia vital.

h) Requerir a 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, conforme lo dispuesto en el literal g) del artículo 8º de la presente ley.

i) Diseñar e implementar planes y acciones de formación ciudadana, capacitación, fortalecimiento, difusión y promoción de la cultura en ciberseguridad.

j) Requerir a los organismos de la Administración del Estado y a las instituciones privadas señaladas en el artículo 4º de la presente ley acceso a la información estrictamente necesaria para prevenir la ocurrencia de incidentes de ciberseguridad o para gestionar uno que ya hubiera ocurrido. Para lo anterior, podrá requerir la entrega del registro de actividades de las redes y sistemas informáticos que

permitan comprender detalles de los incidentes de ciberseguridad que puedan haber ocurrido.

Para el ejercicio de esta atribución, la instrucción siempre tendrá carácter particular, debiendo especificarse la información solicitada y fundarse debidamente. Cuando la información referida en el inciso anterior pudiera incluir datos personales estos deberán ser anonimizados, siempre que ello sea posible sin entorpecer la gestión de incidentes. En cualquier caso, los datos personales sólo podrán ser tratados dando estricto cumplimiento a lo dispuesto en la ley 19.628, y en particular, al principio de finalidad, sin perjuicio de lo que define la presente ley y sus reglamentos.

Con todo, para efectos de lo dispuesto en esta ley, no se considerará que la dirección IP sea un dato personal.

k) Requerir, mediante instrucción de su Director o Directora, en casos de incidentes de impacto significativo cuya gestión lo haga imprescindible, el acceso a redes y sistemas informáticos. Este requerimiento deberá notificarse sin demora al requerido a través de la dirección de correo electrónico que haya sido proporcionada a la Agencia, de conformidad con lo establecido en el reglamento. Una vez notificado, el requerido deberá proporcionar todas las facilidades de acceso que sean necesarias. En caso de que el requerido sea una institución privada de las señaladas en el artículo 4º, podrá oponerse. Formulada la oposición la Agencia solo podrá acceder previa autorización judicial conforme lo dispuesto en los párrafos siguientes y no procederá el reclamo establecido en el artículo 46.

Corresponderá a un ministro de la Corte de Apelaciones de Santiago conocer del requerimiento. Anualmente, el Presidente de la Corte de Apelaciones de Santiago deberá designar, por sorteo, a dos de sus miembros para cumplir esta labor. Si ninguno de los ministros estuviere en funciones, corresponderá otorgar la autorización al Presidente de la Corte o a quien lo subrogue. La autorización deberá solicitarse por escrito y fundarse en hechos específicos que justifiquen la necesidad del requerimiento. Para tales efectos todos los días y horas se entenderán hábiles.

La resolución que autorice o deniegue el acceso a las redes y sistemas, deberá dictarse previa audiencia en el más breve plazo en la que se escuchará a las partes.

En contra de la resolución que dicte el Ministro de Corte procederá el recurso de apelación ante la Corte de Apelaciones de Santiago. Dicha Corte podrá resolver la apelación en cuenta sin más trámite. Los autos se agregarán de manera extraordinaria y con preferencia a la tabla del día siguiente; pero si este fuere inhábil, deberá el tribunal funcionar extraordinariamente para el solo conocimiento del recurso. Si producto de la interposición de recusaciones o implicancias no hubiere tribunal, los autos serán conocidos el día siguiente, según las reglas precedentes.

En caso de que se requiriera la restricción del acceso o uso de redes o sistemas informáticos se estará a lo dispuesto en este literal. No obstante, la Agencia deberá actuar conjuntamente con la autoridad sectorial correspondiente.

El procedimiento dispuesto en los incisos precedentes también será aplicable los requerimientos de acceso a redes y sistemas informáticos a que se refiere en el inciso tercero del literal ñ) del presente artículo.

l) Cooperar con organismos públicos e instituciones privadas, 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 autoridades nacionales de ciberseguridad extranjeras o sus homólogos y con los organismos internacionales con competencia en materia de ciberseguridad.

Cuando se trate de la cooperación con Estados y organizaciones internacionales, dicha actividad deberá realizarse en coordinación con el Ministerio de Relaciones Exteriores, en conformidad con lo previsto en el inciso primero del artículo 2º de la ley N° 21.080.

m) Prestar, cuando sus recursos humanos, técnicos y financieros así lo permitan, 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.

n) Colaborar 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.

ñ) 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.

Para el cumplimiento de su función fiscalizadora, la Agencia podrá realizar inspecciones; instruir de manera particular auditorías por sí o mediante terceros autorizados y análisis de seguridad basados en criterios de evaluación de riesgos objetivos, los cuales deberán ser no discriminatorios, equitativos y transparentes. La entidad fiscalizada deberá cooperar en todo momento con los funcionarios de la Agencia o con los terceros autorizados por ella, según corresponda.

Asimismo, la Agencia podrá requerir el acceso a sistemas informáticos, datos, documentos y demás información que fuere necesaria para el desempeño de sus funciones de supervisión y fiscalización; instruir de manera particular a los sujetos obligados que realicen pruebas que demuestren la implementación de los planes de continuidad operacional y ciberseguridad, referidos en la letra c) del artículo 8°. Adicionalmente, podrá citar a declarar, respecto de hechos cuyo conocimiento estime necesario para el cumplimiento de sus funciones, a los socios, directores, administradores, representantes, empleados, y cualquier persona que, a cualquier título, preste o haya prestado servicios para las personas o entidades fiscalizadas, así como a toda persona que hubiere ejecutado o celebrado con ellas actos o convenciones de cualquier naturaleza. No obstante, no estarán obligadas a concurrir a declarar las personas indicadas en el artículo 361 del Código de Procedimiento Civil, a las cuales la Agencia, para los fines expresados en el párrafo precedente, deberá pedir declaración por escrito.

Para el ejercicio de esta atribución podrá establecer la forma, plazos y procedimientos para que las entidades fiscalizadas cumplan la obligación de presentar los antecedentes e informaciones referidos en los párrafos precedentes.

o) Instruir el inicio de procedimientos sancionatorios y sancionar las infracciones e incumplimientos en que incurran las instituciones obligadas por la presente ley respecto de sus disposiciones, reglamentos e instrucciones generales y particulares que emita la Agencia. Para tales efectos, y de manera fundada, podrá citar a declarar, en los términos señalados en el literal n) de este artículo, 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. La

declaración podrá tomarse presencialmente o por otros medios que aseguren su integridad y fidelidad.

p) 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.

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

r) Informar al CSIRT de la Defensa Nacional y a los CSIRT de los organismos de la Administración del Estado 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.

s) 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.

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

u) 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.

v) 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.

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

x) Administrar la Red de Conectividad Segura del Estado.

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

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

Párrafo 2°
Dirección, organización y patrimonio

Artículo 12. 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 13 Subdirección. Existirá un Subdirector o Subdirectora Nacional de la Agencia, quien dependerá del Director o Directora Nacional y lo subrogará, en caso de ausencia o impedimento, y además ejercerá las funciones de los literales ñ) y o) del artículo 11. Para ello, contará con la atribución de instruir la apertura de procedimientos administrativos sancionadores, designar a los funcionarios a cargo, determinar las sanciones e imponerlas.

El Subdirector o Subdirectora Nacional de la Agencia, estará afecto al Sistema de Alta Dirección Pública, establecido en la ley N° 19.882, como cargo de segundo nivel jerárquico.

Artículo 14. 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, y

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

Artículo 15. 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 16. 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 17. 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 el año 2000 y publicado el año 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 el año 2004 y publicado el año 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 el año 2004 y publicado el año 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. Estos 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 el año 2004 y publicado el año 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, promulgado y publicado el año 1977, del Ministerio de Hacienda, y al decreto supremo N° 1, promulgado y publicado el año 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 fue fijado por el decreto con fuerza de ley N° 1, promulgado el año 2000 y publicado el año 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, promulgado y publicado el año 1975, de Administración Financiera del Estado.

Artículo 18. 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 éstas 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 a fin de 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 el año 2004 y publicado el año 2005, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.834, sobre Estatuto Administrativo.

Artículo 19. Notificación responsable de vulnerabilidades. No serán aplicables las obligaciones previstas en el artículo 175 del Código Procesal Penal y en el artículo 61, literal k), del Estatuto Administrativo, a los trabajadores de la Agencia respecto de la información que reciban por parte de las personas que les notifiquen vulnerabilidades de ciberseguridad. La Agencia deberá mantener en secreto la

notificación, sus antecedentes y la identidad de quien la realice, no pudiendo esta última ser revelada sin el consentimiento expreso de la persona que la realizó.

Párrafo 3°
Consejo Multisectorial sobre Ciberseguridad

Artículo 20. 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, cuyo objeto o razón social se refiera a materias de esta ley, 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 21. 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 51.

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

Párrafo 4°
Red de Conectividad Segura del Estado

Artículo 23. 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 el 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 24. 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 éstos sean de efecto significativo.

b) Coordinar a los CSIRT que pertenezcan a organismos de la Administración del Estado 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, incluida la supervisión de las medidas adoptadas por éstos.

Cuando los ciberataques o incidentes puedan afectar el normal funcionamiento del sistema financiero, la respuesta del CSIRT Nacional deberá realizarse en coordinación con el Consejo de Estabilidad Financiera creado por la ley N° 20.789. Sin perjuicio de la obligación del CSIRT Nacional de comunicar al mencionado Consejo sobre el incidente, podrá tomar medidas sin esperar respuesta en casos de urgencia.

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 que pertenezcan a organismos de la Administración del Estado 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
Coordinación regulatoria y otras disposiciones

Artículo 25. Coordinación regulatoria. Cuando la Agencia deba dictar protocolos, estándares técnicos o instrucciones de carácter general en el ejercicio de sus funciones, y estos tengan efectos en las áreas de competencia de otra entidad sectorial, deberá previamente remitir la información relevante a dicha entidad y solicitar un informe con el propósito de prevenir posibles conflictos normativos y garantizar la coordinación, cooperación y colaboración efectivas entre ambas autoridades.

La autoridad sectorial requerida deberá evacuar su informe dentro de un plazo de treinta días corridos a partir de la fecha en que recibió la solicitud indicada en el inciso anterior. La Agencia considerará el contenido de este informe en la motivación del acto administrativo de carácter general que emita. Transcurrido el plazo sin que se hubiere recibido el informe correspondiente, la Agencia procederá a emitir los protocolos, estándares técnicos o instrucciones generales requeridos.

Cuando una autoridad sectorial, en el ejercicio de sus atribuciones establecidas en sus leyes orgánicas, deba emitir actos administrativos de

carácter general que tengan efectos en los ámbitos de competencia de la Agencia en conformidad a la presente ley, deberá remitir a la Agencia la información pertinente y solicitar un informe con el objeto de prevenir posibles conflictos normativos y garantizar la coordinación, cooperación y colaboración entre ambas entidades. Además, en el ejercicio de estas atribuciones, las autoridades sectoriales deben tener en cuenta, al menos, los protocolos, estándares técnicos e instrucciones generales previamente emitidos por la Agencia.

Lo establecido en los incisos anteriores no se aplicará en los casos en que el acto administrativo respectivo requiera una aplicación inmediata o en el plazo más breve posible atendida a su naturaleza y urgencia, siempre que se justifique dicha circunstancia y se deje constancia. No obstante, en estos casos, la Agencia deberá, en un plazo de tres días corridos, proporcionar a las autoridades sectoriales competentes, o viceversa según corresponda, todos los documentos tenidos a la vista y solicitar un informe con el fin de cumplir con los objetivos mencionados en los incisos primero y tercero.

Artículo 26. Normativa Sectorial. Las autoridades sectoriales podrán emitir normativas generales, técnicas e instrucciones necesarias para fortalecer la ciberseguridad en las instituciones de su sector, en conformidad con la regulación respectiva y siguiendo lo dispuesto en el artículo anterior, cuando corresponda.

Las instituciones supervisadas deberán cumplir obligatoriamente con estas normas e instrucciones en la gestión de sus riesgos, de acuerdo con la autoridad sectorial que las haya emitido. La fiscalización y sanción relacionadas con estas disposiciones se regirán por las leyes respectivas de dicha autoridad sectorial.

Cuando las normas o instrucciones emitidas por una autoridad sectorial establezcan obligaciones para un sector a fin de prevenir incidentes de ciberseguridad, que tengan, al menos, efectos equivalentes a las obligaciones previstas en los protocolos, normas o instrucciones de la Agencia, prevalecerán las disposiciones de la autoridad sectorial. Esto no afectará los deberes de coordinación establecidos en el artículo 25 ni la aplicación de las normas de la presente ley. No obstante, si las normas o instrucciones de una autoridad sectorial no cubren a todas las entidades de un sector o solo se aplican a una parte de sus supervisados, los protocolos, normas o instrucciones de la Agencia seguirán siendo plenamente aplicables a las entidades no exceptuadas en los términos indicado en este inciso.

Para efectos de lo indicado en el inciso anterior, la Agencia y la autoridad sectorial correspondiente deberán previamente dictar una norma conjunta de carácter general. Dicha norma tendrá por objeto establecer criterios para la evaluación de la equivalencia de los efectos entre una normativa o instrucción.

Artículo 27. 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 que pertenezcan a los organismos de la Administración del Estado 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 28. Centros de Certificación. Los operadores de importancia vital deberán obtener las certificaciones de ciberseguridad que señala esta ley y las que determine la Agencia mediante reglamento. Para estos efectos, solo los organismos que sean parte del registro de entidades certificadoras autorizadas a cargo de la Agencia, estarán habilitadas para emitir certificaciones válidas que esta ley exija. Para formar parte de este registro bastará acreditar el cumplimiento de los requisitos que establezca el reglamento, pudiendo mantenerse en tanto cumplan los referidos requisitos.

La Agencia podrá homologar certificaciones técnicas internacionales o extranjeras sobre ciberseguridad mediante resolución fundada de su director o directora.

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

Artículo 29. 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 30. 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 31. 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 32. 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, conforme a lo que determine el reglamento.

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

Artículo 33. 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 que pertenezcan a organismos de la Administración del Estado o de su personal, cualquiera que sea su cargo o la naturaleza de su vinculación jurídica con éstos. Asimismo, tendrán dicho carácter aquellos otros antecedentes respecto de los cuales el personal de tales organismos del Estado tome conocimiento en el desempeño de sus funciones o con ocasión de éstas.

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 éste indique.

Los funcionarios y funcionarias de la Agencia y del CSIRT Nacional, de Defensa o de los que pertenezcan a organismos de la Administración del Estado 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 8°, 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 34. 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 35. Deber de reserva de la Agencia. La Agencia deberá mantener y cautelar la reserva de la información que llegue a conocer en el desempeño de sus funciones cuando ella tenga tal calidad en virtud de una norma legal o porque, habiendo sido requerida por ella, le sea entregada bajo tal calidad. Asimismo, deberá procurar 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.

Sin perjuicio de lo anterior, no se incumple el deber de reserva en aquellos casos en que la Agencia o el CSIRT Nacional, en cumplimiento de sus funciones, deba difundir antecedentes que se encontraren sujetos a reserva, siempre que ello permita gestionar, prevenir o contener un incidente de ciberseguridad.

Artículo 36. 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 37. Competencia de la autoridad sectorial**.** La autoridad sectorial será competente para fiscalizar, conocer y sancionar las infracciones, así como ejecutar las sanciones a la normativa sobre ciberseguridad que hubiere dictado y cuyos efectos sean al menos equivalentes al de la normativa dictada por la Agencia, conforme lo dispuesto en el artículo 26. Para este efecto, las sanciones y procedimientos sancionatorios serán los que correspondan a la autoridad sectorial de conformidad a su normativa. Fuera de dichos casos, corresponderá a la Agencia fiscalizar, conocer y sancionar las infracciones así como ejecutar las sanciones a la presente ley, sin perjuicio de la facultad de los organismos de la Administración del Estado de poner en conocimiento del organismo competente las infracciones a la norma de que tomaren conocimiento.

Artículo 38. Infracciones. Las infracciones a las obligaciones que esta ley prescribe a los sujetos obligados por ella se califican en leves, graves y gravísimas.

Se considerarán infracciones leves las siguientes:

1. Entregar fuera de plazo la información que se le requiera cuando ella no fuere necesaria para la gestión de un incidente de ciberseguridad;
2. Incumplir las instrucciones generales o particulares impartidas por la Agencia en los casos que no esté sancionado como infracción grave o gravísima; y
3. Cualquier infracción a las obligaciones que esta ley establece y que no tenga señalada una sanción especial.

Se considerarán infracciones graves las siguientes:

1. No haber implementado los protocolos y estándares establecidos por la Agencia para prevenir, reportar y resolver incidentes de ciberseguridad;
2. No haber implementado los estándares particulares de ciberseguridad;
3. Entregar fuera de plazo la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de ciberseguridad;
4. Entregar a la Agencia de información manifiestamente falsa o errónea.
5. Incumplir la obligación de reportar establecida en el artículo 9;
6. Negarse injustificadamente a cumplir una instrucción de la Agencia o entorpecer deliberadamente el ejercicio de las atribuciones de la Agencia durante la gestión de un incidente de ciberseguridad, siempre que la atribución no cuente con una sanción especial; y
7. La reincidencia en una misma infracción leve dentro de un año.

Se considerarán infracciones gravísimas las siguientes:

1. Entregar a la Agencia información manifiestamente falsa o errónea, cuando ella sea necesaria para la gestión de un incidente de ciberseguridad;
2. Incumplir las instrucciones generales o particulares impartidas por la Agencia durante la gestión de un incidente de impacto significativo;
3. No entregar la información que se le requiera cuando ella fuere necesaria para la gestión de un incidente de impacto significativo; y
4. La reincidencia en una infracción grave dentro de un año.

Artículo 39. De las infracciones de los Operadores de Importancia Vital. Sin perjuicio de lo prescrito en el artículo precedente, los Operadores de Importancia Vital podrán ser sancionados por infringir las disposiciones del artículo 8º, las que se califican en leves, graves y gravísimas.

Se considerarán infracciones leves las siguientes:

1. No mantener el registro de las acciones de seguridad que señala la letra b);
2. No comunicar al CSIRT Nacional la realización continua de operaciones de revisión, ejercicios y demás acciones que señala el literal d);
3. No contar con programas de capacitación, formación y educación continua para los trabajadores, según dispone el literal g);

4. No designar un delegado de ciberseguridad, según dispone la letra i);
5. No dar cumplimiento a la instrucción particular de la Agencia en orden a certificar los planes de continuidad operacional del párrafo segundo de la letra c); y
6. No contar con las certificaciones que exija la ley, de acuerdo al literal f).

Se considerarán infracciones graves las siguientes:

1. No haber implementado el sistema de gestión de seguridad de la información continuo al que se refiere el literal a);
2. No haber elaborado o implementado los planes de continuidad operacional y ciberseguridad a los que se refiere la letra c);
3. No informar a los potenciales afectados sobre la ocurrencia de incidentes o ciberataques que pudieran comprometer gravemente su información o redes y sistemas informáticos, en los casos que señala la letra g);
4. No adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o un ciberataque, según señala la letra e); y
5. La reincidencia en una misma infracción leve dentro del periodo de un año.

Se considerarán infracciones gravísimas las siguientes:

1. No adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad o un ciberataque, según señala la letra e), cuando este posea un impacto significativo; y
2. La reincidencia en una misma infracción grave dentro del periodo de un año.

Artículo 40. De las sanciones. La infracción a los preceptos de esta ley conlleva la imposición de una multa a beneficio fiscal, de acuerdo a la siguiente escala:

1. Las infracciones leves serán sancionadas con multa de hasta 5.000 unidades tributarias mensuales; o con hasta 10.000 unidades tributarias mensuales si se tratare de un operador de importancia vital;
2. Las infracciones graves serán sancionadas con multa de hasta 10.000 unidades tributarias mensuales; o con hasta 20.000 unidades tributarias mensuales si se tratare de un operador de importancia vital; y
3. Las infracciones gravísimas serán sancionadas con multa de hasta 20.000 unidades tributarias mensuales; o con hasta 40.000 unidades tributarias mensuales si se tratare de un operador de importancia vital.

La multa será fijada teniendo en consideración el grado en que el infractor adoptó las medidas necesarias para resguardar la seguridad informática de las operaciones, la probabilidad de ocurrencia del incidente, el grado de exposición del infractor a los riesgos, la gravedad de los efectos de los ataques incluidas sus repercusiones sociales o económicas, la reiteración en la infracción dentro del plazo de 3 años contado desde el momento en que se produjo el incidente, el tamaño 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 41. Procedimiento simplificado. Tratándose de la formulación de cargos por infracciones calificadas como leves en conformidad al artículo 38, la Agencia estará facultada para proponer de manera inmediata la sanción a aplicar, la cual quedará firme si el presunto infractor opta por allanarse a los cargos formulados en su contra. En caso contrario, si el presunto infractor decide rechazar la imputación y presentar descargos, se procederá conforme a lo indicado en el artículo 40 de la presente ley.

Artículo 42. Procedimiento administrativo sancionador. El procedimiento administrativo se regirá por lo prescrito por la ley Nº19.880, que establece bases de los procedimientos administrativos que rigen los actos de los organismos de la Administración del Estado, sin perjuicio de las siguientes disposiciones:

a) Toda sanción deberá fundarse en un procedimiento que se iniciará con la formulación precisa y fundada de los cargos y contendrá la descripción de los hechos en los que se fundamentan y de cómo éstos constan en la investigación, la indicación de por qué se consideran una infracción a la normativa, especificando la o las normas que se estimen infringidas y el presunto responsable de la infracción. Además, se designará al funcionario a cargo de la instrucción del procedimiento. Se fijará un plazo para la formulación de descargos que no podrá ser inferior a quince ni superior a treinta días. Las notificaciones del procedimiento deberán realizarse a la dirección de correo electrónico que haya sido proporcionada a la Agencia, de conformidad al reglamento.

b) En los descargos deberán señalarse todas las circunstancias o antecedentes de hecho y de derecho que eximan o atenúen la presunta responsabilidad de la persona objeto de cargos, así como aquellas que nieguen la efectiva ocurrencia de los hechos, o que demuestren que éstos no constituyen infracción. Todo ello, sin perjuicio de otras presentaciones o antecedentes posteriores que se hagan valer en el curso del procedimiento sancionatorio con el mismo objetivo. Asimismo, deberán solicitarse las diligencias probatorias que correspondieren.

c) Vencido el plazo para formular descargos, se abrirá un término probatorio por un plazo no inferior a diez ni superior a veinte días, según la naturaleza y complejidad del asunto. Dicho plazo podrá prorrogarse por una sola vez y hasta por un máximo de quince días. Se podrá rendir prueba mediante cualquier medio admisible en Derecho, los que se apreciarán de acuerdo a las reglas de la sana crítica.

d) Excepcionalmente, se realizarán las diligencias que, decretadas de oficio o a petición de parte, se estimen estrictamente necesarias para la resolución del asunto. Las diligencias podrán solicitarse dentro de los cinco días siguientes al vencimiento del término probatorio.

e) Una vez transcurrido el plazo mencionado en el literal previo, el procedimiento deberá concluir. El instructor del procedimiento emitirá un informe en el cual deberá incluir un análisis detallado de todas las defensas, alegatos y pruebas presentadas durante el procedimiento sancionatorio a partir del cual se determinará si se ha infringido la normativa vigente y si procede la imposición de la sanción respectiva o la absolución de los cargos. El informe deberá emitirse dentro del plazo de quince días.

f) Una vez recibido el informe del instructor del procedimiento, corresponderá al Subdirector de la Agencia resolver los procesos

sancionatorios en el plazo de quince días, dictando al efecto resolución fundada en la cual absolverá al infractor o aplicará la sanción, en su caso. La resolución del Subdirector deberá incluir el mismo contenido que el informe señalado en el literal precedente.

Artículo 43. De los recursos. En contra de la resolución del Subdirector mediante la cual se concluye el procedimiento administrativo procederán los recursos que establezca la ley Nº19.880. El recurso deberá resolverse dentro del plazo de quince días. La interposición del recurso suspenderá el plazo para reclamar de ilegalidad, siempre que se trate de materias por las cuales procede dicho recurso.

Artículo 44. Forma de pago de las multas. Las multas deberán pagarse dentro de los diez días siguientes contados desde que el acto administrativo que las impone quede firme. Vencido ese plazo, la resolución que establezca la sanción tendrá mérito ejecutivo y se hará exigible por la Tesorería General de la República. Para su cobro se aplicará el inciso segundo del artículo 35 del decreto ley N° 1.263, de 1975, orgánico de Administración Financiera del Estado.

El pago de toda multa deberá ser acreditado ante la Agencia, dentro de los diez días siguientes a la fecha en que ésta debió ser pagada.

El retardo en el pago de estas multas devengará los intereses y reajustes establecidos en el artículo 53 del Código Tributario.

Artículo 45. Pronto pago. El sancionado que no interponga recurso alguno podrá, dentro de los cinco días siguientes a que le sea notificada la resolución del Subdirector que le impone la sanción, pagar directamente en la Tesorería General de la República en cuyo caso, el monto de la misma será reducido en un veinticinco por ciento. Una vez ejercido este derecho, se entenderán renunciado todos los recursos.

Lo dicho en este artículo no será aplicable para el caso previsto en el artículo anterior.

Artículo 46. 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, los que deberán computarse de acuerdo al artículo 25 de la ley N°19.880, 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 pueda ocasionar 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 se podrá apelar ante la Corte Suprema, dentro del plazo de diez días hábiles, la que resolverá en cuenta.

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 47. Responsabilidad administrativa del jefe superior del organismo de la administración del Estado. El jefe superior del organismo de la administración del Estado deberá velar porque el organismo respectivo aplique las medidas idóneas y necesarias para prevenir, reportar y resolver incidentes de ciberseguridad con arreglo a lo establecido en esta ley.

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

TÍTULO VIII
Del Comité Interministerial sobre Ciberseguridad

Artículo 48. 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 ésta incida en materias de ciberseguridad.

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

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

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

Artículo 49. De los integrantes del Comité. El Comité estará integrado por los siguientes miembros permanentes:

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

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

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

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

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

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

g) Por el Subsecretario de Ciencia, Tecnología, Conocimiento e Innovación o quien éste 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 50. 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 51. 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 52. 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 53. Regímenes especiales. El Senado y la Cámara de Diputados, el Poder Judicial, la Contraloría General de la República, el Banco Central, el Ministerio Público, el Servicio Electoral y el Consejo Nacional de Televisión deberán adoptar las medidas de seguridad de sus redes y sistemas informáticos que sean pertinentes. Para estos efectos, la Corte Suprema, el respectivo jefe de servicio o los órganos colegiados que ejerzan dicha función, podrán dictar la normativa que sea conveniente a tales efectos, pudiendo considerar en su formulación las recomendaciones que efectúe la Agencia.

Las instituciones y órganos señalados en este artículo no estarán sujetos en modo alguno a la regulación, fiscalización o supervigilancia de la Agencia; sin perjuicio de que deberán convenir mecanismos de reporte de incidentes de ciberseguridad y de coordinación y cooperación para la respuesta a incidentes de ciberseguridad.

Asimismo, si el órgano autónomo constitucional revistiera el carácter de autoridad sectorial, deberá considerársele para los efectos de los artículos 6, 25 y 26.

TÍTULO X
De las modificaciones a otros cuerpos legales

Artículo 54. 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 55. Introdúcense las siguientes enmiendas en 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°, el siguiente inciso final, nuevo:

“No será objeto de sanción penal por haber incurrido en los hechos tipificados en el inciso primero, el que habiendo accedido a un sistema informático cuyo responsable tenga domicilio en Chile, lo hiciera cumpliendo con las siguientes condiciones:

1) Encontrarse inscrito en el registro que al efecto lleve la Agencia Nacional de Ciberseguridad;

2) Que el acceso se haya realizado habiendo informado previamente de ello a la Agencia;

3) Que el acceso y las vulnerabilidades de seguridad detectadas hayan sido reportadas al responsable del sistema informático y a la Agencia, tan pronto se hubiere realizado;

4) 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 utilizando métodos que pudieran conducir a denegación de servicio, a pruebas físicas, utilización de código malicioso, ingeniería social y alteración, eliminación, exfiltración o destrucción de datos;

5) No haber divulgado públicamente la información relativa a la potencial vulnerabilidad;

6) Que se trate de un acceso a un sistema informático de los organismos de la administración del Estado. En el resto de los casos, requerirá del consentimiento del responsable del sistema informático.

7) Haber dado cumplimiento a las demás condiciones sobre comunicación responsable de vulnerabilidades que al efecto hubiere dictado la Agencia.

2. Derógase el artículo 16.

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. Determinar un periodo para la vigencia de las normas establecidas por la presente ley el cual no podrá ser inferior a seis meses desde su publicación.

3. 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.

4. 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.

5. 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 párrafos 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 párrafo anterior cumpla con los requisitos respectivos y dé su consentimiento, las modificaciones de estatuto laboral señaladas en el mencionado párrafo 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 párrafo 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.

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

7. 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 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.

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. 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 20, 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 sexto. 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.”.”.

SALA DE LA COMISIÓN, a 22 de noviembre de 2023.

Tratado y acordado en sesiones de fechas 10 y 31 de mayo, 7 y 14 de junio, 10 de julio, 2 y 30 de agosto, 6, 13 y 27 de septiembre, 4, 11, 18 y 25 de octubre y 8 y 22 de noviembre de 2023, con la asistencia de las y los diputados señores Jorge Alessandri, Jaime Araya, Cristián Araya, José Miguel Castro, Lorena Fries, Andrés Jouannet, Henry Leal, Raúl Leiva, Andrés Longton (Presidente), Gloria Naveillan, Maite Orsini, Alejandra Placencia y Diego Schalper.

Reemplazos temporales:

La diputada señora Ximena Ossandón al diputado señor Diego Schalper.

Pareos:

De los diputados señores Jaime Araya y Andrés Longton.

De los diputados señora Maite Orsini y señor Cristián Araya.

De los diputados señores José Miguel Castro y Jaime Araya

De las diputadas señoras Lorena Fries y Gloria Naveillan.

De los diputados señores Raúl Leiva y Andrés Jouannet.

Otros Diputados:

Sergio Bobadilla, Mauricio Ojeda y Hugo Rey.

ALVARO HALABI DIUANA
Abogado Secretario de la Comisión

ÍNDICE